УДК 343.32

Д.К. ЧИРКОВ,

кандидат юридических наук, доцент, старший научный сотрудник

НИИ Академии Генеральной прокуратуры РФ, г. Москва, Россия,

А.Ж. САРКИСЯН,

кандидат юридических наук, инспектор кафедры учебно-методической работы

Институт повышения квалификации Следственного комитета РФ, г. Москва, Россия

ПРЕСТУПНОСТЬ В СФЕРЕ ТЕЛЕКОММУНИКАЦИЙ И КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ КАК УГРОЗА НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ СТРАНЫ

Цель: изучить состояние преступности в сфере телекоммуникаций и компьютерной информации и выработать эффективные меры по их предупреждению.

Методы: восхождение от абстрактного к конкретному; системно-структурный анализ; исторический метод; динамический и статистический методы, а также применялась конкретно-социологическая методика оценки этой преступности.

Результаты: показаны особенности преступлений в сфере телекоммуникаций и компьютерной информации по их общественной опасности. Предложены эффективные меры по противодействию рассматриваемым преступлениям.

Научная новизна: проведен анализ динамики зарегистрированных в Российской Федерации преступлений, совершенных в сфере телекоммуникаций и компьютерной информации к числу пользователей Интернетом в течение 2009–2012 гг. Сделаны выводы о латентности рассматриваемых преступлений.

Практическая значимость: Данные исследования позволяют проследить уровень латентности рассматриваемых преступлений, а также оптимизировать меры по противодействию указанным преступлениям.

Ключевые слова: высокие технологии в сфере телекоммуникаций и компьютерной информации; характеристика преступлений; интернет-пользователи.

Введение

Современные достижения в области телекоммуникаций и повседневное массовое внедрение цифровых технологий предопределили возникновение новых угроз и рисков в данной сфере. Целью статьи является изучение состояния преступности в сфере телекоммуникаций и компьютерной информации и выработка эффективных мер по их предупреждению.

В настоящее время наибольшую значимость и распространенность имеет Интернет, предоставивший человеку безграничные возможности в области передачи, распространения информации и позволивший выполнять финансово-банковские операции, несмотря на расстояния и границы. Получив очевидные преимущества сети Интернет, общество столкнулось с новыми видами и способами совершения преступлений в сфере высоких технологий. Интернет, с одной стороны, позволил более эффективно и безнаказанно совершать ранее существовавшие традиционные преступления, с другой – породил новые, неизвестные ранее мировому сообществу виды общественно опасных посягательств.

Результаты исследования

За последние десять лет (2003–2012 гг.) количество пользователей Интернета в России выросло приблизительно в 5,4 раза (2003 г. – 12 млн, 2010 г. – 59,7 млн (43% всего населения), 2012 г. – 68,0 млн (48% всего населения) [1]. За период с 2010 по 2012 гг. количество пользователей увеличилось на 8,3 млн чел., а в 2014 г. этот показатель, по прогнозам Министерства связи массовых коммуникаций Российской Федерации, может достигнуть 80 млн человек [2]. Интернет стал не просто технологией, а уникальным новшеством, изменившим мир (табл. 1).

Вызывает опасение, что в современных условиях огромный технический потенциал и безграничные возможности Интернета все чаще могут быть использованы в преступных целях.

В последнее десятилетие Интернет играет важную роль в сфере коммуникаций: мы проводим различные операции с денежными средствами как с использованием компьютера, так и банкомата, пользуемся электронными платежными системами, прокладываем маршруты, ищем хорошие рестораны, узнаем, на какой фильм сходить, – все эти действия зависят от информационных технологий. В связи с этим многие пользователи Интернета подвергаются атакам со стороны киберпреступников[1].

Анализ статистических данных о преступности в сфере компьютерной информации показывает, что с 1997 по 2005 гг. в России количество зарегистрированных преступлений в сфере компьютерной информации (гл. 28 УК РФ) выросло более чем в 300 раз (10 214 преступлений за год).

