УДК 004.056.5+343.3

Номоконов В.А., Тропина Т.Л.

КИБЕРПРЕСТУПНОСТЬ: УГРОЗЫ, ПРОГНОЗЫ, ПРОБЛЕМЫ БОРЬБЫ

Анотація:

У цій роботі розглядається поняття кіберзлочинності та основні способи вирішення проблем, пов'язаних з кіберзлочинністю. Також увага зосереджена на проблемах боротьби з кіберзлочинності в Росії.

Аннотация:

В данной работе рассматривается понятие киберпреступности и основные способы решения проблем, связанных с киберпреступностью. Также внимание сосредоточено на проблемах борьбы с киберпреступностью в России .

Abstract:

This paper is devoted to the concept of cybercrime and basic solutions to the problems associated with cybercrime. It is also focused on the problem of combating cybercrime in Russia.

Понятие и виды киберпреступности

Рост информационных технологий в России, как и во всем мире, обусловил не только быстрое развитие и эффективное применение информационных сетей в предпринимательской деятельности и в повседневной жизни, но и рост новых угроз. Анонимность глобальных информационных сетей, быстрота передачи информации и простота их использования (то, что является основными причинами технологического бума и проникновения сети Интернет во все сферы жизни) одновременно позволяют использовать все эти преимущества для совершения противоправных деяний. Информационно-коммуникационные технологии внедряются и развиваются гораздо быстрее, чем законодатели и правоохранительные органы могут реагировать на этот рост.

По данным ООН, в 2011 году, по меньшей мере, 2,3 миллиарда человек или более одной трети от общей численности населения планеты имели доступ к Интернету, а к 2017 году доступ к мобильному широкополосному Интернету получат уже до 70 процентов от общей численности населения мира [1].

В России количество пользователей возросло почти вдвое всего за три года: с 47 миллионов в 2009 году до 70 миллионов в 2012 [2]. Одновременно с количеством пользователей увеличивается как число потенциальных жертв, так и возможность использовать сеть Интернет для совершения противоправных деяний. На протяжении последних десятилетий угроза киберпреступности превратилась в острую проблему, требующую координации действий на международном уровне.

С момента, когда сеть Интернет, изначально использовавшаяся в военных и научных целях стала доступна широкому кругу пользователей и до момента, когда угроза преступности в информационных сетях стала очевидной, прошло достаточно времени, чтобы разрыв между развитием цифровых технологий и разработкой механизмов их регулирования, особенно в сфере борьбы с электронными посягательствами, создал правовой вакуум.

Этот разрыв не уменьшается и по сей день, обусловливая появление новых проблем защиты компьютерных сетей и их пользователей от посягательств, новых способов совершения преступлений, а также их рост.

При этом проблема преступности в глобальных информационных сетях имеет два компонента. Во-первых, появляются новые преступления, такие как нарушение целостности, доступности и конфиденциальности электронных данных, объектом которых являются *новые* охраняемые законом интересы, возникшие в связи с развитием информационных технологий. Во-вторых, глобальные информационные сети используются для совершения деяний, уже криминализованных в законодательстве многих государств, таких как хищение имущества, распространение детской порнографии, нарушение тайны частной жизни, и др. В связи с этой двойственностью возникает вопрос о дефиниции «киберпреступности» как явления, включающего как «традиционные» преступные деяния, совершенные с помощью новых технологий, так и деяния, направленные на новые объекты посягательств.

Термин «киберпреступность» часто употребляется наряду с термином «компьютерная преступность», причем нередко эти понятия используются как синонимы. Действительно, эти термины очень близки друг другу, но все-таки, на наш взгляд, не синонимичны. Понятие «киберпреступность» (в англоязычном варианте – cybercrime) шире, чем «компьютерная преступность» (computer crime), и более точно отражает природу такого явления, как преступность в информационном пространстве.

Глобальное информационное пространство, информационная мегасреда нематериальны и по сути своей несводимы к физическому носителю, в котором воплощены. Поэтому термин «компьютерная преступность» все-таки несколько уже по своей смысловой нагрузке, и сводит суть явления к преступлениям, совершенным с помощью компьютера. В настоящее же время с развитием информационных технологий уже само понятие «компьютер» становится размытым. Например, сегодня практически все мобильные телефоны имеют доступ в сеть Интернет.

