Содержание:

ВВЕДЕНИЕ

Информационная Эра привела к драматическим изменениям в способе выполнения своих обязанностей для большого числа профессий. Теперь нетехнический специалист среднего уровня может выполнять работу, которую раньше делал высококвалифицированный программист. Служащий имеет в своем распоряжении столько точной и оперативной информации, сколько никогда не имел.

Но использование компьютеров и автоматизированных технологий приводит к появлению ряда проблем для руководства организацией. Компьютеры, часто объединенные в сети, могут предоставлять доступ к колоссальному количеству самых разнообразных данных. Поэтому люди беспокоятся о безопасности информации и наличии рисков, связанных с автоматизацией и предоставлением гораздо большего доступа к конфиденциальным, персональным или другим критическим данным. Все увеличивается число компьютерных преступлений, что может привести в конечном счете к подрыву экономики. И поэтому должно быть ясно, что информация - это ресурс, который надо защищать.

Целью данной работы являются преступления в сфере компьютерной информации, для достижения поставленной цели были выделены следующие задачи:

- рассмотреть принятие и общественную опасность компьютерных преступлений;
- изучить виды компьютерных преступлений;
- рассмотреть особенность квалификации отдельных видов компьютерных преступлений.

Объектом работы являются компьютерные преступления.

Структура работы состоит из введения, основной части, заключения и списка литературы.

Теоретической и методологической базой данной работы послужили труды российских авторов в области уголовного права, нормативно-правовая база РФ, материалы периодических изданий и сети Интернет.

ГЛАВА 1. ТЕОРЕТИЧЕСКИЕ АСПЕКТЫ ИЗУЧЕНИЕ ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

1.1 Понятие компьютерная преступность

Одной из социальных проблем современного технократического общества стало появление компьютерной преступности, причиняющей колоссальный вред существующим информационным отношениям.

Масштабы ущерба, причиняемого компьютерными преступлениями в РФ, впечатляют. Так, по оценкам аналитиков компании Group-IB объем рынка киберпреступности в РФ в 2012 году составил 1,93 миллиарда долларов [14], а с середины 2013 по середину 2014 года в России и СНГ русскоговорящие хакеры «заработали» $2,5 млрд, что составляет 2 % от глобального рынка [15].

В свою очередь, американская корпорация Symantec оценила ущерб от киберпреступности в России за 2013 год в 1 миллиард долларов, а в 2012 году в 1,48 миллиарда долларов. При этом общий ущерб от киберпреступности в мире в 2013 году составил 113 миллиардов долларов [16].

По данным исследования Cost of CyberCrime Study, проведенного в 2014 году компанией Ponemon Institute при поддержке HP Enterprise Security, среднегодовой ущерб российской организации от киберпреступлений в 2014 году достиг $3,3 млн. [17].

Проведенный анализ специальной и научной литературы показывает, что вопросам противодействия компьютерным преступлениям в Российской Федерации уделяется достаточно пристальное внимание со стороны научного сообщества [4, 5, 10, 11].

Однако, что же следует понимать под компьютерной преступностью? На этот, казалось бы, простой вопрос в криминологической науке нет однозначного ответа, и до сих пор ведутся многочисленные дискуссии о содержании и значении этого юридического понятия. В настоящее время в отечественной науке сложилось несколько подходов к определению рассматриваемого понятия.

Во-первых, компьютерная преступность - это совокупность преступлений, в которых предметом преступных посягательств выступает компьютерная информация. При этом понятия компьютерное преступление и преступление в сфере компьютерной информации являются синонимами [7, с. 830; 1, с. 9].

Во-вторых, компьютерная преступность - это совокупность совершенных на определенной территории за определенный период преступлений (лиц, их совершивших), непосредственно посягающих на отношения по сбору, обработке, накоплению, хранению, поиску и распространению компьютерной информации, а также преступлений с использованием компьютера в целях извлечения материальной выгоды или иной личной заинтересованности [8, с. 39].

В-третьих, компьютерная преступность - это совокупность всех преступлений в сфере «информационных технологий», а не только общественно опасных деяний, предметом которых является компьютерная информация [2; с. 45-46].

В-четвертых, компьютерная преступность - это совокупность преступлений, совершаемых с помощью компьютерной системы или сети, в рамках компьютерной системы или сети и против компьютерной системы или сети. Данный подход предполагает, что кроме преступлений в сфере компьютерной информации, компьютерными преступлениями также являются и преступления, связанные с компьютерами. То есть такие традиционные по характеру преступные деяния, совершенные с помощью вычислительной техники, как кража, мошенничество, причинение вреда и некоторые другие, за которые предусматриваются уголовные санкции в законодательствах большинства стран [6, с. 18-19].

Между тем, в ряде научных работ российских авторов [12, 13] можно встретить упоминание о «киберпреступности», юридическом понятии, которое часто употребляется в научном обороте за рубежом и, по мнению указанных ученых более полно отражает преступные деяния в сфере компьютерной информации, а также преступления совершенные с помощью компьютерных устройств, информационно-телекоммуникационных сетей и информационных технологий.

Поэтому, пятый подход предполагает, что компьютерная преступность является только частью киберпреступности, как более широкого понятия.

Например, Т.Л. Тропина считает, что понятие «компьютерная преступность» недостаточно для охвата всех деяний, совершаемых при помощи вычислительной техники, глобальных сетей. Киберпреступность, по ее мнению, - это совокупность преступлений, совершаемых в киберпространстве с помощью или посредством

компьютерных систем или компьютерных сетей, а также иных средств доступа к киберпространству, в рамках компьютерных систем или сетей, и против компьютерных систем, компьютерных сетей или компьютерных данных [12, с. 36].

Схожей позиции придерживается И.Г. Чекунов, считая, что киберпреступность предлагается рассматривать в качестве самостоятельного вида преступности, определяемого на основе обнаружения обязательного присутствия в преступлениях таких признаков объективной стороны, как средство или орудие, в качестве которых выступает вредоносная компьютерная программа или программно-техническое средство, подключенное к компьютерной сети или сотовому оператору связи [13, с. 7].

Шестой подход заключается в отождествлении понятий «преступность в Интернете», «киберпреступность», «компьютерная преступность» [9, с. 251-253].

Наконец, следующий подход, предполагает существование понятий «интернет-преступность» и «компьютерная преступность». При этом «Интернет-преступность» является частью компьютерной преступности, если выделять компьютерную преступность по средству совершения, так как любое Интернет-преступление - это компьютерное преступление, но не наоборот. Не каждое преступление в сфере компьютерной информации является Интернет-преступлением, в тоже время такие традиционные преступления, как мошенничество, кража, вымогательство и другие, совершенные посредством Интернет, - это Интернет-преступления. При этом последствия не обязательно должны наступать в сети Интернет. В свою очередь, российской Интернет-преступностью (или Интернет-преступностью в России) называется социально негативное явление, представленное в виде совокупности преступлений (запрещенных УК РФ деяний) и их системы, которые совершены посредством или с помощью сети Интернет с территории Российской Федерации, либо с территории других государств, но направленных против интересов Российской Федерации [3, с. 44-45].

С учетом рассмотренных подходов к пониманию компьютерной преступности, автор полагает, что было бы логичным рассматривать компьютерную преступность в узком и широком смыслах.

В «узком смысле», по мнению автора, компьютерная преступность представляет собой совокупность преступлений, где в качестве непосредственного основного объекта преступления выступают охраняемые законом общественные отношения в

сфере безопасного создания, хранения, обработки и передачи компьютерной информации, а предметом преступного посягательства являются компьютерная информация, средства защиты компьютерной информации, информационно-телекоммуникационные сети, средства хранения, обработки и передачи компьютерной информации.

Тем самым, понятие «компьютерные преступления» полностью совпадает с установленным законодателем понятием «преступления в сфере компьютерной информации».

В свою очередь, компьютерная преступность в широком смысле представляет собой совокупность преступлений, где объектом преступного посягательства выступают любые общественные отношения в сфере информационных технологий и безопасного функционирования компьютерной информации. При этом компьютерная информация, информационно-телекоммуникационные сети; средства создания, хранения, обработки, передачи компьютерной информации (компьютеры, смартфоны, айфоны, кассовые аппараты, банкоматы, платежные терминалы и иные компьютерные устройства) являются не только предметом преступного деяния, но и используются в качестве средства и орудия совершения преступления. Таким образом, компьютерная преступность в ее «широком смысле» больше по объему и содержанию таких понятий как «киберпреступность», «интернет-преступность», «преступность в сфере компьютерной информации», «преступность в сфере информационных технологий», поглощая их как структурные элементы. Следует также отметить, что по нашему мнению, понятия «киберпреступность» и «интернет-преступность» являются равнозначными по смыслу, характеризуя преступления, где информационная сеть «Интернет» выступает местом, способом, средством и орудием совершения преступного деяния.

Дуалистический подход к пониманию компьютерной преступности, по мнению автора, позволяет оценить всю сложность, многообразие, разноуровневость рассматриваемого криминального явления и найти определенный баланс среди существующих научных позиций

1.2 Виды компьютерных преступлений

Самым распространенным видом преступления, где компьютерная информация выступает в качестве средства совершения преступления, являются хищения.

С развитием и повсеместным внедрением сети Интернет появились новые возможности ее использования. Но все эти нововведения привели и к расширению сферы деятельности для правонарушителей и появлению новых видов преступных посягательств, в том числе такого, как мошенничество с использованием компьютерной информации. В 2014 г. по данным МВД РФ было зарегистрировано около 11000 компьютерных преступлений, т.е. 41%. В 2013 г. киберпреступность составляла 30% [5].

При этом, по оценкам экспертов, реальное число интернет-мошенничеств в несколько раз выше, так как подобные преступления характеризуются высоким уровнем латентности. Именно поэтому взоры многих исследователей- правоведов сегодня вновь обращены к проблеме уголовной ответственности за мошенничество с использованием компьютерной информации.