В 2012 г. число зарегистрированных преступлений *в сфере телекоммуникаций и компьютерной информации* составило 10 227, что на 28,3% выше показателя 2011 г. (7 974 эпизода). В 2010 г. количество аналогичных преступлений составило

Таблица 1

20 стран с самым высоким числом интернет-пользователей [3]

№	Страна или регион	Население, 2012 Est	Интернет-пользователей, 2000 г.	Интернет-пользователей, последние данные	Проникновение (% населения)	Пользователи, (% в мире)
1	Китай	1,343,239,923	22,500,000	538,000,000	40,1%	22,4%
2	США	313,847,465	95,354,000	245,203,319	78,1%	10,2%
3	Индия	1,205,073,612	5,000,000	137,000,000	11,4%	5,7%
4	Япония	127,368,088	47,080,000	101,228,736	79,5%	4,2%
5	Бразилия	193,946,886	5,000,000	88,494,756	45,6%	3,7%
6	Россия	142,517,670	3,100,000	67,982,547	47,7%	2,8%
7	Германия	81,305,856	24,000,000	67,483,860	83,0%	2,8%
8	Индонезия	248,645,008	2,000,000	55.000,000	22,1%	2,3%
9	Великобритания	63,047,162	15,400,000	52,731,209	83,6%	2,2%
10	Франция	65,630,692	8,500,000	52,228,905	79,6%	2,2%
11	Нигерия	170,123,740	200,000	48,366,179	28,4%	2,0%
12	Мексика	114,975,406	2,712,400	42,000,000	36,5 %	1,7%
13	Иран	78,868,711	250,000	42,000,000	53,3 %	1,7%
14	Корея	48,860,500	19,040,000	40,329,660	82,5 %	1,7%
15	Турция	79,749,461	2,000,000	36,455,000	45,7 %	1,5%
16	Италия	61,261,254	13,200,000	35,800,.000	58,4%	1,5%
17	Филиппины	103,775,002	2,000,000	33,600,000	32,4%	1,4%
18	Испания	47,042,984	5,387,800	31,606,233	67,2,%	1,3%
19	Вьетнам	91,519,289	200,000	31,034,900	33,9%	1,3%
20	Египет	83,688,164	450,000	29,809,724	35,6%	1,2%
ТОП-20 Стран		**4,664,486,873**	**273,374,200**	**1,776,355,028**	**38,1%**	**73,8%**
Прочее Мир		**2,353,360,049**	**87,611,292**	**629,163,348**	**26,7%**	**26,2%**
Общая Мир Пользователей		**7,017,846,922**	**360,985,492**	**2,405,518,376**	**34,3%**	**100%**

[1] Киберпреступник – человек, совершающий преступления с использованием информационных технологий.

12 698. Приведенный анализ динамики числа зарегистрированных преступлений, совершенных в сфере телекоммуникаций и компьютерной информации, свидетельствует о том, что максимальное количество преступлений было совершено в 2009 г. (17 535) (табл. 2).

Таблица 2

Динамика преступлений, совершенных в сфере телекоммуникаций и компьютерной информации, зарегистрированных в Российской Федерации, и число пользователей сети Интернет в течение 2009–2012 гг.

Показатель	Год			
	2009	2010	2011	2012
Абсолютный показатель	17 535	12 698	7 974	10 227
Темп прироста, к АППГ (%)	–	–27,6	–37,2	28,3
Число интернет-пользователей, (млн чел.) [4, с. 16; 5; 6]	53,5	59,7	60,4	68,0

* *Источник:* Статистические данные: Форма № 615 ГИАЦ МВД России № 615.

Очевидно, что тенденция снижения количества зарегистрированных преступлений, отмеченная в 2009–2011 гг., вряд ли адекватно отражает реальную динамику фактической преступности. На наш взгляд, подобные процессы могут быть объяснены, с одной стороны, реформой в органах внутренних дел и ослаблением контроля учетно-регистрационной дисциплины, с другой – снижением активности правоохранительных органов по выявлению такого вида преступлений, поскольку действие основных факторов, обуславливающих их совершение, не уменьшилось, а напротив увеличилось. Вместе с тем необходимо отметить, что рост вышеуказанных преступлений в 2012 г. связан с увеличением числа интернет-пользователей – (68,0) на 7,6 млн по сравнению с 2011 г. (60,4).

