10.7256/2073-8560.2013.01.3

Д.К. Чирков, А.Ж. Саркисян

ПРЕСТУПНОСТЬ В СФЕРЕ ВЫСОКИХ ТЕХНОЛОГИЙ: ТЕНДЕНЦИИ И ПЕРСПЕКТИВЫ

Аннотация: *в статье рассматривается общая криминологическая характеристика преступлений в сфере телекоммуникаций и компьютерной информации, дается динамика этих преступлений за период с 2009 по 2012 гг. в сравнении с числом пользователей сетей Интернет за этот же период. За последние десять лет сети Интернет, превратились в виртуальную площадку, в пространство, где люди могут выражать идеи и заниматься общественной деятельностью и т.д. В настоящее время сети Интернет, играют важную роль в сфере коммуникаций: мы проводим различные операции с денежными средствами, как с использованием компьютера, так и банкомата, и других платежных систем, прокладываем маршруты, ищем хорошие рестораны, узнаем, на какой фильм сходить,— все эти дей-ствия зависят от информационных технологий. В связи с этим, многие пользователи Интернетом, подвергаются атакам со стороны киберпре-ступников. Вышеуказанные проблемы затронуты автором в статье. Работа будет полезна для сотрудников правоохранительных органов занимающихся противодействиям преступлениям в сфере высоких технологий.*

Ключевые слова: *высокие технологии, в сфере телекоммуникаций и компьютерной информации, характеристика преступлений, Интернет пользователи.*

Современные достижения в области телекоммуникаций и повседневное массовое внедрение цифровых технологий во все сферы человеческой жизни в конце XX – начале XXI вв. предопределило возникновение новых угроз и рисков в сфере общественных отношений.

В настоящее время наибольшую значимость и распространенность имеет технология Интернет, которая соединила людей по всему земному шару, сделала коммуникации дешевыми и беспрепятственными и открыла новые горизонты для всего мирового сообщества. Интернет в последнее время дал человеку безграничные возможности в области передачи, распространения и рассылки информации, позволил выполнять финансово-банковские операции, несмотря на расстояния и границы. Получив очевидные преимущества сети Интернет, общество столкнулось с новыми видами и способами совершения преступлений, с преступлениями в сфере высоких технологий. При этом Интернет, с одной стороны, позволил более эффективно и безнаказанно совершать ранее существовавшие традиционные преступления, с другой – породил новые, неизвестные еще совсем недавно мировому сообществу виды общественно опасных посягательств.

За последние десять лет (с 2003 по 2012 гг.) количество пользователей Интернетом в России выросло приблизительно в 5,4 раз (2003 г. – 12 млн., 2010 г. – 59.7 млн. (43% всего населения), 2012 г. – 68,0 млн. (48% всего населения)[1]. За период с 2010г. по 2012 г. количество пользователей увеличилось на 8,3 млн. чел., а в 2014 году 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.

[1] http://www.internetworldstats.com/top20.htm – 30.06.2012.

[2] http://www.gazeta.ru/social/news/2012/07/30/n_2460333.shtml – Газета.ru 30/07/2012

20 стран с самым высоким числом Интернет пользователей[3]

ТОП-20 СТРАНЫ С НАИБОЛЬШИМ КОЛИЧЕСТВОМ ПОЛЬЗОВАТЕЛЕЙ ИНТЕРНЕТА – 30 ИЮНЯ 2012 ГОДА						
#	Страна или Регион	Населения, 2012 Est	Интернет-пользователей Год 2000	Интернет-пользователей Последние Данные	Проникновение (% Населения)	Пользователи % 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 %	**100.0 %**

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

За последние десять лет сети Интернет, превратились в виртуальную площадку, в пространство, где люди могут выражать идеи и заниматься общественной деятельностью и т.д. В настоящее время сети Интернет, играют важную роль в сфере коммуникаций: мы проводим различные операции с денежными средствами, как с использованием компьютера, так и банкомата, и других платежных систем, прокладываем маршруты, ищем хорошие рестораны, узнаем, на какой фильм сходить,— все эти действия зависят от информационных технологий. В связи с этим, многие пользователи Интернетом, подвергаются атакам со стороны киберпреступников[4].