Одной из тенденций в области IT-преступлений стало возрастающее использование мобильных телефонов, смартфонов, гаджетов, как средства получения конфиденциальной информации. Киберпреступники, в частности, активно эксплуатируют вредоносные программы, ориентированные на хищение средств с банковских счетов с использованием системы мобильного банка.

Во многих зарубежных странах имеется специальная норма, предусматривающая уголовную ответственность за кибермошенничество или компьютерное мошенничество [3, с.113]. Подобная норма имеется и в России (ст.159.6 УК РФ), появление которой вызвало достаточно много споров и вопросов среди ученых и практических работников.

Развитие технологий в современном мире не только позволяет человечеству решать множество проблем его прогрессивной эволюции, но и в связи с этим одновременно порождает новые угрозы в области виртуального Интер- нет-пространства (киберпространства), которое в большинстве случаев исследователи называют информационным.

Данная норма - 159.6 УК РФ «мошенничество в сфере компьютерной информации» не только не решает существующие проблемы, но еще в большей степени может усугубить их. Так, в различных научных статьях встречаются такие понятия как «компьютерное мошенничество» и «кибермошенничество», которые являются синонимами. Следует отметить, что понятие «компьютерное мошенничество» в ст.159.6 УК РФ не раскрывается, а лишь дается понятие «мошенничества в сфере компьютерной информации», и носит лишь криминологический характер.

Под мошенничеством в сети Интернет подразумевается совокупность преступлений, характеризующихся единством способа совершения преступления (использование технологических и коммуникационных возможностей компьютерных систем, подключенных к глобальной сети Интернет, для совершения обмана человека или "обмана" компьютерной системы), а также корыстной мотивацией преступной деятельности [2, с.20]. Таким образом, мошенничество в сети Интернет - это разновидность компьютерного мошенничества. Особое внимание следует обратить на мошенничество с пластиковыми картами. Для того чтобы совершить мошенничество с пластиковой картой, преступнику достаточно знать ее номер и секретный код. Довольно часто преступники, узнав пин-код владельца карты, завладевают всеми денежными средствами или просят набрать определенную комбинацию, после чего сумма с карты владельца переходит на счет преступника.

Отдельно следует отметить мошенничество с использованием средств мобильной связи (телефонное или мобильное мошенничество), получившее достаточно широкое распространение в России. Мобильные телефоны также способны обрабатывать и хранить компьютерную информацию, с их помощью можно выйти в глобальную сеть Интернет. Кроме того, существуют и иные устройства, которые выполняют схожие с компьютером функции и также могут являться носителями компьютерной информации - смартфоны, i-phone и др. Поэтому было бы правильнее говорить не о компьютерной, а об электронной информации, которая обрабатывается как в компьютерах, и в мобильных телефонах, и в иных схожих по функциям устройствах.

Также следует обратить внимание на то, что компьютерные преступления делятся на две группы: к первой группе относятся преступления, где компьютерная информация является объектом преступления, ко второй - относятся преступления, при которых информация является средством совершения преступления. Компьютерное мошенничество входит во вторую группу преступлений. Следовательно, была бы, наверное, более верной такая формулировка, как "мошенничество с использованием электронной информации".

Понятие «компьютерной информации» приводится в примечании к ст.272 УК РФ. В последнее время правоприменительная практика сталкивается с проблемой, что следует считать «средствами хранения, обработки и передачи информации». В некоторых случаях к этим средствам относят мобильные телефоны и кассовые аппараты. Так, Грачевским районным судом Ставропольского края было рассмотрено уголовное дело в отношении Л., которая осуждена по двум эпизодам:

по ч.1 ст.159.6 и ч.2 ст.159.6 УК РФ. Л., получив на мобильный телефон смс-сообщение посредством услуги Мобильный банк, о доступном лимите денежных средств в сумме 1149 рублей 90 копеек, на не принадлежащем ей банковском счету, который был открыт на имя гр. Р., использовала принадлежащий ей мобильный банк и сим-карту, к которой ошибочно была подключена данная услуга банка. Таким образом, Л. путем ввода компьютерной информации в форме электрических сигналов «смс-сообщения» на номер «900», посредством телекоммуникационной сети оператора сотовой связи похитила (перечислила) денежные средства в сумме 1100 рублей 00 копеек, которые находились на расчетном счете карты Сбербанка на сим-карту телефона. Затем, получив сообщение о том, что на расчетном счете имеется 7417 рублей 10 копеек, похитила денежные средства 7400 рублей 00 копеек, которые находились не на ее расчетном счете, а принадлежали гр. Р., и таким образом перевела денежные средства на сим-карту, принадлежащую ей [4].

Таким образом, можно сделать вывод о том, что не совсем ясна цель, которую преследовал законодатель, включив ст. 159.6 в УК РФ. Более логичным было бы включение в основной состав мошенничества (ст.159 УК РФ) наиболее распространенных способов совершения мошенничества, в том числе и электронной информации, под которой следует понимать хищение чужого имущества или права на чужое имущества путем ввода, копирования, удаления, блокировки или модификации электронной информации.

ГЛАВА 2 АНАЛИЗ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ В СЕТИ ИНТЕРНЕТ

2.1 Обзор преступлений в сети Интернет

В настоящее время ЭВМ настолько прочно вошли в нашу жизнь, что с каждым днем все больше и больше граждан хранят в них свою «виртуальную собственность». И если многие из них весьма трепетно относятся к таковой в реальном мире, то сосредоточенным в сложных кибернетических устройствах, каковыми являются персональные ЭВМ, они явно не уделяют должного внимания. Большинство правообладателей интеллектуальной собственности, находящейся в их

персональных компьютерах, продолжают считать, что никому нет дела до информации, сосредоточенной в ПЭВМ, что в файлах нет ничего ценного для хакера, и что все вирусные атаки пройдут мимо. Это далеко не так. За последние годы интенсивного развития телекоммуникационных технологий преступные структуры, постоянно изобретая новые вредоносные программы, превратили Интернет в высокодоходное занятие, своеобразный криминальный бизнес, который при- носит миллиардную прибыль.

В данной главе мы хотели бы дать характеристику наиболее распространенным способам криминального обогащения в сфере Интернет, а также методы и формы противодействия данным противоправным проявлениям. Для этого мы предлагаем проанализировать современное состояние борьбы с киберпреступностью с двух позиций: какая информация, сосредоточенная на компьютерах пользователей, представляет интерес для хакеров и каким образом происходят непосредственно сами хищения интеллектуальной собственности. Отметим, что в подавляющем большинстве случаев для совершения кражи информации пользователей сети Интернет преступники используют специализированные вредоносные программы или методы социального инжиниринга, либо и то, и другое в совокупности — для большей эффективности.

По результатам проведенного нами исследования, можно выделить 4 группы сведений, которые наиболее часто подвергаются атакам с помощью вредоносных программ. Подчеркиваем, что это далеко не весь спектр данных, интересующих криминальные элементы. Это, в частности, информация, позволяющая получить:

• доступ к различным финансовым операциям (онлайн-банкингу, пластиковым картам, электронным деньгам), интернет-аукционам и т.д.; доступ к почтовым ящикам, которые являются неотъемлемой частью ICQ-аккаунтов, как и все найденные на компьютере адреса электронной почты;

• пароли, коды для доступа к интернет-пейджерам, сайтам и др.;

• пароли, коды к онлайн-играм.

Социальная инженерия — это метод управления действиями человека без использования технических средств воздействия. Метод основан на использовании психологических особенностей человека, его восприятии окружающей среды и нравственного состояния.

С помощью услуги «Онлайн-Банкинг» клиенты Банка могут в режиме реального времени контролировать состояние своих счетов.

Интернет-аукцион (он же «онлайновый аукцион») — аукцион, проводящийся посредством интернета. В отличие от обычных аукционов, интернет-аукционы проводятся на расстоянии (дистанционно) и в них можно участвовать, не находясь в определённом месте проведения, делая ставки через интернет-сайт или компьютерную программу аукциона.

Аккаунт — это учётная запись, где хранится персональная информация пользователя для входа на сайт.

Интернет-пейджер, то есть программа для моментального обмена сообщениями, главной функцией которого является вызов заданного пользователя (этот процесс состоит из двух стадий — определения доступности пользователя и установления канала связи).

Целью любой вредоносной программы является контроль за действиями пользователя (например, запись последовательности всех нажатых клавиш), либо целенаправленный поиск ключевых данных в пользовательских файлах или системном реестре. Полученные данные вредоносная программа в итоге передает своему изобретателю или лицу, намеревающемуся совершить преступление. Подобные «творения» относятся к программам типа Trojan-Spy или Trojan-PSW.

«Заразиться» такими программами можно самыми различными путями: при просмотре вредоносного сайта, по почте, в чате, форуме, через интернет-пейджер или иным способом «во время путешествия» в сети Интернет. В качестве примера давайте рассмотрим одну из модификаций широко распространенного программного продукта Trojan-PSW.Win32. LdPinch, который занимается кражей паролей к интернет-пейджерам, почтовым ящи-кам, FTP и другой информации.

Эта вредоносная программа, оказавшись на компьютере, рассылает всем «друзьям» по контакт-листу сообщения типа: «Смотри «далее идет ссылка_на_вредоносную_программу» Классная вещь!)». В результате прак- тически каждый получатель данного сообщения идет по этой вредоносной ссылке и запускает «троянца». И так далее: заразив один компьютер, «троянец» рассылает себя дальше по всем контакт-листам, обеспечивая хакера всеми необходимыми пользовательскими данными для проведения дальнейших преступных операций. Происходит это из-за высокого уровня доверия к ICQ-сообщениям: получатель не сомневается, что сообщение пришло от его знакомого и добросовестно отвечает

ему.