По пути разделения терминов «киберпреступность» и «компьютерная преступность» и использованию именно первого термина идет также международное право. В Конвенции Совета Европы о киберпреступности (2001 г.) употребляется именно термин «cybercrime», а не «computer crime».

Киберпреступность – это преступность в так называемом киберпространстве. Авторы «модельного закона» о киберпреступности Международного Союза Электросвязи (2009 г.) определяют киберпространство как «физическое и не физическое пространство, созданное и (или) сформированное следующим образом: компьютеры, компьютерные системы, сети, их компьютерные программы, компьютерные данные, данные контента, движение данных, и пользователи».

В настоящее время официальное определение киберпространства на международном уровне отсутствует, впрочем, как и определение киберпреступности. В 2013 г. Управление ООН по наркотикам и преступности отметило, что понятие «киберпреступность» зависит от контекста и цели употребления этого термина. При этом, хотя основное «ядро» этого термина представляют преступления против конфиденциальности, целостности и доступности данных, кроме этого довольно ограниченного списка компьютерных преступлений, в понятие «киберпреступность» включаются любые деяния, направленные на не-

легальное извлечение прибыли, контент-преступления, и прочие противозаконные деяния в киберпространстве [3].

Авторы настоящей работы придерживаются точки зрения о том, что понятие киберпреступности как совокупности преступлений распространяется на все виды преступлений, совершенных в информационно-телекоммуникационной сфере, где информация, информационные ресурсы, информационная техника могут выступать (являться) предметом (целью) преступных посягательств, средой, в которой совершаются правонарушения и средством или орудием преступления.

Киберпреступления подразделяют на виды в зависимости от объекта, от предмета посягательства, от способов совершения и т. п. По объекту посягательства выделяются следующие группы киберпреступлений: преступления против конфиденциальности, целостности и доступности компьютерных данных и компьютерных сетей, экономические компьютерные преступления, компьютерные преступления против личных прав и неприкосновенности частной сферы, компьютерные преступления против общественных и государственных интересов. Однако стоит отметить, что многие киберпреступления посягают сразу на несколько объектов: например, незаконный перехват частных электронных коммуникаций посягает на неприкосновенность частной сферы и на конфиденциальность компьютерных данных, компьютерное мошенничество – на собственность и на целостность компьютерных данных и т.д.

Состояние, структура и динамика киберпреступности

Киберпреступность – это явление по своей природе трансграничное. Поэтому анализ киберпреступности или ее разновидности – компьютерной преступности – в рамках одной страны или группы стран, безусловно, ценен, но вряд ли способен дать представление об истинных масштабах и о размахе этого явления. Глобальность и трансграничность компьютерных и телекоммуникационных сетей, возможность манипуляций преступника с идентичностью (т.е., использования чужих имен, адресов, паролей и т.п.) создает ситуации, когда преступник находится на одном континенте, преступление непосредственно совершается на другом, а последствия преступления наступают на третьем. Более того, в последние несколько лет в связи с появлением и распространением ботнетов – сетей инфицированных компьютеров, проводящих атаки независимо от пользователей, ситуация усложнилась еще больше: преступник, сотни атакующих компьютеров и потерпевший от преступления могут находиться на территории более чем двух или трех государств.

В настоящее время не существует ни релевантной статистики, отражающей реальную картину состояния киберпреступности, ни надежных методов сбора таких данных. И дело не только в отсутствии единообразия национального уголовного законодательства стран в сфере борьбы с киберпреступностью и разной практике его применения, различиях в формировании уголовной статистики и особенностях правоохранительной системы. Так, до сих пор неясно, до какой степени достоверна статистика об экономических потерях в результате киберпреступности.

Есть мнение, например, что доход от киберпреступлений значительно превысил доход от других преступлений, включая торговлю наркотиками. По последним данным, приведенным в июле 2013 г. в совместном анализе американского Центра стратегических и международных исследований и компании McAfee, ежегодные потери мировой экономики от киберпреступлений достигли уже 500 миллиардов долларов [4].

Чтобы представить себе масштабы и обороты этого криминального бизнеса, достаточно привести некоторые примеры. Виртуальные мошенники, завладев через Сеть номерами более чем миллиона банковских карт граждан США, одновременно совершили хищения в 130 банкоматах в 49 городах Америки. При этом вся операция заняла не более 30 минут, а размер прибыли преступников составил около 9 млн. долларов, которые затем были переведены на счета в различные государства, в основном на постсоветском пространстве. В 2010 г. ФБР выдвинуло обвинения против 37 жителей России, Украины и других восточноевропейских стран, подозреваемых в использовании компьютерного вируса для взлома американских банковских счетов [5].