[3] http://www.internetworldstats.com/top20.htm

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

10.7256/2073-8560.2013.01.3

В российском законодательстве кроме главы 28 Уголовного кодекса Российской Федерации, предусматривающей ответственность за преступления в сфере компьютерной информации, нет иных норм, предусматривающих ответственность за незаконные действия в сфере телекоммуникаций и компьютерной информации, нет соответственно и понятий, определяющих либо регламентирующих незаконные преступные деяния, совершаемые с помощью высоких технологий.

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 (Глава 28 УК РФ) выросло более чем в 300 раз и достигло около 10214 преступлений за год.

В 2012 г. число зарегистрированных преступлений *в сфере телекоммуникаций и компьютерной информации* составило 10 227 преступлений, что на 28,3 % выше показателя 2011 г. (7 974 эпизода). В 2011 г. число аналогичных посягательств составило – 7 142 преступления, что на 37,2 % меньше, чем в 2010 г. (12 698 эпизода). 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 преступлений) (см. табл. 1).

Из представленной таблицы прослеживается тенденция снижения количества зарегистрированных преступлений, зафиксированная в 2009 – 2011 гг., вряд ли адекватно отражает реальную динамику фактической преступности. На наш взгляд, подобные процессы могут быть объяснены, с одной стороны, проводимой реформой в органах внутренних дел и ослаблением контроля учетно-регистрационной дисциплины, с другой стороны – 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 2011г.(60,4).

Это обстоятельство дает основание нам полагать, что отмечаемое сокращение количества зарегистрированных преступлений в 2009-2011гг носит искусственный характер. Об этом свидетельствует выше таблица 1, динамики зарегистрированных в Российской Федерации преступлений, совершенных в сфере телекоммуникаций и компьютерной информации, и число пользователей Интернетом в течении 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

Таблица 1

Динамика преступлений, совершенных в сфере телекоммуникаций и компьютерной информации, зарегистрированных в Российской Федерации, и число пользователей Интернетом в течении 2009 – 2012 гг.[5]

	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.)[6]	53,5	59,7	60,4	68,0

[5] Статистические данные: Форма № 615 ГИАЦ МВД России № 615

[6] *Мирошников Б.Н.* Сетевой фактор. Интернет и общество. Взгляд. – М.: Инфорос, 2012. С.16; http://www.r-trends.ru/trends/social/social_531.html – Сколько в России интернет-пользователей. 05.05.2012; http://www.internetworldstats.com/top20.htm

граждан… . Эта устойчивая тенденция, причем, очевидно, что рост обращений серьезно отстает от реального роста количества преступлений»[7].

Нельзя не говорить о латентности данного вида преступлений. По оценкам экспертов, латентность «компьютерных» преступлений в США достигает 80%, в Великобритании — до 85%, в ФРГ — 75%, в России — более 90%.[8]

Жертвы редко обращаются в полицию. 1/4 пользователей сети утверждают, что не предпримут никаких действий, став жертвами кибератаки.[9] 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.[10]

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. долларов ежегодно в мире. Банковский грабитель рискует жизнью за 10 тыс. долларов, а хакер[11], манипулируя компьютером и ничем не рискуя, может получить 1 млн.[12] В России средний ущерб, причиняемый потерпевшему от одного совершаемого преступления в сфере телекоммуникаций и компьютерной информации равен 1,7 млн. рублей.[13]

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. около полутора миллиарда и продолжает в наши дни стремительно 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 года. 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.[14] Российская Федерация в настоящей Конвенции не участвует.

Преступления, совершенные в сфере телекоммуникаций и компьютерной информации, кроме главы 28 УК РФ, по нашему мнению не целесообразно относить к видам преступления, а скорее способа 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 это, безусловно. Поэтому, изучение и анализ криминологической характеристики данным преступлениям весьма актуален и необходим на сегодняшний день.