Image not found or type unknown

Рис. 1 - Trojan-Spy.Win32.Agent.ih

FTP позволяет подключаться к серверам и просматривать содержимое каталогов, загружать файлы с сервера или на сервер, передавать файлы между серверами.

В большинстве случаев хакеры одновременно с вредоносными програм-мами вынуждают пользователя компьютера совершить определенные действия, необходимые для достижения ими преступного умысла. Например, при запуске вредоносная программа Trojan-Spy.Win32.Agent.ih выводит следующее диалоговое сообщение (см. рис. 1):

Примерный перевод текста указывает пользователю на необходимость заплатить всего 1 $ за пользование услугами интернета провайдеру. При этом отметим, что сообщение составлено по всем правилам социального инжиниринга, а это:

- пользователю не оставляют времени для размышлений, так как заплатить необходимо быстро, не раздумывая, в день получения письма;

- предлагается заплатить символическую плату — всего лишь 1 доллар, что резко увеличивает шансы мошенников, так как мало кто будет что-либо выяснять из-за одного доллара;

- для стимулирования действий пользователя злоумышленники угрожают: если не заплатишь, администратор заблокирует доступ к Интернету.

При этом, чтобы минимизировать подозрения пользователя в истинности намерений, в качестве отправителя указана администрация провайдера, которая якобы уже проявила заботу о своем пользователе и подготовила все необходимое, осталось только оплатить и не тратить драгоценное время на оформление документации и отправку сообщения. Вполне логично предположить, что администрация провайдера знает адрес электронной почты своего пользователя. Законопослушному пользователю просто не оставляют выбора, и он нажимает кнопку «Pay 1 $», что приводит к появлению следующего диалогового окна (см. рис. 2). Естественно, что после заполнения всех полей и нажатия кнопки «Pay 1 $» никакой оплаты не происходит, а вся информация о вашей кредитной карте

отправляется по почте к мошенникам.

Методы социального инжиниринга используются и отдельно от вредоносных программ. Красноречивым подтверждением этого является фишинг — атака, направленная на клиентов того или иного банка, использующих для управления своего счета систему онлайн-банкинга. Так, например, в рассылаемых от имени банка фальшивых письмах авторы могут утверждать, что учетная запись клиента заблокирована по той или иной причине, и что для ее разблокирования необходимо ввести учетные данные пользователя. При этом в теле письма приводится специальным образом сформированная ссылка. Приводимая ссылка создается хакерами таким образом, что на экране пользователя она отображается как реально существующий сетевой адрес сайта банка (на самом же деле ссылка при ее активации приведет на сайт лица, намеревающегося совершить преступление). Введенные данные опять же попадут не в банк, а к преступнику, который получит данные клиента, а вместе с ними и возможность доступа к его счету.

Фишинг (англ., от fi shing — рыбная ловля, выуживание) — вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей — логинам и паролям.

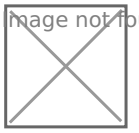

Рис. 2 Всплывающее окно

Похожим образом рассылаются и письма от имени различных служб поддержки, социальных служб и т. п.

Однако преступники «охотятся» не только за данными пользователей кредитных карт. Их интересуют и та- кие данные, как списки электронных адресов пользователей компьютеров.

Неоценимую помощь в этом хакерам оказывают вредоносные программы, которые получили название SpamTool.

Эти программы занимаются сканированием файлов данных на компьютере пользователя и ищут там все адреса электронной почты, хранящиеся в операционной системе. Собранные адреса тут же отфильтровываются по заданным критериям (например, удаляются принадлежащие антивирусным компаниям) и отсылаются лицу, намеревающемуся совершить преступление.

Существуют и куда более циничные способы проникновения вредоносных программ в компьютеры пользователей. Отмечены случаи, когда преступники предлагают оплачивать владельцам сайтов загрузку их «посетителям» вредоносных программ.

Рис. 3

Так, например, поступали с сайтом iframeDOLLARS.biz. Согласно расположенной там «партнерской программе», веб-мастерам предлагалось установить на собственных сайтах эксплойты для дальнейшей автоматической загрузки посетителям вредоносных программ. «Партнерам по бизнесу» авторы предлагали вредоносные программы купить по цене 61 $ за 1000 заражений.

Безусловно, основная причина совершения хищений пользовательской информации имеет корыстную направленность. В конечном итоге практически вся украденная информация продается либо напрямую используется для материального обогащения. Но получить данные кредитных карт и электронные адреса пользователей — это только часть дела, далее злоумышленникам необходимо вывести награбленное из платежной системы, то есть реализовать полученную информацию.

Способы обналичивания преступно нажитых средств путем использования интернет-технологий весьма разнообразны. Если результатом проведенной фишинг-атаки стали, например, параметры для доступа к системе онлайн-банкинга или электронному кошельку пользователя, то средства могут быть выведены через цепочку виртуальных электронных обменных пунктов, например путем перевода одной электронной валюты в другую через электронные платежные системы либо с помощью аналогичных услуг «представителей» киберкриминала. В самом крайнем случае можно приобрести товар непосредственно в интернет-магазине

Во многих случаях этап легализации преступно нажитых средств является самым опасным для преступника, так как приходится указывать какие-либо «свои» идентификационные признаки, например адрес для доставки товара, номер индивидуального счета/электронного кошелька и т. д.

Изощренность в достижении преступных замыслов толкает мошенников на поиск новых путей решения проблем такого рода. Одним из таких направлений приложения усилий современного преступного мира является привлечение людей, которых на языке киберкриминала называют «дропами». Эти люди нужны для того, чтобы преступники избежали уголовной ответственности, получили деньги или товар, оставаясь вне подозрения, а правоохранительные органы пошли по ложному «следу». При этом сами «дропы» зачастую и не знают, для чего их используют.

Существуют самые абсурдные способы вовлечения «дропов» в криминальный бизнес. В частности, их может нанять на работу якобы международная компания, разместившая на интернет-сайтах объявления о трудоустройстве. С такими работниками даже заключается трудовой договор.

Но в случае их задержания сотрудниками правоохранительных органов при передаче денег те ничего вразумительного о своих работодателях сказать не могут. Договор, впрочем, как и все указанные, в нем реквизиты, оказывается, безусловно, фальшивым. Преступник или, зачастую, организованная преступная группа не ищут «дропа», их поставкой занимается «дроповод» — лицо, на которое замкнуты все «работники» организации. Естественно, каждому в этой криминальной цепочке приходится платить, но «безопасность» в этом случае стоит того. Что же касается украденных адресов электронной почты путем сканирования операционной системы, то их можно потом продать на «черном» рынке за немалые деньги тем же «спамерам», использующим эти данные в социальных сетях Интернета в своих рассылках.

Другой представляющий оперативный интерес криминальный промысел — учетные записи онлайн-игр, которые приобретают все большую популярность. В процессе таких игр многие пользователи «покупают» себе с помощью электронных денег виртуальное оружие, заклинания, всевозможную защиту и другие атрибуты.

Отмечены случаи, когда виртуальные ресурсы продаются за тысячи вполне реальных долларов. И все эти богатства злоумышленники, получив их абсолютно бесплатно путем взлома данных учетных записей, могут продать желающим по очень низким ценам, чем и объясняется рост популярности вредоносных программ, занимающихся кражей игровой виртуальной собственности. В настоящее время количество модификаций таких вредоносных программ, ворующих пароли от известных игр, может достигать 1500.

Один из наиболее распространенных способов обогащения в сфере Интернет считается злоупотребление доверием. Любой бизнес, расширяясь, постоянно ищет новые области своего применения. Не является исключением в данном случае и киберкриминал. Через сети Интернета продается все больше товаров и предлагается такое же количество услуг, постоянно появляются новые. Преступность оперативно внедряет в них мошеннические схемы из реального мира. Задача мошенника склонить «клиента» к добровольной сделке, и для этого в подавляющем большинстве случаев используется фиктивное занижение цен. Как правило, в таких схемах для привлечения покупателей ставка делается на значительно более низкие цены по сравнению с существующими на потребительском рынке. Вся аргументация таких цен в подобных интернет-магазинах весьма и весьма сомнительна. Но многие «покупатели» верят этим аргументам: «А почему бы им не продавать товар дешево, если он достался бесплатно!».

Так, например, один из интернет-магазинов на своем сайте предлагал ноутбуки по приемлемой цене, обосновывая это следующими положениями (см. рис. 3):

- продажа конфиската (таможенный конфискат);

- продажа товаров, купленных по украденным ранее кредитным картам;

- продажа товара, купленного в кредит через подставных лиц.

При заказе товара «клиента» просят внести предоплату, а иногда и заплатить стоимость товара полностью, после чего телефоны или адреса преступников перестают отвечать, а деньги, безусловно, никто не возвращает.

При этом способы обмана покупателя разнообразны. Например, широко распространена доставка купленного в интернет-магазинах товара с помощью курьеров. В этом случае мошенники могут требовать предоплату только за доставку, аргументируя свое требование тем, что курьер часто приходит по адресу, где никто ничего не заказывал и затраты на курьера приходится покрывать интернет-магазину. В этом случае покупатель оплачивает затраты за доставку, а товар, естественно, не доставляется.

Такие интернет-магазины это далеко не единственные ловушки для обманутых пользователей, в сфере компьютерной информации находят свою вторую жизнь практически все криминальные идеи из реального мира. В качестве очередного примера можно рассмотреть еще один из «проектов» мошенников, когда

«клиенту» предлагают вложить определенную сумму денег под очень привлекательный процент (см. рис. 4). Комментарии, как говорится, здесь излишни. В один момент люди, доверяющие таким «инвестиционным» сайтам, превращаются из «инвесторов» в обманутых вкладчиков. Способов мошенничества и здесь предостаточно: постоянно обнаруживаются ложные обменные сайты для электронных денег, клиенты которых также лишаются своих средств, периодически появляются интернет-пирамиды (аналог сетевого маркетинга из реального мира), рассылается «спам» о существовании секретных специализированных электронных кошельков, которые удваивают или утраивают полученные суммы и т.д.