Это обстоятельство дает основание нам полагать, что отмечаемое сокращение количества зарегистрированных преступлений в 2009–2011гг. носит искусственный характер. Об этом свидетельствует табл. 1, динамика зарегистрированных в Российской Федерации преступлений, совершенных в сфере телекоммуникаций и компьютерной информации, и число пользователей сети Интернет в течение 2009–2012 гг.

По мнению бывшего начальника Управления компьютерной и информационной безопасности ФСБ России и руководителя Бюро специальных технических мероприятий МВД России Б. Мирошникова, «… из года в год в России наблюдается лавинообразный рост числа пострадавших от компьютерных преступлений. Растут убытки. Нарастает недовольство граждан… Эта устойчивая тенденция, причем, очевидно, что рост обращений серьезно отстает от реального роста количества преступлений» [4, с. 78–79].

Нельзя не говорить о латентности данного вида преступлений. По оценкам экспертов, латентность «компьютерных» преступлений в США достигает 80%, в Великобритании – 85%, в ФРГ – 75%, в России – более 90% [7].

Жертвы редко обращаются в полицию. 1/4 пользователей сети утверждают, что не предпримут никаких действий, став жертвами кибератаки [8]. К тому же органы правопорядка вряд ли бы справились с постоянным потоком жалоб, так как на раскрытие одного преступления требуется в среднем 28 дней и 334 доллара [9].

Также следует отметить тот факт, что сумма ущерба от преступлений, совершенных в сфере телекоммуникаций и компьютерной информации (если сравнить удельный вес исследуемого состава с иными преступлениями), значительна по отношению к другим видам составов УК РФ.

Даже по неполным оценкам экспертов, эти преступления обходятся минимум в 200 млрд долл. ежегодно в мире. Банковский грабитель рискует жизнью за 10 тыс. долл., а хакер[2], манипулируя компьютером и ничем не рискуя, может получить 1 млн [10]. В России средний ущерб, причиняемый потерпевшему от одного совершаемого преступления в сфере телекоммуникаций и компьютерной информации равен 1,7 млн руб. [11].

Высокая социальная опасность преступлений в Глобальной сети вытекает, прежде всего, из их транснационального характера, так как последствия подобных деяний могут охватывать неограниченный круг лиц в самых разных странах. При этом количество пользователей сетью Интернет во всем мире в 2007 г. было около полутора миллиарда и продолжает в наши дни стремительно

[2] Ха́кер (от англ. *hack* – разрубать) – чрезвычайно квалифицированный специалист в сфере информационных технологий, который понимает самые глубины работы компьютерных систем.

увеличиваться, что предполагает дальнейший рост причиненного от интернет-преступлений ущерба.

Следует отметить, что действует Конвенция о преступности в сфере компьютерной информации, принятая в Будапеште 23 ноября 2001 г. В данной Конвенции предусмотрены вопросы обеспечения каждой Стороной законодательных и иных мер, необходимых для того, чтобы квалифицировать в качестве уголовного преступления согласно ее внутригосударственному праву неправомерный доступ, когда он является преднамеренным, к компьютерной системе в целом или любой ее части.

Стороны, участвующие в Конвенции, осуществляют максимально широкое сотрудничество друг с другом путем применения соответствующих международных документов о международном сотрудничестве по уголовным делам, связанных с компьютерными системами и данными, или сбора доказательств по уголовному преступлению в электронной форме[3]. Российская Федерация в настоящей Конвенции не участвует.

Преступления, совершенные в сфере телекоммуникаций и компьютерной информации, кроме гл. 28 УК РФ, по нашему мнению, нецелесообразно относить к видам преступления, а скорее, к способам его совершения, и поэтому выделение рассматриваемого вида преступлений в отдельный сегмент УК РФ не имеет смысла. Например, совершение мошенничества с помощью высоких технологий. Но то, что они носят распространенный характер, безусловно. Поэтому изучение и анализ криминологической характеристики данных преступлений весьма актуальны и необходимы.

При совершении преступлений в сфере телекоммуникаций и компьютерной информации преступник, в отличие от других видов совершения преступных деяний, не контактирует с жертвой, зачастую находится от нее на значительном расстоянии и в положении анонимности. Часто преступления в данной сфере совершаются организованными группами, что характерно для киберпреступников.