Наибольшая часть киберпреступности остается за рамками статистики – можно с уверенностью утверждать, что в официальную статистику попадает лишь десять, в лучшем случае двадцать процентов совершенных деяний.

Структура киберпреступности различается заметно в разных странах в зависимости, прежде всего, от характера и степени развития информационных технологий, распространения сети Интернет, использования электронных сервисов и электронной коммерции и т.п.

Киберпреступность имеет разные последствия и структуру для развитых и развивающихся стран. Так, например, если проблема СПАМ (незаконных массовых рассылок по электронной почте) для развитых государств опасна в основном из-за вирусных программ, которые рассылаются вместе со СПАМом, то в развивающихся странах проблемой является также пропускная способность телекоммуникационных сетей, которые не могут выдержать подобной нагрузки. Структура и динамика киберпреступности, а также ее масштабы зависят и от культуры кибербезопасности пользователей в отдельном государстве, что также имеет разные аспекты в зависимости от степени развития экономики той или иной страны.

Угрозы в информационном пространстве меняются с развитием технологий.

В 2013 г., согласно прогнозу специалистов McAfee, на первый план выходят угрозы, связанные с использованием мобильного доступа в сеть Интернет (зараженные вредоносным ПО приложения для мобильных телефонов и вирусы, блокирующие обновления антивирусного ПО, смс-сообщения, зараженные вирусами). Кроме того, среди опасных тенденций отмечаются: постоянное развитие способов атак на Windows 8 и HTML5; атаки, направленные не на извлечение выгоды, а на причинение вреда инфраструктуре; использование вредоносного ПО для ботнетов, которое обновляет соединение даже после того, как ботнет уничтожен, что позволяет дальнейшее распространение инфекции; развитие аутсорсинга кибератак среди криминальных групп и продажа ПО и услуг по совершению киберпреступлений. Также предупреждается, что политическая активность в Интернете будет замещаться экстремистскими группами, а причастность государств к киберпреступности увеличится как в плане атак, организованных на государственном уровне, так и в плане возможности стать мишенью атак [6].

В 2011 г. российские хакеры заработали около 3,7 млрд., а в 2013 г., как ожидается, удвоят данный показатель. При обзоре актуальных услуг и типовых цен на них, существующих на российском рынке киберпреступности, эксперты выделили следующие виды преступлений, которые представляют наибольшую общественную опасность: DDoS-атаки – сетевые атаки, направленные на отказ в обслуживании; мошенничество в системах ДБО – неправомерная отправка электронных платежных поручений с целью хищения денеж-

ных средств; спам – массовая рассылка нежелательных сообщений электронной почты; продажа трафика – услуги по установке программ на большое количество компьютеров и услуги по перенаправлению посетителей на определенные веб-сайты (услуга относится к внутреннему рынку киберпреступности); партнерские программы – нелегальная продажа медикаментов, продажа контрафактного ПО, загрузок и т.п. (услуга относится к внутреннему рынку киберпреступности) [7].

Сегодня практически все исследователи и специалисты признают, что ситуация с киберпреступностью в мире пока имеет тенденцию к ухудшению. Еще одна опасная тенденция – все большая связь между киберпреступностью и организованной преступностью. Большинство киберпреступлений совершается индивидуумами или небольшими преступными группами. Однако специалисты отмечают растущую взаимосвязь между киберпреступностью и организованной преступностью. Можно с уверенностью сказать, что Интернет используется преступными группами уже не только как вспомогательное средство, но и как место и основное средство совершения традиционных преступлений – мошенничеств, краж, вымогательств. По данным Европола, только в ЕС действует около 3600 таких групп [8]. Более того, в течение последних лет отмечается «профессионализация» организованной киберпреступности: не только компьютерные атаки становятся все более комплексными и явно требующими участия профессионалов в их подготовке, но и мошенничества в сети Интернет, кража данных, отмывание денег превращаются в большой сектор теневого рынка с разделением труда между преступными группами и целыми площадками для торговли программным обеспечением для совершения преступлений, для продажи информации, для «аутсорсинга» навыков, необходимых на той или иной стадии совершения Интернет-преступлений.