Как мы уже сказали ранее, все подобные мошеннические схемы используют психологию, менталитет населения, склонного к легкой наживе.

С середины 2006 года в России появились новые вирусные технологии, направленные на вымогательство денег пользователей сети Интернет.

Так, вредоносная программа Trojan. Win32. Krotten модифицировала реестр компьютера пользователя таким образом, что нормальная работа системы становилась невозможной. Появляющийся периодически «информер» выдвигал требование о переводе некоему владельцу сайта через СМС-сообщение определенной суммы денег за пользование ресурсами сети, взамен в сообщении гарантировалось восстановление работоспособности компьютера.

Некоторые пользователи компьютеров, обладая достаточной квалификацией, восстанавливали исходное рабочее состояние системы самостоятельно, другие — переустанавливали операционную систему, что в конечном итоге позволяло избавиться от этой вредоносной программы. Однако основная масса пользователей склонялась в пользу «платить», обосновывая свое решение экономией времени или средств либо по морально-этическими соображениям, так как выскакивающий постоянно баннер носил преимущественно эротический характер.

В результате после нескольких «неудачных» попыток ввода предлагаемого мошенниками пароля пользователь приходил к правильному выводу — это обман и нужна квалифицированная помощь, но его деньги уходили безвозвратно.

Рис. 4 - Вклады под высокие проценты

Распространялся Trojan. Win32. Krotten в чатах, на форумах под видом программ, позволяющих получать бесплатную IP-телефонию, бесплатный доступ к сети Интернет, к сотовым коммуникациям и т. д.

Достаточно было только «кликнуть» мышкой на появляющийся рекламный баннер, и пользователь становился очередным «владельцем» вредоносной программы.

Рыночная экономика инициирует появление все новых и новых методов, форм, способов криминального обогащения в сфере компьютерной информации, а наша психология (менталитет) и другие факторы определяют вектор его развития. Почему же в интернет-сфере такие преступления как вымогательство, мошенничество, кража и другие популярны среди лиц, их совершающих? Ответ на этот вопрос банально прост: в надежде восстановить утерянные или испорченные данные пользователи компьютеров, зачастую и сами склонные к противоправным действиям, возможным благодаря пробелам в законодательстве, нередко согласны выполнить любые условия «доброжелателей» или немного отступить от требований закона. Предрасположенность определенного контингента лиц к добровольной передаче данных и нарушению законов, халатность в работе на компьютерах, характерные для части населения, зачастую являются инициирующими факторами преступного обогащения и осложняют процесс привлечения к уголовной ответственности злоумышленников.

2.2 Технология совершения компьютерных преступлений в социальных сетях

В современном мире достижения научного и технического прогресса оказывают воздействие на все явления общественной жизни. Не исключение и преступность. Одна из наиболее опасных тенденций — проникновение криминальных угроз в информационно-телекоммуникационную среду, в том числе и в сеть Интернет. В западной литературе актуальность проблемы понимания, оценки преступности в сфере информационных технологий и противодействия ей признавалась более 15 лет назад [1, p. 27].

Все общественно опасные деяния, совершаемые при помощи информационно-телекоммуникационных технологий, условно можно разделить на две группы: деяния, связанные с взаимодействием человека и техники (например, хищения,

совершаемые при помощи программных и аппаратных средств), и деяния, связанные с организованным при помощи технических средств взаимодействием человека с человеком (группой людей). Именно вторая группа преступлений представляет наибольшую угрозу для криминологической безопасности личности, общества и государства и называется преступностью в социальных сетях Интернета. Говоря о тенденциях преступности в сфере информационных технологий, исследователи отмечают, что, во-первых, появляются новые преступления, такие как нарушение целостности, доступности и конфиденциальности электронных данных, объектом которых выступают охраняемые законом новые интересы, возникшие в связи с развитием информационных технологий. Во-вторых, глобальные информационные сети используются для совершения деяний, ответственность за которые уже предусмотрена уголовным законодательством многих государств. Это такие деяния, как хищение имущества, распространение детской порнографии, нарушение тайны частной жизни и др. [2, p. 18].

При этом совершение преступления в сети Интернет не требует больших усилий и затрат — достаточно иметь компьютер, программное обеспечение и подключение к информационной сети. В настоящее время не нужно даже глубоких технических познаний: в Интернете существуют специальные форумы, на которых можно приобрести программное обеспечение для совершения преступлений, украденные номера кредитных карт и идентификационные данные пользователей, а также найти услуги по помощи в совершении электронных хищений и атак на компьютерные системы как в целом, так и на отдельных стадиях совершения преступлений [3, с. 87].

Помимо того, при изучении вопросов информационного взаимодействия двух социальных субъектов следует помнить о трех уровнях коммуникации: межличностном (человек — человек), контакт-коммуникационном (человек — группа) и масс-коммуникационном (человек — общество). К.Д. Рыдченко справедливо отметил, что специфика каждого уровня должна учитываться при квалификации деяния и назначении наказания [4, с. 166].

Социальное взаимодействие в телекоммуникационных сетях во многом подвержено тем же закономерностям, что и взаимодействие реальное. Криминальная психология основой такого взаимодействия, в том числе носящего преступный характер, считает принцип детерминизма, который выявляет соотношение внешних (прежде всего, социальных) и внутренних (психических) факторов и условий, оказывающих влияние на взаимодействующих субъектов, в их

причинной взаимосвязи [5, с. 126]. Однако взаимодействие индивидов происходит в новых, недостаточно исследованных криминологией условиях информационного пространства социальных сетей, что накладывает отпечаток на характер преступности [6, p. 407].

Социальная сеть понимается как часть информационного пространства сети Интернет (совокупность веб-сайтов, платформ, онлайн-сервисов), в которой возможна организация социального взаимодействия. Такое понимание способствует тому, что объектами исследования становятся не только «традиционные» социальные сети («ВКонтакте», «Одноклассники»), но и такие сервисы, как ICQ, Skype и др. Подобный подход является достаточно широким, его придерживаются ряд исследователей, в том числе зарубежных [7, p. 220].

Масштабы криминальных проявлений в социальных сетях Интернета сложно оценить. Объективному анализу исследуемого вида преступности не способствует как несовершенство статистической отчетности правоохранительных органов (в первую очередь отчета о преступлениях, совершенных в сфере телекоммуникаций и компьютерной информации, ГИАЦ МВД России — форма 1-ВТ) [8, с. 123], так и трудности в выявлении, расследовании и раскрытии преступлений, совершаемых с использованием информационно-технологических средств.

Учеными отмечается, что в целом возможности исследования статистических показателей в данной сфере крайне ограниченны в связи со сложностью получения достоверных сведений и их запаздыванием по сравнению с интенсивностью развития технологий. В то же время не приходится ждать устойчивой фазы, в которой изучаемые показатели были бы стабильными, а значит, рассматривать соответствующие явления необходимо в динамике [9, с. 11].

Основой исследования явился поиск упоминаний названий социальных сетей в текстах приговоров, опубликованных в сети Интернет, а при отсутствии таких названий — описания совершения преступлений при помощи социальных сетей.

Всего в ходе исследования было проанализировано содержание 300 обвинительных приговоров судов первой инстанции, вынесенных в период с 2008 по 2014 г. на территории России, размещенных на интернет-сайте rospravosudie.com, в которых получила отражение квалификация 331 преступления, совершенного с использованием социальных сетей. При этом описание в одном приговоре совершения нескольких одинаковых преступлений не бралось в расчет при определении совокупности (например, описание в приговоре

четырех фактов сбыта наркотических средств считалось за одно преступление, в то время как описание факта контрабанды и факта сбыта считалось за два преступления).

Использование с целью анализа судебной практики именно интернет-сайта rospravosudie.com обусловлено тем, что это позволило применять для изучения приговоров возможности поискового механизма сайта. Для получения искомых приговоров были сформированы следующие запросы: «вконтакте», «vk», «vkontakte», «v kontakte», «в контакте», «одноклассники. ру», «odnoklassniki», «facebook», «фейсбук», «livejournal», «Мой Мир», «твиттер», «twitter», «социальная сеть». Такой выбор формулировок поисковых запросов обусловлен тем, что на сегодняшний день активными пользователями трех самых массовых российских сетей («ВКон- такте», «Одноклассники», «Мой Мир@Mail.ru») являются более 120 млн чел. [10, с. 5]. При поиске приговоров возникла следующая сложность: различные суды в приговорах по-разному обозначают одни и те же социальные сети. Некоторые суды ограничиваются указанием в приговоре на то, что преступление было совершено в социальной сети, интернет-сети, сети Интернет, информационно-телекоммуникационной сети. Такие приговоры анализировались, и если устанавливалось, что совершению преступления способствовало именно социальное взаимодействие внутри сети, то такие судебные решения включались в исследование. В ряде случаев название социальной сети исключалось из приговоров при их опубликовании в сети Интернет.

Основной криминологический показатель, который позволило выявить исследование,— это структура преступности, связанной с использованием социальных сетей в криминальных целях.

Наибольшую долю преступлений, совершаемых в социальных сетях, составляют общественно опасные деяния, связанные с незаконным оборотом наркотических средств и психотропных веществ (24,5 %). В основном это незаконные приобретение (43,2 % от числа наркопреступлений) и сбыт (53,1 %) наркотиков, совершенные при помощи социальных сетей. Также встречаются приговоры, в которых фигурирует пересылка и контрабанда наркотических средств.