Основными причинами киберпреступности в России являются: недостаточно развитое законодательство, регулирующее общественные отношения в сфере высоких технологий из-за ее высокотехнологичности, функциональности, глобальности; анонимность, которая является привлекательным элементом среды Интернет; безграмотность населения. В частности, только 13% населения являются продвинутыми пользователями, 17% владеют компьютером на среднем уровне, 70% признаются, что ничего не понимают в компьютерах [12].

По сравнению с другими странами в России хакеры – самые богатые в мире. Оборот рынка компьютерных преступлений достигает 1 млрд долл. в год[4]. Умелому хакеру кибератаки приносят от 30 до 900 млн руб. в месяц. Самыми прибыльными операциями хакера являются рассылка спама, кража конфиденциальной информации и Ddos-атаки[5], блокирующие работу сайта. Число вредоносных программ возросло на 1/3 по сравнению с прошлым годом и составило свыше миллиона. В прошлом году на каждого жителя планеты пришлось по 5000 спам-писем, многие из них содержали вредоносные программы для взлома счетов [13]. Вместе с тем правоохранительными органами Российской Федерации в 2012 г. по ст. 273 УК РФ (Создание, использование и распространение вредоносных программ для ЭВМ) было выявлено 889 преступлений, что на 28,3% выше показателя 2011 г. (693).

На сегодняшний день в сети Интернет существуют сайты, где предлагаются услуги хакера. Так, например, за взлом почты хакеры требуют 50 долл., за внедрения шпионской программы в компьютер – 100 долл., Ddos-атаки – 300–400 долл. [14]. В Америке аналогичные услуги стоят в 5 раз дороже.

Такими услугами в большинстве случаев пользуются преступники. Так, например, полицейские-борцы с киберпреступностью рассказывают,

---

[3] Система ГАРАНТ ЭКСПЕРТ. Конвенция о преступности в сфере компьютерной информации (Будапешт, 23 ноября 2001 г.).

[4] Такие данные приводит «Letogroup».

[5] DdoS-атака (сокр. от англ. Distributed Denial of Service) – атака на компьютерную систему с целью довести ее до отказа, т.е. до такого состояния, что правомочные пользователи системы не могут получить доступ к предоставляемым системой ресурсам (серверам, сервисам), либо этот доступ затруднен.

что недавно квартирные воры освоили новый способ вычислять отсутствующих дома жильцов. Для этого группировки профессиональных грабителей понемногу начинают сотрудничать с хакерами. Они взламывают наиболее распространенные социальные сети, устанавливают состоятельных посетителей и из переписки узнают, когда те уезжают на отдых. В таких случаях даже «закладки» не требуются [15].

Социальные сети уже давно используются злоумышленниками всех мастей для совершения преступлений. Исследование, проведенное в Великобритании, показало, что четыре из пяти ограблений совершаются при помощи Twitter и Facebook. В РФ такая статистика не ведется, но практика показывает, что российские преступники не отстают от зарубежных «коллег» в использовании информационных технологий. Личные страницы в социальных сетях часто позволяют получать сторонним пользователям значимую информацию о каждом из нас. Многие люди публикуют на своих страницах фотографии машин, техники, ювелирных украшений и других дорогих вещей. Такие фотографии представляют несомненный интерес для преступников и могут использоваться при выборе жертвы для ограбления [15].

В связи с этим существует угроза того, что компьютерные сети и электронная информация могут также использоваться для совершения уголовных преступлений, а доказательства совершения таких правонарушений могут храниться в этих сетях и передаваться по ним.

Глобальная сеть в последние годы стала использоваться не только для совершения общеуголовных преступлений, но и крайне опасных деяний международного значения – таких как «сетевая война», «интернет-терроризм», «интернет-забастовка», что создает угрозу безопасности целых государств и всего мирового сообщества.