Проблемы борьбы с киберпреступностью

Борьба с киберпреступностью невозможна без глубокого понимания правовых проблем регулирования информационных сетей. Именно анализ взаимосвязи между техническими характеристиками сети и обусловленными этими характеристиками правовыми и социальными сложностями, с которыми сталкиваются законодатели и правоохранительные органы, является первым шагом к возможной выработке механизмов адекватного реагирования на развитие и рост киберпреступности.

Отсутствие механизмов контроля. Основная проблема борьбы с преступностью в сети Интернет заключается в транснациональности самой сети и в отсутствии механизмов контроля, необходимых для правоприменения. Когда сеть Интернет создавалась технологически как структура без иерархии и без некоего «ядра», разрушив которые, можно было бы парализовать её работу, вряд ли кто-то мог представить масштабы развития проекта, изначально не предназначенного для широкой аудитории. Основной целью создания этой сети была устойчивость к атакам извне, и вряд ли кто-то мог предвидеть последующий масштаб ее развития и ее социальную и экономическую роль в будущем. Именно отсутствие разработанных механизмов контроля сети изнутри вкупе с ее доступностью и легкостью использования стало одной из глобальных проблем информационного сообщества: децентрализованная структура сети и отсутствие национальных границ в киберпространстве обусловили возможности для роста преступности и на годы отложили разработку механизмов социального и правового контроля в сфере использования информационных сетей для совершения преступлений.

В последние годы информационные сети развиваются слишком быстро, чтобы существующие механизмы контроля успевали реагировать на новые проблемы. Облачная обработка данных, автоматизация атак, уязвимость персональной информации в социальных сетях, распространение так называемого «информационного оружия», примером которого является вирус Stuxnet – на все эти проблемы правовое регулирование пока не может найти адекватного ответа.

С того момента, когда государство включается в информационный обмен посредством сети Интернет, оно само и его граждане становятся уязвимыми для посягательств из любой точки земного шара. Механизмы контроля, предотвращения и расследования посягательств в киберпространстве очень ограничены как социально, так и технологически. Например, как показывает пример атак на ядерное производство Ирана, даже отключение особо важных для государства объектов от глобальных информационных сетей не защищает их от возможных атак: вирус Stuxnet распространялся через портативные накопительные устройства, подключаемые к компьютеру через порт USB [9]. Единственный способ полностью обезопасить особо важные объекты для функционирования общества – это полностью отключить сеть Интернет не только от объектов защиты, но и во всём государстве в целом. Разумеется, это невозможно, поскольку информационные технологии играют важнейшую роль в функционировании общества.

Количество пользователей. С увеличением количества пользователей возрастают следующие факторы риска: увеличивается зависимость общества от информационных технологий, что, в свою очередь, обусловливает его уязвимость к различного рода информационным посягательствам; увеличивается возможность использования сети для совершения преступлений, а также растёт потенциальная возможность стать жертвой использования информационных технологий в преступных целях. При этом совершение преступления не требует больших усилий и затрат – достаточно иметь компьютер, программное обеспечение и подключение к информационной сети. Не требуется даже глубоких технических познаний: существуют специальные форумы, на которых можно приобрести программное обеспечение для совершения преступлений, украденные номера кредитных карт и идентификационные данные пользователей, а также воспользоваться услугами по оказании помощи в совершении электронных хищений и атак на компьютерные системы как в целом, так и на отдельных стадиях совершения преступлений.

Автоматизация и быстрота использования. Компьютерные данные могут быть переданы из одной точки мира в другую за несколько секунд. Более того, практически любая передача данных в сети обычно включает несколько стран, поскольку, когда информация разбивается на части и идёт по наиболее удобным и доступным каналам. Контролировать передачу данных, с учётом их объёма и количества пользователей, очень трудно, если не невозможно. Преступник, потерпевший, сервер с необходимой информацией могут находиться в разных странах и на разных континентах, что требует сотрудничества правоохранительных органов нескольких стран при расследовании преступления.