Среди веществ, являющихся предметом незаконных действий, наибольшую часть составляют спайс (синтетический каннабиноид группы JWH) — 40 % от числа приговоров, в которых указано вещество, являющееся предметом незаконного оборота, амфетамин и его производные — 18,7 %, марихуана — 14,7 %, гашиш и гашишное масло, героин, наркотические средства эфедриновой группы — по 6,7 %.

Оставшиеся 6,5 % приходятся на различные синтетические стимуляторы.

Основными способами осуществления незаконных операций по приобретению или сбыту наркотиков являются «закладки» (оплата покупателем наркотического средства при помощи электронных платежных систем с последующим сообщением ему места, где расположен тайник с наркотиком) — 44,1 %, а также заранее обговоренные личные встречи между продавцом и покупателем — 40,3 %. Кроме указанных способов, незаконные операции с наркотиками осуществляются посредством почтовых отправлений, путем передачи посылки через водителей общественного транспорта, не осведомленных о ее содержимом, незаконного проноса наркотических средств в исправительные учреждения. Сотрудники УФСКН России отмечают, что использование электронных платежных систем Webmoney, «Яндекс. Деньги» существенно затрудняет возможность выявления наркопреступлений, не позволяет проследить связь между поставщиком и потребителями наркотиков. Криминальную сделку могут совершить лица, которые лично не знакомы и не обладают информацией друг о друге, находятся не только в разных регионах, но и в разных государствах, где действует различное законодательство [11, с. 47].

Наиболее часто для незаконных операций с наркотиками использовалась социальная сеть «ВКонтакте» — 81 % от числа приговоров, в которых указано название сети.

Использование социальных сетей для осуществления незаконных действий с наркотическими средствами чаще всего наблюдалось в Свердловской, Новосибирской, Самарской, Вологодской областях, а также в Москве.

Вторую по величине группу общественно опасных деяний, совершаемых при помощи социальных сетей, составляют преступные посягательства на собственность (18,4 %). В их структуре наибольшая доля принадлежит мошенническим действиям (70,5 %). Помимо мошенничества, при помощи социальных сетей совершаются кражи, присвоения, грабежи, разбои, причинение имущественного ущерба собственнику путем обмана при отсутствии признаков хищения, а также умышленное повреждение чужого имущества.

Использование социальных сетей для совершения тайного хищения чужого имущества в основном заключается в знакомстве преступника и жертвы с последующим приглашением жертвой преступника к себе домой, откуда похищаются деньги и ценности.

Исследуя проблемы противодействия мошенничеству, ученые приходят к выводу о том, что появление в УК РФ ст. 159^6 породило массу проблем в квалификации деяний, поскольку возникла конкуренция уголовно-правовых норм [12, с. 196].

Зарубежные авторы делят интернет-мошенничество на два вида — мошенничество в финансовой (маркетинговой) и нефинансовой сферах [13, p. 665]. При этом почти половина случаев мошенничества (46,8 %) приходится на фродинг (несанкционированное списание денежных средств с карты), т.е. мошеннические действия осуществляются без непосредственного социального взаимодействия между преступником и жертвой [14, с. 137].

Большинство мошеннических действий, совершенных посредством взаимодействия преступника и жертвы, осуществлено при помощи размещения преступником объявлений в социальных сетях о продаже товаров и оказании услуг (60,5 %). В литературе эта разновидность мошеннических схем именуется виртуальным товарообменом [15, с. 32]. Также мошеннические действия осуществляются в ответ на объявления, размещенные потерпевшим (11,6 %).

К числу иных способов мошенничества, реализуемых преступниками в ходе знакомства с потерпевшими при помощи социальных сетей, относятся следующие:

- виновный обманным путем получил пароль от кошелька букмекерской конторы под предлогом коллективной ставки, после чего похитил с него деньги;
- мошенница предложила сожительнице подозреваемого в сбыте наркотиков заплатить за изменение свидетельских показаний;
- преступник завладел сотовым телефоном путем обмана под предлогом его продажи по завышенной стоимости;
- виновный сообщил недостоверные сведения об организации работы автошколы, после чего похитил предоплату за занятия, внесенную потерпевшим;
- мошенник представился «менеджером международного класса» и под видом привлечения денежных средств для развития предпринимательской деятельности и для организации фармацевтического бизнеса похитил их;
- виновный узнал о желании потерпевшей ускорить процедуру оформления заграничных паспортов, после чего предложил ей свою помощь за денежное вознаграждение;
- преступник познакомился в социальной сети с девушкой и несколько раз брал деньги в долг без намерения отдать их;

- мошенник познакомился с девушкой и убедил ее оформить на себя автокредит, пояснив, что будет сам погашать его;
- виновная предложила ранее незнакомому лицу через социальную сеть увеличить капитал, пояснив, что в банке работает ее знакомый сотрудник, который сможет увеличить денежные средства в несколько раз, после чего похитила деньги;
- мошенница познакомилась с мужчиной в социальной сети при помощи созданной на вымышленное лицо страницы, после чего сообщила ему о финансовых трудностях и попросила прислать деньги, чтобы приехать к нему;
- в двух случаях преступники предлагали помочь за денежное вознаграждение сдать экзамены на получение водительского удостоверения.

Интерес представляет содержание публикуемых мошенниками объявлений о продаже товаров и оказании услуг, благодаря которым они похищают денежные средства потерпевших. Мошенники публикуют объявления о продаже смартфонов, компьютерной и другой электронной техники (26,9 % случаев мошенничества с публикацией объявления), одежды, обуви, сумок (26,9 %), авиабилетов по низким ценам (7,7 %), о сдаче квартиры в аренду (7,7 %). В остальных случаях преступники похищали деньги под предлогом продажи музыкального оборудования, масок Гая Фокса, автомобильных колес, военного билета, установки заборов, ворот и калиток. Кроме того, деньги похищались под видом взимания страхового взноса за оформление кредита под низкий процент, а также в ходе предложения посреднических услуг при оформлении банковской карты. В одном из решений используется обобщенная формулировка «несуществующая продукция»[1].

В ходе мошенничества в ответ на объявления, размещенные потерпевшими, преступники предлагали приобрести щенка, курительные смеси, водительское удостоверение, требовали вознаграждение за возвращение якобы найденных документов.

Для совершения грабежей и разбоев социальные сети в большинстве случаев использовались следующим образом: преступники размещали объявления (о продаже военных билетов, сотовых телефонов, об оказании услуг сексуального характера), договаривались с жертвами о встречах, в ходе которых открыто похищали денежные средства и иное имущество.

Вымогательство, совершаемое при помощи социальных сетей, в большинстве случаев связано с угрозой распространения позорящих потерпевшего сведений. В ряде случаев такие действия сопровождаются неправомерным доступом к

компьютерной информации, нарушением тайны переписки и дополнительно квалифицируются по ст. 272 и 138 УК РФ. В связи со случаями вымогательства в сети Интернет актуальными становятся такие проблемы, как определение предмета виртуального вымогательства, его способы, реальность ущерба и др. [16, с. 150].

Анализ приговоров, в которых указана социальная сеть, через которую осуществлялись преступные посягательства на собственность, свидетельствует о том, что преступники в основном использовали социальную сеть «ВКонтак- те» (эта сеть отмечена в 74,3 % приговоров).

Наибольшее количество посягательств на собственность при помощи социальных сетей было совершено в Москве и Московской области, а также в Мурманской области.

Третью группу общественно опасных деяний, совершаемых при помощи социальных сетей, составляют преступления, связанные с экстремистской и террористической деятельностью (10,9 %). В криминологических исследованиях указывается на опасность распространения таких материалов в сетевой среде, поскольку они способны оказать негативное влияние на несовершеннолетних пользователей, сделать экстремистские взгляды нормой жизни [17, с. 38]. Экстремистские организации и их представители под видом осуществления социально значимой деятельности используют активность студенческой молодежи в своих преступных целях [18, с. 123]. Кроме того, современные экстремистские организации разбиты на незначительные по численности ячейки (от 5 до 7 чел.), которые связаны между собой и координируются через социальные сети [19, с. 33].

В указанной группе преступлений наибольшую долю составляют деяния, связанные с распространением экстремистских материалов в социальных сетях, квалифицируемые по ст. 282 УК РФ «Возбуждение ненависти либо вражды, а равно унижение человеческого достоинства» (80,6 %).

Объектами экстремистских проявлений (согласно формулировкам, приводимым в приговорах) выступают нерусские — 25,6 % от числа приговоров, в которых указан объект экстремистских проявлений, представители Кавказа и евреи — по 16,3 %, русские и выходцы из Средней Азии — по 11,6 %. Также в качестве объектов экстремизма в приговорах фигурируют таджики, немусульмане, гастарбайтеры, дагестанцы, чеченцы, грузины, турки, азербайджанцы.

Большая часть экстремистской информации представлена в форме видеофрагментов (51,2 %). Кроме того, экстремистская информация представлена в виде текста (30,8 %), графических изображений (10,3 %), аудиофайлов (7,7 %).

Зафиксированы случаи организации при помощи социальных сетей мероприятий экстремистского характера в форме массовых шествий и расклеивания листовок.

В приговорах описаны два случая использования социальных сетей для осуществления террористической деятельности.

В первом случае виновный решил создать на территории Республики Дагестан незаконное вооруженное формирование для осуществления джихада, т.е. для ведения вооруженной борьбы против подразделений Вооруженных сил и правоохранительных органов Российской Федерации с целью установления верховенства законов шариата на территории Северного Кавказа.

Во исполнение преступного замысла он занимался поиском соучастников преступления среди пользователей социальной сети «Одноклассники», а также искал возможности незаконного приобретения оружия и боеприпасов для вооружения незаконного формирования, которое он намеревался создать. Деяние было квалифицировано как приготовление к созданию вооруженного формирования, не предусмотренного федеральным законом (ч. 1 ст. 30, ч. 1 ст. 208 УК РФ), в совокупности с публичными призывами к осуществлению террористической деятельности (ч. 2 ст. 205[2] УК РФ)[2].