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 находится в положении анонимности. Часто преступления в данной сфере, совершаются организованными группами, что характерно для киберпреступников.

Основными причинами совершения киберпреступности в России, является: недостаточно развитое законодательство, регулирующее общественные от-

---

[7] *Мирошников Б.Н.* Сетевой фактор. Интернет и общество. Взгляд. – М.: Инфорос, 2012. С.78-79.

[8] http://trustweb.ru/index.php?go=Pages&in=view&id=

[9] http://www.symantec.com (сообщает компания Symantec).

[10] http://www.sinet.ru/ (пишет компьютерная сеть Sinet).

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

[12] http://referat.ru/referats/view/29084

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

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

10.7256/2073-8560.2013.01.3

ношения 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.[15]

По сравнению с другими странами, в России хакеры самые богатые в мире. Оборот рынка компьютерных преступлений достигает 1 миллиард долларов в год[16]. Умелому хакеру кибератаки приносят от 30 до 900 млн. рублей в месяц. Самым прибыльными операциями хакера являются рассылка спама, кража конфиденциальной информации и Ddos атаки,[17] блокирующие работу сайта. Число вредоносных программ возросло на 1/3 по сравнению с прошлым годом и составило свыше миллиона. Интернет пользователей становились жертвами кибератак. В прошлом году на каждого жителя планеты пришлось по 5000 спам писем, многие из них содержали вредоносные программы для взлома счетов.[18] 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., за Ddos атаки 300-400 долл.[19] В Америке аналогичные услуги стоят в 5 раз дороже.

Такими услугами в большинстве случаев пользуются преступники. Так например, полицейские-борцы с киберпреступностью рассказывают, 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.[20]

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.[21]

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

[15] http://www.fom.ru (такие данные приводит Фонд общественного мнения).

[16] Такие данные приводит «Letogroup».

[17] DDoS-атака (сокр. от англ. Distributed Denial of Service) — атака на компьютерную систему с целью довести её до отказа, то есть, до такого состояния, что правомочные пользователи системы не могут получить доступ к предоставляемым системой ресурсам (серверам, сервисам), либо этот доступ затруднён.

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

[19] http://www.antichat.ru/

[20] Журнал «Коммерсантъ Деньги», №3 (860), 23.01.2012

[21] Журнал «Коммерсантъ Деньги», №3 (860), 23.01.2012

дистанционного изменения технологических температурных режимов ректификационного оборудования по сети Интернет.

Еще из множестванедавних и наиболее потенциально опасных подозрительных инцидентов одним примеров является, одновременное нарушение 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.[22]

На основании вышеизложенного, можно сделать выводы, о существовании 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 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 автоматический (данные компьютера могут прописываться автоматически) при использовании личного логина, при этом необходимо использовать опыт КНР[23];

– 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 вызывает 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 через электронный кошелек или другие платежные системы.

Представляется, что в новых стремительно изменяющихся современных реалиях необходимы системное и последовательное исследование в России Интернет преступности как в целом, так и отдельных наиболее распространенных ее видов, 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.

[22] http://burneft.ru/archive/issues/2011-06/20

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

10.7256/2073-8560.2013.01.3

Библиография:

1. Мирошников Б.Н. Сетевой фактор. Интернет и общество. Взгляд. – М.: Инфорос, 2012.
2. http://trustweb.ru/index php?go=Pages&in=view&id=
3. http://www.symantec.com (сообщает компания Symantec).
4. http://nikolaevsc.ru/nikolaevcy-i-gosti-pishut/spasu-net-ot-spama-rossijskie-soobshheniya-priznany-samymi-razdrazhayushhimi.html – Спасу нет от спама. Российские сообщения признаны самыми раздражающими.
5. Журнал «Коммерсантъ Деньги», №3 (860), 23.01.2012
6. http://susanin.udm.ru/news/2012/12/28/395742 – Власти КНР обязали интернет-пользователей регистрироваться в Сети под настоящими именами

References (transliteration):

1. Miroshnikov B.N. Setevoy faktor. Internet i ob-shchestvo. Vzglyad. – M.: Inforos, 2012.