Автоматизация увеличивает риск совершения множественных преступлений без особых финансовых и временных затрат. Более того, она позволяет преступникам аккумулировать большую финансовую прибыль путём хищения небольших сумм у тысячи пользователей, что создаёт проблемы обнаружения преступлений (владелец банковского счета может просто не заметить исчезновения финансовых средств) и возбуждения уголовных дел. Например, если тот же владелец банковского счета обратится с заявлением о пропаже

незначительной суммы, правоохранительным органам будет достаточно трудно оценить масштаб деятельности тех, кто совершил хищение, поскольку ущерб, причинённый одному потерпевшему, очень мал, в то время как правонарушители путём аккумуляции этих небольших сумм могут добиться внушительной прибыли.

Анонимность сети Интернет, уязвимость беспроводного доступа и использование прокси-серверов существенно затрудняют обнаружение преступников: для совершения преступления может использоваться «цепочка» серверов, преступления могут быть совершены путём выхода в Интернет через точки общего доступа, такие, как Интернет-кафе, технологии позволяют также «взломать» доступ в чужую беспроводную сеть Wi-Fi. Таким образом, существует достаточно способов затруднить расследование преступлений.

Проблема территориальной юрисдикции в киберпространстве и правового сотрудничества. Расследование преступлений в информационных сетях обычно требует быстрого анализа и сохранения компьютерных данных, которые очень уязвимы по своей природе и могут быть быстро уничтожены. В этой ситуации традиционные механизмы правовой взаимопомощи и принцип суверенитета, одним из проявлений которого является то, что только правоохранительные органы государства могут производить следственные действия на его территории, требуют множество формальных согласований, делая расследование транснациональных киберпреступлений проблематичным. Помимо сотрудничества правоохранительных органов, которое требует временных затрат и соблюдения множества формальностей, встаёт также вопрос о соблюдении фундаментального принципа законности, когда необходима двойная криминализация деяния как в стране, с территории которой действовал правонарушитель, так и в государстве, где находится потерпевший. Разница в криминализации деяний, различия в определении тяжести совершенного деяния, особенно в сфере религиозных преступлений и преступлений против общественного порядка, в области нелегального контента, экстремистских преступлений значительно затрудняют процесс сотрудничества правоохранительных органов, иногда делая его невозможным.

Таким образом, эффективный контроль негативных явлений в киберпространстве, таких как преступность, требует гораздо более интенсивного международного сотрудничества, чем существующие меры по борьбе с любыми другими формами транснациональной преступности. Именно поэтому помимо гармонизации уголовно-правовых норм требуется гармонизация процессуальных инструментов и выработка новых механизмов международного сотрудничества. Важную роль в борьбе с киберпреступностью поэтому играют международные соглашения в соответствующей области, такие, как Конвенция Совета Европы о киберпреступности и др.

Все указанные инструменты не являются по своей сути универсальными международными инструментами, несмотря на то, что такие соглашения как Конвенция Совета Европы вышли по своему влиянию далеко за рамки региона, в котором они были приняты. Однако мировое сообщество пока не располагает ни международным органом, специально занимающимся интернет-преступностью, ни общемировым правовым инструментом, определяющим масштабы ответственности за соответствующие преступления, и, что более важно – принципы сотрудничества при расследовании противоправных деяний.

Тем не менее, в мире предпринимаются определенные шаги в направлении более решительного противодействия новой глобальной угрозе. Так, как известно, Россия выступила в последние годы с инициативой принятия специальной Конвенции ООН, пола-

гая, что назрела потребность в разработке и принятии универсальной международной конвенции по борьбе с киберпреступностью. В Совете безопасности и МИДе РФ подготовлен проект конвенции ООН «Об обеспечении международной информационной безопасности». Однако следует отметить, что этот документ направлен скорее на предотвращение агрессивных актов в киберпространстве, чем на создание или развитие уголовно-правовой и уголовно-процессуальной основы для борьбы с киберпреступностью. В настоящее время одной из проблем выработки механизмов борьбы с киберпреступностью является отсутствие четкого понимания границы между вопросами информационной безопасности и вопросами предотвращения и преследования киберпреступлений. Между тем, эту границу можно провести на уровне разделения отраслей права – для борьбы с киберпреступностью требуются уголовно-правовые и уголовно-процессуальные механизмы, в то время как вопрос информационной безопасности, информационной агрессии, кибервойн находится в сфере дипломатии, внешней политики и международного гуманитарного права.

В начале 2013 г. в Совете Федерации (СФ) России прошло обсуждение проекта национальной стратегии кибербезопасности. В ней предложено создать «экспертно-консультационный орган при президенте РФ по вопросам кибербезопасности», расширить полномочия правоохранительных органов, а также подключить бизнес и граждан к анализу «подозрительных информационных потоков». Все это, как считают в СФ, позволит создать «фронт борьбы с киберпреступниками» [10].