Во втором случае к ответственности привлечена виновная, которая, имея религиозные убеждения, связанные с пропагандой идеологии терроризма, ознакомилась со статьей, содержащей информацию, призывающую к осуществлению террористической деятельности, обосновывающую и оправдывающую ее необходимость. Преследуя цель ознакомления с текстом данной статьи неопределенного круга лиц, желая распространить идеологию терроризма, имея умысел на публичные призывы к осуществлению террористической деятельности и публичное оправдание терроризма, она разместила текст статьи на своей личной странице в социальной сети. Опасность использования информационно-телекоммуникационных сетей для координации действий террористов подчеркивается и в зарубежных исследованиях [20, p. 283].

Для экстремистской и террористической деятельности в подавляющем большинстве случаев используется социальная сеть «ВКонтакте» (95,8 % от числа приговоров, где указана социальная сеть, при помощи которой осуществлялась

экстремистская деятельность).

В территориальном аспекте описываемый вид криминального использования социальных сетей распространен достаточно равномерно. Приговоры выносились на территории Курской, Тюменской, Волгоградской, Архангельской,

Свердловской, Новосибирской областей, Республики Башкортостан и других регионов.

Преступления, связанные с незаконным распространением порнографических материалов, составляют 10,3 % от числа общественно опасных деяний, совершаемых при помощи социальных сетей. Среди распространяемых материалов примерно равные доли образуют порнография с изображением взрослых лиц (55,9 %) и порнография, изображающая несовершеннолетних (44,1 %). Об опасности таких явлений свидетельствуют данные исследователей, согласно которым в сети Интернет насчитывается около 260 млн страниц порнографического содержания и 40 тыс. порнографических сайтов с изображениями несовершеннолетних; более 40 % несовершеннолетних пользователей уже сталкивались со случаями онлайновых обращений к ним взрослых лиц, просивших о личной встрече или виртуальном общении с помощью установленной на компьютере веб-камеры [21, с. 191].

Практически во всех случаях использование социальной сети выражалось в том, что виновный публиковал порнографические видеоматериалы у себя на странице. Наибольшее количество приговоров, касающихся распространения порнографических материалов в социальных сетях, было вынесено в Пензенской и Новгородской областях, Республике Коми.

Следующей по величине группой преступлений, совершаемых при помощи социальных сетей, являются общественно опасные деяния, направленные против конституционных прав и свобод человека и гражданина (9,1 %). В их структуре выделяются такие преступления, как нарушение неприкосновенности частной жизни (40,0 %), нарушение авторских и смежных прав (33,3 %), нарушение тайны переписки (20,0 %), незаконный оборот специальных технических средств, предназначенных для негласного получения информации (6,7 %).

Большинство преступлений, квалифицированных по ст. 137 УК РФ «Нарушение неприкосновенности частной жизни», связано с распространением в социальной сети информации о частной жизни лица, по тем или иным причинам, но на законных основаниях ставшей известной виновному. Чаще всего на почве личных неприязненных отношений размещались фотографии и видеофрагменты

интимного содержания. В двух случаях для получения сведений о частной жизни лица виновный применял вредоносное программное обеспечение, поэтому деяние квалифицировалось по совокупности со ст. 273 УК РФ «Создание, использование и распространение вредоносных компьютерных программ».

Во всех приговорах, связанных с нарушением тайны переписки, содержится указание на то, что виновный при помощи вредоносных компьютерных программ незаконно получал доступ к личной странице потерпевшего в социальной сети. При этом в пяти приговорах деяние было квалифицировано по совокупности со ст. 273 УК РФ, еще в одном приговоре по неизвестным причинам такая квалификация отсутствовала.

Совершая преступления, связанные с незаконным оборотом специальных технических средств, предназначенных для негласного получения информации, виновные использовали социальную сеть либо для заказа, либо для последующего сбыта таких средств.

В 60 % приговоров, связанных с нарушением авторских прав, зафиксировано, что преступники размещали на страницах в социальных сетях объявления с предложением услуг по настройке и обслуживанию компьютера, установке программного обеспечения. После этого они устанавливали программы и при помощи вредоносного программного обеспечения модифицировали их, нейтрализуя систему защиты и делая программы работоспособными.

В 40 % таких приговоров отмечено, что виновные при помощи социальных сетей заказывали контрафактные экземпляры аудиовизуальных произведений (видеофильмов) либо программных продуктов (игр) для последующего их сбыта через розничную торговую сеть.

Для совершения преступлений против конституционных прав и свобод человека и гражданина в 76,2 % случаев использовалась социальная сеть «ВКонтакте», в 14,3 % — «Одноклассники», в 9,5 % — «Мой Мир@Mail.ru».

Наибольшее количество приговоров по указанным преступлениям вынесено в Вологодской и Кировской областях.

Преступления в сфере компьютерной информации составляют 7,9 % от общего количества общественно опасных деяний, совершаемых при помощи социальных сетей. Основная часть таких преступлений — неправомерный доступ к компьютерной информации (80,8 %). Помимо этого, в приговорах указаны факты

создания, использования и распространения вредоносных компьютерных программ. В большинстве случаев преступники блокировали доступ законных пользователей к их аккаунтам в социальных сетях, изменяли логин и пароль, модифицировали содержащуюся на страницах информацию. Для совершения преступлений в сфере компьютерной информации в 47,6 % случаев использовалась социальная сеть «ВКонтакте», в 28,6 % — «Мой Мир@Mail.ru», в 23,8 % — «Одноклассники». Наибольшее распространение такого рода деяния получили в Чувашской Республике, Тамбовской, Архангельской и Кировской областях.

Седьмой по распространенности в социальных сетях является группа преступлений, связанных с незаконным оборотом сильнодействующих веществ[3] (6,6 %).

В 82 % случаев при помощи социальных сетей распространяются анаболические стероиды и иные сильнодействующие вещества, используемые при спортивных тренировках для увеличения мышечной массы и улучшения спортивных показателей (метандиенон, метилтестостерон, дегидрохлорметилтестостерон, станозолол, тренболон, эфиры тестостерона и другие сильнодействующие вещества). В остальных ситуациях распространялись средства для похудения, содержащие в своем составе сибутрамин.

В 60 % приговоров зафиксировано, что виновные создавали рекламные страницы или группы, занимались массовой рассылкой сообщений с предложением приобрести сильнодействующие вещества.

В 36 % случаев незаконный оборот сильнодействующих веществ в целях сбыта сопровождался контрабандой таких веществ. Вопросы вызывает позиция судов в отношении квалификации преступлений, связанных с перемещением сильнодействующих веществ через государственную границу Российской Федерации. Из восьми приговоров, в которых содержалось упоминание о незаконном перемещении сильнодействующих веществ на территорию России,

[3] Об утверждении списков сильнодействующих и ядовитых веществ для целей статьи 234 и других статей Уголовного кодекса Российской Федерации, а также крупного размера сильнодействующих веществ для целей статьи 234 Уголовного кодекса Российской Федерации : постановление Правительства РФ от 29 дек. 2007 г. № 964 : (в ред. от 7 нояб. 2013 г.) // Собрание законодательства Российской Федерации. 2008. № 2. Ст. 89.

в двух приговорах получатель вещества на территории России был признан подстрекателем к контрабанде сильнодействующих веществ, еще в двух приговорах — исполнителем, в одном — организатором, в одном — пособником. В двух приговорах факт незаконного перемещения сильнодействующих веществ на территорию России попросту игнорировался. При этом деяния, описанные в приговорах, практически не отличались друг от друга.

В качестве примеров можно привести формулировки из соответствующих приговоров.

Квалифицируя действия получателей сильнодействующих веществ как подстрекателей к контрабанде, суд приводит следующие аргументы: «Б., имея преступный умысел, направленный на совершение незаконного перемещения через Государственную границу Российской Федерации сильнодействующих веществ, осознавая степень и характер общественной опасности своих действий, через информационно- телекоммуникационную сеть Интернет на сайте www.vk.com у не установленного следствием лица, являющегося пользователем данного сайта, незаконно заказал сильнодействующие вещества, оплатив заказ, тем самым склонил неустановленное лицо к совершению преступления, а именно осуществить незаконную пересылку через Государственную границу Российской Федерации, то есть совершить контрабанду сильнодействующих веществ. А неустановленное лицо, в свою очередь, переслало почтовым отправлением Б. через Государственную границу Российской Федерации сильнодействующие вещества»[3].

Квалификация действий виновного в качестве исполнителя в одном из приговоров сомнений не вызывает, поскольку он самостоятельно посредством железнодорожного транспорта перевез сильнодействующие вещества через государственную границу Российской Федерации. В другом же случае деяние лица квалифицировано по ст. 226^1 УК РФ без ссылки на ст. 33 УК РФ. При этом в приговоре указано, что виновный договорился о приобретении сильнодействующих веществ (анаболических стероидов) за пределами России, оплатил их путем электронного денежного перевода, после чего получил посылку. Очевидно, что самостоятельно вещества через государственную границу он не перемещал. Более того, в приговоре указано, что «суд не находит оснований к признанию в качестве отягчающего обстоятельства признака совершения преступления в составе группы лиц по предварительному сговору ввиду совершения указанных действий одним подсудимым».

Квалифицируя действия получателя сильнодействующего вещества как организатора контрабанды, суд указывает, что «И. организовал совершение преступлений, так как лично совершил активные и целенаправленные действия, целью которых было совершение преступления в форме исполнительства иным лицом на территории Республики Беларусь, — вступил в переписку с неустановленным лицом на территории Республики Беларусь в целях дальнейшего приобретения на территории РФ сильнодействующих веществ, оплатил сильнодействующие вещества и их доставку (включая незаконное перемещение через Государственную границу РФ в почтовых отправлениях) на территорию РФ, осознавая при этом, что сильнодействующие вещества будут сокрыты от пограничного контроля в международных почтовых отправлениях».