К примеру, одной из окончательных версий, выдвинутой ФБР в ходе расследования катастрофического пожара и многочисленных мощных взрывов в марте 2004 г. на крупном американском нефтеперерабатывающем заводе компании British Petroleum Amoco в американском г. Техас-Сити, практически уничтоживших предприятие, вызвавших многочисленные человеческие жертвы и резкий рост биржевых цен на топливо, стала возможность подтвержденного следственными экспериментами замаскированного дистанционного изменения технологических температурных режимов ректификационного оборудования по сети Интернет.

Еще из множества недавних и наиболее потенциально опасных подозрительных инцидентов можно привести пример одновременного нарушения работы сразу двух американских АЭС компании Entergy Corp в ноябре 2010 г. Сначала из-за отказа дистанционно управляемых клапанов трубопроводных систем охлаждения, утечек радиоактивных вод и неисправности насосов первого контура была на неделю остановлена АЭС «Vermont Yankee» в штате Вермонт. Менее чем через час после первого инцидента в Вермонте неожиданно и без видимых причин взорвался и сгорел один из мощных силовых трансформаторов на территории атомной станции «Indian Point», расположенной в штате Нью-Йорк, что вызвало аварийное отключение ее реакторов. Во всех отмеченных случаях регистрировались сбои компьютерных систем управления и несанкционированный удаленный доступ к программному обеспечению [16].

14 февраля на Коллегии ФСБ Президент России В. Путин поставил задачу «формировать единую систему обнаружения, предупреждения и отражения компьютерных атак на информационные ресурсы России». По его словам, «нам нужны самые современные подходы к организации контрразведывательной деятельности, в том числе к защите секретной информации в связи с участившимися случаями попыток взлома национальных электронных баз данных» [17].

Выводы

На основании вышеизложенного можно сделать выводы о необходимости:

– разработки и реализации в приоритетном порядке в рамках уголовной политики целенаправленной на защиту общества и населения от преступности в сфере телекоммуникаций и компьютерной информации, в том числе путем принятия соответствующих законодательных актов, ужесточающих свободный доступ без регистраций на использование сетей Интернет. На наш взгляд, для эффективного противодействия преступлениям в сфере высоких технологий необходимо ввести регистрационный контроль и

учет продаваемой компьютерной техники. Этот учет можно ввести автоматически (данные компьютера могут прописываться автоматически) при использовании личного логина, при этом необходимо использовать опыт КНР [18];

– сотрудничества между государствами и частным сектором в борьбе против преступности в сфере компьютерной информации и необходимость защиты законных интересов в сфере использования и развития информационных технологий;

– принятия нового законодательства, регулирующего общественные отношения в сфере компьютерной информации для сдерживания действий, направленных против конфиденциальности, целостности и доступности компьютерных систем, сетей и компьютерных данных;

– обеспечения уголовной наказуемости деяний в сфере компьютерной информации и предоставления полномочий, достаточных для эффективной борьбы с такими уголовными преступлениями путем содействия выявлению и расследованию таких уголовных преступлений и судебному преследованию за их совершение как на внутригосударственном, так и на международном уровнях путем разработки договоренностей относительно оперативного и надежного международного сотрудничества.

Также для эффективной борьбы против преступности в сфере компьютерной информации требуется более широкое, оперативное и хорошо отлаженное межведомственное сотрудничество.

Необходимо отметить, что недостаток комплексных исследований, высокая латентность интернет-преступности в России приводят к неэффективности выработанных мер ее предупреждения, которые носят фрагментарный и противоречивый характер, предопределяя трудности в противодействии и борьбе с данным видом общественно опасных деяний. В последнее время особую тревогу вызывают бесконтрольные форумы в сетях Интернет, где на конспиративном и зашифрованном «сленге» происходит продажа различного рода препаратов (от сильнодействующих до наркосодержащих) без рецепта. Кроме того, информация о переписке и своих намерениях удаляются «безличностными» аккаунтами в короткий срок. В этом случае продавец и покупатель друг друга могут и не знать, общение на форуме безличностное, а оплата производится через электронный кошелек или другие платежные системы.

Представляется, что в новых стремительно изменяющихся реалиях необходимы системное и последовательное исследование в России как интернет-преступности в целом, так и отдельных наиболее распространенных ее видов, а также разработка эффективных мер борьбы и предупреждения преступлений в Глобальной сети, что будет способствовать развитию сетевых технологий в нашей стране. Бездействие государства в этой области, в борьбе с преступлениями в сфере высоких технологий, способствует увеличению уровня виктимности населения от этих преступлений, тем самым вызовет массовое недовольство жителей, пострадавших от киберпреступников.