Разработка специальной Стратегии кибербезопасности представляет весьма актуальную задачу для России в сфере противодействия угрозам в виртуальном пространстве. Частью этой стратегии должна стать стратегия борьбы с киберпреступностью. Подобный опыт уже имеет целый ряд государств. Информационная безопасность уже рассматривается государствами как одна из приоритетных задач в сфере национальной безопасности и международной политики – при этом концепция информационной безопасности включает как защиту пользователей сетей, так и защиту государства и критических инфраструктур.

Однако, поскольку ни одно государство не может защитить себя, принимая меры только на национальном уровне, для комплексного противодействия киберпреступности необходимы:

– гармонизация уголовного законодательства о киберпреступлениях на международном уровне;

– разработка на международном уровне и имплементация в национальное законодательство процессуальных стандартов, позволяющих эффективно расследовать преступления в глобальных информационных сетях, получать, исследовать и представлять электронные доказательства с учетом трансграничности проблемы;

– отлаженное сотрудничество правоохранительных органов при расследовании киберпреступлений на оперативном уровне;

– механизм решения юрисдикционных вопросов в киберпространстве.

Таким образом, международное сотрудничество является ключевым моментом в ликвидации правового вакуума, существующего между развитием информационных технологий и реагированием на них законодательства. Процесс выработки мер на международном уровне, как показывает опыт, сам по себе является комплексной проблемой. Однако это единственный путь обеспечить безопасность пользователей и государства от

электронных посягательств, а также эффективно расследовать и преследовать киберпреступления.

Литература:

1. The Economic impact of cybercrime and cyberspionage. Center for Strategic and International Studies. July 2013. Report [Electronic Resource]. – Santa Clara, California: Mission College Boulevard, 2013. – Mode of access: http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime.pdf.

2. 10 наиболее тяжких преступлений в интернете по версии CNet [Электронный ресурс]. – Режим доступа: http://www.itsec.ru/newstext.php?news_id=62874. – Название с экрана.

3. 2013 Threats predictions. By McAfee Labs. Report [Electronic Resource]. – Santa Clara, California: Mission College Boulevard, 2013. – Mode of access: http://www.mcafee.com/us/resources/reports/rp-threat-predictions-2013.pdf.

4. За 2010 год русские хакеры заработали около $2.5 млрд. [Электронный ресурс] // CNEWS. Издание о высоких технологиях. – Режим доступа: http://www.cnews.ru/news/line/index.shtml?2011/03/28/433836. – Название с экрана.

5. Ustinova A. Russian Cybercrime Thrives as Soviet-Era Schools Spawn Hackers [Electronic Resource] / Anastasia Ustinova. – Mode of access: http://www.bloomberg.com/news/2010-10-05/russian-cybercrime-thrives-as-soviet-era-schools-spawn-world-s-top-hackers.html.

6. Orrey K. A Survey of USB Exploit Mechanisms, profiling Stuxnet and the possible adaptive measures that could have made it more effective [Electronic Resource] / Kevin Orrey. – Mode of access: http://www.vulnerabilityassessment.co.uk/education/whitepaper.pdf.

7. Иванов М. Борьбу с киберпреступлениями предлагают вывести на новый уровень [Электронный ресурс] / Максим Иванов. – Режим доступа: http://www.kommersant.ru.

8. UNODC. Всестороннее исследование проблемы киберпреступности и ответных мер со стороны государств-членов, международного сообщества и частного сектора [Электронный ресурс]. – Vienna, 2013. – 21 с. – Режим доступа: http://www.unodc.org/documents/organized-crime/unodc_ccpcj_eg.4_2013/unodc_ccpcj_eg4_2013_2_r.pdf.

9. Сергей Фомин. Количество пользователей в России и другие показатели аудитории интернета [Электронный ресурс] / Сергей Фомин. – Режим доступа: http://www.bizhit.ru/index/users_count/0-151.

10. UNODC. Comprehensive Study on Cybercrime, February 2013. [Electronic Resource]. – Vienna, 2013. – 320 c. – Mode of access: http://www.unodc.org/documents/organized-crime/unodc_ccpcj_eg.4_2013/cybercrime_study_210213.pdf.