Практически аналогичные аргументы приводит суд, квалифицируя действия получателя сильнодействующего вещества в качестве пособника. В приговоре указано, что «суд приходит к выводу, что действия Я. следует квалифицировать по ч. 5 ст. 33 УК РФ как пособничество в совершении вышеуказанных преступлений, поскольку Я. не являлся организатором, инициатором данных преступлений, а всего лишь содействовал его совершению. В частности, предоставил информацию для совершения данных преступлений лицу под псевдонимом «Стероид Тренович», уголовное дело в отношении которого выделено в отдельное производство, указав свои анкетные данные и почтовый адрес, поддержав, таким образом, решимость вышеуказанного лица совершить данные преступления».

Наконец, еще в двух случаях в приговорах указано, что сильнодействующие вещества были незаконно перемещены через государственную границу России, однако по каким-то неизвестным причинам это обстоятельство не получило соответствующей правовой оценки. В одном случае в ходе судебного заседания государственный обвинитель отказался от поддержки обвинения по ст. 226^1 УК РФ.

Очевидно, что действия получателей сильнодействующих веществ, заказавших их с территории другого государства, должны иметь одинаковую квалификацию. Исходя из смысла уголовного закона действия лица должны быть квалифицированы как подстрекательство к совершению контрабанды сильнодействующих веществ.

Практически три четверти подобных преступлений было совершено с использованием социальной сети «ВКонтакте». К регионам, где подобные преступления получили наибольшее распространение, относятся Красноярский край, Псковская, Владимирская, Кировская, Нижегородская области.

Еще одной группой преступлений, совершению которых способствуют социальные сети, являются насильственные общественно опасные деяния, направленные против жизни и здоровья личности (5,4 %). Практически во всех приговорах описаны ситуации, когда общение в социальных сетях приводило к тому, что между преступником и потерпевшим возникали неприязненные отношения, они договаривались о встрече, в ходе которой причинялся тот или иной вред здоровью. Больше всего таких фактов было зафиксировано в Московской и Волгоградской областях, Республике Башкортостан.

Помимо перечисленных преступлений, в приговорах встречается описание совершения при помощи социальных сетей других общественно опасных деяний, каждое из которых представлено в общей структуре в виде единичных случаев, однако вместе они составляют 6,9 % от числа преступлений, совершенных при помощи социальных сетей.

Среди деяний, квалифицированных по ч. 4 ст. 222 УК РФ как незаконный сбыт холодного оружия, в одном случае через страницу в социальной сети «ВКонтакте» осуществлялась реализация продукции с изображением нацистской атрибутики и холодного оружия — кастетов. Во втором случае преступник самостоятельно и незаконно изготовил кастет из свинца. После этого сфотографировал его на свой мобильный телефон, а затем разместил фотографию в социальной сети на своей странице. В обоих случаях кастеты были проданы.

Оказание услуг, не отвечающих требованиям безопасности жизни и здоровья потребителей, повлекших по неосторожности смерть человека (п. «в» ч. 2 ст. 238 УК РФ), происходило при следующих обстоятельствах: преступник в социальной сети создал страницу, разместил там свои контактные данные и информацию о предоставлении платных услуг по обучению полетам на параплане, а также по организации одноразовых платных полетов. При этом он знал, что не имеет на свой параплан никаких документов, подтверждающих безопасность полетов на нем.

На объявление откликнулась женщина и договорилась с ним об организации полета на параплане ее малолетнего сына. При оказании услуги преступник забыл пристегнуть пассажира к ремням безопасности подвесной системы, и через небольшой промежуток времени после старта, во время полета на высоте примерно 40 м от земли, малолетний сорвался с параплана, упал на землю и от полученных травм скончался на месте.

В следующей ситуации в социальной сети «ВКонтакте» было размещено объявление с предложением студентам одного из вузов помощи в сдаче экзаменов. Через страницу представители правоохранительных органов обратились к лицу, разместившему объявление, с просьбой оказать помощь в сдаче экзамена, зачета и курсового проекта за деньги у одного из преподавателей. После этого по телефону была названа стоимость услуги и оговорен порядок взаимодействия. В результате проведенных оперативно-розыскных мероприятий преподаватель и посредник были задержаны при получении взятки.

В приговорах отражены два случая организации совершения преступлений против общественного порядка при помощи социальных сетей. В одном из них описана организация акции по раскрашиванию вагонов электропоездов в стиле граффити. Деяние было квалифицировано по ст. 214 УК РФ «Вандализм».

В другом случае в одной из групп социальной сети было размещено приглашение участвовать в нападении на автобус с болельщиками футбольного клуба «Зенит», которое планировалось совершить по пути следования автобуса по трассе. Участники акции в количестве 30 чел. на шести автомашинах стали преследовать автобус. Находясь на участке трассы, водители машин начали блокировать автобус, вынуждая его прекратить движение, бросая по корпусу автобуса камни и металлические предметы, в результате чего водителю автобуса пришлось остановиться. Сразу же после остановки автобуса участники акции стали бросать по его корпусу и стеклам камни и металлические предметы, разбив при этом три стекла, а также пытались проникнуть в салон автобуса. Преступление квалифицировано по ч. 2 ст. 213 УК РФ «Хулиганство» и ч. 2 ст. 167 УК РФ «Умышленные уничтожение или повреждение имущества».

При совершении преступлений против военной службы в отношении военнослужащих совершались оскорбительные действия, которые снимались на камеру мобильного телефона и впоследствии размещались в социальной сети «ВКонтакте».

В одном из приговоров по ст. 241 УК РФ «Организация занятия проституцией» преступник был признан виновным в организации интим- салона, деятельность которого была направлена на оказание услуг сексуального характера. Он систематически подбирал и нанимал проституток для оказания клиентам услуг сексуального характера за материальное вознаграждение, размещая объявления в социальных сетях.

Преступления против свободы, чести и достоинства личности представлены тремя деяниями, квалифицированными по ст. 128^1 УК РФ «Клевета». Во всех случаях преступники на почве личных неприязненных отношений размещали в социальных сетях заведомо ложную информацию, порочащую честь и достоинство другого лица. Во всех случаях потерпевшими выступали девушки, с которыми у преступников ранее были близкие отношения.

От имени потерпевших создавались страницы в социальных сетях, где размещалась заведомо ложная информация об интимных предпочтениях потерпевших, в том числе об оказании ими коммерческих сексуальных услуг. Для написания сообщений от имени потерпевших использовалась ненормативная лексика. В одном случае на странице была размещена фотоиллюстрация порнографического характера с изображением девушки, внешне похожей на потерпевшую, и подпись под фото «Интим звони» с номером телефона. При этом суд, несмотря на указание в приговоре на порнографический характер изображения, дополнительно не квалифицировал действия лица по ст. 242

УК РФ. В подобных случаях на стадии предварительного расследования и судебного разбирательства представляется обоснованным решение вопроса об отнесении материалов к порнографическим.

В каждом из случаев, помимо заведомо ложной информации, порочащей честь и достоинство потерпевших, распространялась информация, составляющая личную тайну граждан, в частности фотографии, сведения о фамилии, имени, месте рождения, семейном положении, месте учебы, номер телефона, домашний адрес (в том числе и город проживания). Однако лишь в одном случае в приговоре имелась дополнительная квалификация деяния по ст. 137 УК РФ.

В подобных случаях целесообразно рассматривать вопрос о дополнительной квалификации деяний по ст. 137 УК РФ. При этом необходимо выяснять, размещал ли потерпевший аналогичную информацию в открытом доступе, в том числе на своих страницах в социальных сетях, и каковы были настройки приватности, связанные с этой информацией. Если информация, размещенная потерпевшим, была доступна неопределенному кругу лиц, дополнительной квалификации по ст. 137 УК РФ не требуется.

Как покушение на торговлю малолетним ребенком было квалифицировано деяние беременной женщины, которая, увидев в социальной сети объявление о желании воспользоваться услугами суррогатной матери, направила автору объявления

сообщение о том, что она желает продать своего ребенка после рождения. В ходе сделки виновная была задержана сотрудниками правоохранительных органов.

Наконец, в приговорах было зафиксировано десять преступлений, связанных с нарушением порядка выдачи и оборота официальных документов. При помощи рекламных страниц и групп в социальных сетях осуществлялся сбыт листков нетрудоспособности, поддельных документов о высшем образовании, свидетельств о присвоении квалификации частного охранника, поддельных водительских удостоверений.

Социальные сети, используемые для совершения преступлений, указаны в 61,7 % приговоров. Наибольшее количество общественно опасных деяний совершено при помощи социальной сети «ВКонтакте» (80,9 % от числа приговоров, где указана социальная сеть, при помощи которой совершалось преступление). Кроме того, в приговорах упоминаются такие социальные сети, как «Одноклассники» (9,3 %), «Мой Мир@МзМ.ш» (4,1 %), ICQ (3,1 %), «Друг вокруг» (1,5 %), Skype (1,1 %).

Приговоры по делам о преступлениях, совершенных с использованием социальных сетей, были вынесены в 65 субъектах Российской Федерации. Наибольшее число таких приговоров вынесено в Самарской области (6,3 %), Москве (4,7 %), Пензенской (4,7 %), Московской (4,3 %), Новосибирской (4,3 %), Волгоградской (4,0 %), Свердловской (4,0 %), Вологодской (4,0 %) областях. На перечисленные восемь регионов приходится 36,3 % преступлений, поэтому можно говорить об относительно равномерном распределении исследуемого вида преступности по всей территории России.