Список литературы

1. URL: http://www.internetworldstats.com/top20.htm (дата обращения: 30.06.2012).

2. URL: http://www.gazeta.ru/social/news/2012/07/30/n_2460333.shtml (дата обращения: 30.07.2012).

3. URL: http://www.internetworldstats.com/top20.htm

4. Мирошников Б.Н. Сетевой фактор. Интернет и общество. Взгляд. – М.: Инфорос, 2012. – С. 16.

5. Сколько в России интернет-пользователей. – URL: http://www.r-trends.ru/trends/social/social_531.html

6. URL: http://www.internetworldstats.com/top20.htm

7. URL: http:// trustweb.ru/index.php?go=Pages&in=view&id=

8. URL: http://www.symantec.com (сообщает компания Symantec).

9. URL: http://www.sinet.ru/ (пишет компьютерная сеть Sinet).

10. URL: http://referat.ru/referats/view/29084

11. URL: http://www.lib.tsu.ru/mminfo/000063105/300%28I%29/image/300_1_151-154.pdf

12. URL: http://www.fom.ru (такие данные приводит Фонд общественного мнения).

13. Спасу нет от спама. Российские сообщения признаны самыми раздражающими. – URL: http://nikolaevsc.ru/nikolaevcy-i-gosti-pishut/spasu-net-ot-spama-rossijskie-soobshheniya-priznany-samymi-razdrazhayushhimi.html

14. URL: http://www.antichat.ru/

15. Коммерсантъ Деньги. – № 3 (860). – 23 января.

16. URL: http://burneft.ru/archive/issues/2011-06/20

17. URL: http://www.tass-ural.ru/lentanews/putin_poruchil_fsb_sformirovat_edinuyu_sistemu_obnaruzheniya_preduprezhdeniya_i_otrazheniya_kompyute.html

18. Власти КНР обязали интернет-пользователей регистрироваться в Сети под настоящими именами. –URL: http://susanin.udm.ru/news/2012/12/28/395742

В редакцию материал поступил 15.02.13

© Чирков Д.К., Саркисян А.Ж., 2013

Информация об авторах

Чирков Дмитрий Константинович, кандидат юридических наук, доцент, старший научный сотрудник НИИ Академии Генеральной прокуратуры РФ, г. Москва

Адрес: 123022, г. Москва, ул. 2-я Звенигородская, 15, тел.: (499) 256-15-65

E-mail: Dk8888@mail.ru

Саркисян Армен Жораевич, кандидат юридических наук, инспектор кафедры учебно-методической работы, Институт повышения квалификации Следственного комитета РФ, г. Москва, Россия

Адрес: 119121, 7-й Ростовский пер., 21, тел.: (499) 248-18-09

E-mail: sarkisyangp@bk.ru

Как цитировать статью: Чирков Д.К., Саркисян А.Ж. Следственно-судебные действия: проблемы регламентации // Преступность в сфере телекоммуникаций и компьютерной информации как угроза национальной безопасности страны. – 2013. – № 3(27). – С. 219–226.

D.K. CHIRKOV,

PhD (Law), associate professor, senior researcher

Scientific-Research Institute of the Academy of Prosecutor General's Office of the Russian Federation, Moscow, Russia,

A.ZH. SARKISYAN,

PhD (Law), inspector of chair of educational and methodical work

Institute of Professional Development of the Investigative Committee of the Russian Federation, Moscow, Russia

CRIMES IN THE SPHERE OF TELECOMMUNICATIONS AND COMPUTER INFORMATION AS A THREAT TO THE NATIONAL SECURITY OF THE COUNTRY

Objective: to research the criminality in the sphere of telecommunications and computer information and elaborate efficient measures of its prevention.

Methods: ascent from the abstract to the specific; systemic-structural analysis; historical method; dynamic and statistical methods, specific-sociological methodology of estimating criminality.

Results: the features of crimes in the sphere of telecommunications and computer information are shown by their public threat. Efficient preventive measures are suggested.