Нельзя утверждать, что проведенное исследование отражает истинное состояние и структуру преступности в социальных сетях Интернета. Фактически описаны результаты работы правоохранительных органов по выявлению, раскрытию и расследованию таких преступлений. Однако и эти результаты могут служить основой для оценки тенденций преступности, для организации профилактической деятельности, в том числе виктимологической профилактики. В ряде случаев они позволяют обнаружить проблемы, связанные с юридической оценкой деяний, требующие дополнительной разработки и решения.

В качестве предложений по совершенствованию практики противодействия преступлениям, совершаемым в социальных сетях Интернета, можно указать следующее:

1. Для придания системности уголовному законодательству необходимо привести к единым формулировкам диспозиции и квалифицирующие признаки статей УК РФ, предусматривающих ответственность за преступления, которые возможно совершить с использованием информационно-телекоммуникационных сетей. Такой формулировкой является совершение преступления «с использованием средств массовой информации либо информационно- телекоммуникационных сетей (включая сеть Интернет)». При этом необходим постоянный криминологический мониторинг, направленный на выявление общественно опасных деяний, совершаемых при помощи информационно-телекоммуникационных сетей, для своевременной их криминализации или усиления уголовной ответственности.

2. Статистическая отчетность ГИАЦ МВД России (отчет о преступлениях, совершенных в сфере телекоммуникаций и компьютерной информации, — форма 1-ВТ) на сегодняшний день устарела. Она не учитывает массу актуальных криминальных угроз, таких как распространение экстремистских материалов в телекоммуникационной среде, использование компьютерных технологий для совершения преступлений против половой свободы и половой неприкосновенности несовершеннолетних, незаконного оборота наркотических средств и других противоправных деяний. В связи с этим статистическая форма должна быть скорректирована с учетом современных криминологических реалий киберпреступности.

ЗАКЛЮЧЕНИЕ

Изменения, происходящие в экономической жизни России – создание финансово-кредитной системы, предприятий различных форм собственности и т.п. – оказывают существенное влияние на вопросы защиты информации. Долгое время в нашей стране существовала только одна собственность – государственная, поэтому информация и секреты были тоже только государственные, которые охранялись мощными спецслужбами.

Проблемы информационной безопасности постоянно усугубляется процессами проникновения практически во все сферы деятельности общества технических средств обработки и передачи данных и прежде всего вычислительных систем. Это дает основание поставить проблему компьютерного права, одним из основных аспектов которой являются так называемые компьютерные посягательства. Об актуальности проблемы свидетельствует обширный перечень возможных способов

компьютерных преступлений.

В этом смысле компьютер может выступать и как предмет посягательств, и как инструмент. Если разделять два последних понятия, то термин компьютерное преступление как юридическая категория не имеет особого смысла. Если компьютер – только объект посягательства, то квалификация правонарушения может быть произведена по существующим нормам права. Если же – только инструмент, то достаточен только такой признак, как «применение технических средств». Возможно объединение указанных понятий, когда компьютер одновременно и инструмент и предмет. В частности, к этой ситуации относится факт хищения машинной информации. Если хищение информации связано с потерей материальных и финансовых ценностей, то этот факт можно квалифицировать как преступление. Также если с данным фактом связываются нарушения интересов национальной безопасности, авторства, то уголовная ответственность прямо предусмотрена в соответствии с законами РФ.

Каждый сбой работы компьютерной сети это не только «моральный» ущерб для работников предприятия и сетевых администраторов. По мере развития технологий платежей электронных, «безбумажного» документооборота и других, серьезный сбой локальных сетей может просто парализовать работу целых корпораций и банков, что приводит к ощутимым материальным потерям. Не случайно что защита данных в компьютерных сетях становится одной из самых острых проблем в современной информатике. На сегодняшний день сформулировано три базовых принципа информационной безопасности, которая должна обеспечивать:

– целостность данных – защиту от сбоев, ведущих к потере информации, а также неавторизованного создания или уничтожения данных.

– конфиденциальность информации и, одновременно, ее

– доступность для всех авторизованных пользователей.

Следует также отметить, что отдельные сферы деятельности (банковские и финансовые институты, информационные сети, системы государственного управления, оборонные и специальные структуры) требуют специальных мер безопасности данных и предъявляют повышенные требования к надежности функционирования информационных систем, в соответствии с характером и важностью решаемых ими задач

СПИСОК ЛИТЕРАТУРЫ

1. Ефимов Е.Г. Социальные интернет-сети (методология и практика исследования) / Е.Г. Ефимов. — Волгоград : Волгоград. науч. изд-во, 2015. — 169 с.
2. Иванченко Р.Б. Проблемы квалификации мошенничества в сфере компьютерной информации / Р.Б. Иванченко, А.Н. Малышев // Вестник Воронежского института МВД России. — 2014. — № 1. — С. 194-200.
3. Использование возможностей ЕИТКС ОВД в деятельности органов предварительного следствия в системе МВД России : учеб. пособие / под ред. И.А. Попова. — М. : Проспект, 2013. — 124 с.
4. Комаров А.А. Интернет-мошенничество: проблемы детерминации и предупреждения / А.А. Комаров. — М. : Юр- литинформ, 2013. — 184 с.
5. Никулин И.В. О практике противодействия незаконному обороту и пропаганде наркотических средств и иных психотропных веществ в информационно-телекоммуникационной сети Интернет / И.В. Никулин // Вестник Сибирского юридического института ФСКН России. — 2013. — № 2 (13). — С. 46-50.
6. Осипенко А.Л. Сетевая компьютерная преступность: теория и практика борьбы / А.Л. Осипенко. — Омск : Ом. акад. МВД России, 2009. — 480 с.
7. Польшиков А.В. Криминологическая характеристика лиц, совершающих изготовление и оборот детской порнографии в сети «Интернет» / А.В. Польшиков // Общество и право. — 2009. — № 3. — С. 190-194.
8. Прогноз криминогенной обстановки и противодействие преступности в Рязанской области : науч.-аналит. обзор с метод. рекомендациями / Д.Е. Некрасов, Э.Ю. Бадальянц, Я.Г. Ищук, О.Н. Чистотина, Г.С. Шкабин ; под общ. ред. Д.Н. Архи- пова. — Рязань : Рязан. фил. Моск. ун-та МВД России, 2013. — 153 с.
9. Простосердов М.А. Вымогательство, совершенное в сети Интернет / М.А. Простосердов // Библиотека криминалиста. — 2013. — № 6 (11). — С. 150-152.
10. Рыдченко К.Д. Административно-правовое обеспечение информационно-психологической безопасности органами внутренних дел Российской Федерации : дис. ... канд. юрид. наук : 12.00.14 / К.Д. Рыдченко. — Воронеж, 2011. — 308 с.
11. Симоненко А.В. Оценка криминальной ситуации в вузовской студенческой среде и меры ее коррекции / А.В. Си- моненко, Е.В. Грибанов // Вестник Воронежского института МВД России. — 2015. — № 1. — С. 122-127.

12. Смагина А.В. Причины распространения экстремизма в России / А.В. Смагина, Д.И. Сопун // Российский следователь. — 2012. — № 8. — С. 33-36.
13. Сынгаевский Д.В. Мошенничество в глобальной сети Интернет как объект виктимологического исследования / Д.В. Сынгаевский // Современный юрист. — 2013. — № 4. — С. 136-144.
14. Тропина Т.Л. Борьба с киберпреступностью: возможна ли разработка универсального механизма? / Т.Л. Тропина // Международное правосудие. — 2012. — № 3. — С. 86-95.
15. Уразаева Г.И. Методологические принципы изучения личности преступника и преступного поведения / Г.И. Уразае- ва // Вестник Казанского юридического института МВД России. — 2014. — № 3 (17). — С. 126-130.
16. Boyd D. Social Network Sites: Definition, History, and Scholarship / D. Boyd, N. Ellison // Journal of Computer-Mediated Communication. — 2007. — Vol. 13, № 1. — P. 210-230.
17. Conway M. Terrorism and the Internet: new media — new threat? / M. Conway // Parliamentary Affairs. — 2006. — Vol. 59, № 2. — P. 283.
18. Goodman M. International Dimensions of Cybercrime / M. Goodman // Cybercrimes: A Multidisciplinary Analysis / S. Ghosh, E. Turrini (eds). — Berlin : Heidelberg, 2010. — 361 p.
19. Metchik E. A typology of crime on the Internet / E. Metchik // Security Journal. — 1997. — Vol. 9, № 1-3. — P. 27-31.
20. Whitty M.T. The Scammers Persuasive Techniques Model: Development of a Stage Model to Explain the Online Dating Romance Scam / M.T. Whitty // The British Journal of Criminology. — 2014. — № 53 (4). — P. 665-684.
21. Yar M. The Novelty of Cybercrime: An Assessment in Light of Routine Activity Theory / M. Yar // European Journal of Criminology. — 2005. — Vol. 2, № 4. — P. 407-427.

1. Приговор Сургутского городского суда Ханты- Мансийского автономного округа — Югры Тюменской области по уголовному делу № 1-586/2013. URL: https:// rospravosudie.com/court-surgutskij-gorodskoj-sud-xanty- mansijskij-avtonomnyj-okrug-s/act-422314559 (дата обращения: 31.03.2014). ↑

2. Приговор Верховного Суда Республики Дагестан по уголовному делу № 2-35/13. URL: https://rospravo- sudie.com/court-verxovnyj-sud-respubliki-dagestan-re-spublika-dagestan-s/act-430038044. ↑

3. Приговор Энгельсского районного суда Саратовской области по уголовному делу № 1-298/2013. URL: https://rospravosudie.com/court-engelsskij-rajonnyj-sud-saratovskaya-oblast-s/act-459430034. ↑