Scientific novelty: analysis is carried out of dynamics of crimes in the sphere of telecommunications and computer information registered in the Russian Federation, to the number of Internet users in 2009–2012. Conclusions are made that the viewed crimes are latent.

Practical value: The research results allow to trace the level of latency of such crimes, and to optimize measures for their counteraction.

Key words: high technologies in the sphere of telecommunications and computer information; crime characteristics; Internet users.

References

1. http://www.internetworldstats.com/top20.htm (accessed: 30.06.2012)
2. http://www.gazeta.ru/social/news/2012/07/30/n_2460333.shtml (accessed: 30.07.2012)
3. http://www.internetworldstats.com/top20.htm
4. Miroshnikov B.N. *Setevoi faktor. Internet i obshchestvo. Vzglyad* (Network factor. Internet and society, View). Moscow: Inforos, 2012, p. 16.
5. http://www.r-trends.ru/trends/social/social_531.html
6. http://www.internetworldstats.com/top20.htm
7. http:// trustweb.ru/index.php?go=Pages&in=view&id=
8. http://www.symantec.com
9. http://www.sinet.ru/
10. http://referat.ru/referats/view/29084
11. http://www.lib.tsu.ru/mminfo/000063105/300%28I%29/image/300_1_151-154.pdf
12. http://www.fom.ru
13. *Spasu net ot spama. Rossiiskie soobshcheniya priznany samymi razdrazhayushchimi* (There's no escaping from spam. Russian messages are voted as the most irritating), available at: http://nikolaevsc.ru/nikolaevcy-i-gosti-pishut/spasu-net-ot-spama-rossijskie-soobshheniya-priznany-samymi-razdrazhayushhimi.html
14. http://www.antichat.ru/
15. *Kommersant. Den'gi*, No. 3(860), January, 23.
16. http://burneft.ru/archive/issues/2011-06/20
17. http://www.tass-ural.ru/lentanews/putin_poruchil_fsb_sformirovat_edinuyu_sistemu_obnaruzheniya_preduprezhdeniya_i_otrazheniya_kompyute.html
18. *Vlasti KNR obyazali internet-pol'zovatelei registrirovat'sya v Seti pod nastoyashchimi imenami* (China authorities obliged Internet users to register under their true names), available at: http://susanin.udm.ru/news/2012/12/28/395742

Information about the authors

Chirkov Dmitriy Konstantinovich, PhD (Law), associate Professor, senior researcher of Scientific and Research Institute of the Academy of Prosecutor General's Office of the Russian Federation, Moscow

Address: 15 2nd Zvenigorodskaya Str., 123022, Moscow, tel.: (499) 256-15-65

E-mail: Dk8888@mail.ru

Sarkisyan Armen Zhorayevich, PhD (Law), inspector of chair of educational and methodical work, Institute of Professional Development of the Investigative Committee of the Russian Federation

Address: 21 7th Rostovskiy pereulok, 119121, tel.: (499) 248-18-09

E-mail: sarkisyangp@bk.ru

How to cite the article: Chirkov D.K., Sarkisyan A.Zh. Crimes in the sphere of telecommunications and computer information as a threat to the national security of the country, *Aktyal'nye problemy economiki i prava*, 2013, No. 3(27), pp. 219–226.

© Chirkov D.K., Sarkisyan A.Zh. , 2013

ПОЗНАНИЕ

Процессуальные, криминалистические, уголовно-правовые и криминологические проблемы ответственности за тяжкие и особо тяжкие преступления в России и Германии: материалы Международного научно-практического форума в рамках Года Германии в России 2012/13, 4–5 апреля 2013 г. / отв. ред. А.Г. Никитин, Э.Ю. Латыпова. – Казань: Изд-во «Познание» Института экономики, управления и права, 2013. – 452 с.

В сборнике представлены доклады по широкому спектру вопросов, касающихся квалификации, расследования и рассмотрения тяжких и особо тяжких преступлений в России и Германии.

Предназначен для научных и педагогических работников, практикующих юристов, аспирантов, студентов и всех интересующихся проблемами ответственности за тяжкие и особо тяжкие преступления в России и Германии.