КРИМИНОЛОГИЯ ИНТЕРНЕТ-ПРОСТРАНСТВА

УДК 343.9
ББК 67.51

В.А. Номоконов*, ***Т.Л. Тропина*****

КИБЕРПРЕСТУПНОСТЬ КАК НОВАЯ КРИМИНАЛЬНАЯ УГРОЗА

Аннотация: Киберпреступность — 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 и компьютерных данных.

Ключевые слова: киберпреступность; компьютерная преступность; Интернет.

V.A. Nomokonov , T.L. Tropina

CYBERCRIME AS A NEW CRIMINAL THREAT

Summary: Cybercrime is a number of crimes committed in cyberspace through computer systems or networks and other means of access to cyberspace within the bounds of computer systems and networks or against computer systems, networks and computer data.

Key words: cybercrime; computer crime; Internet.

1. Понятие и виды киберпреступности

Процессы глобализации, в том числе глобализации информационных технологий, предоставляют неограниченные возможности для оказания воздействия на личность и общество. Одним из негативных последствий развития информационных технологий является появление и развитие новой формы преступности — преступности в сфере высоких технологий, когда компьютеры или компьютерные сети выступают в качестве объекта преступных посягательств, а также средства или способа совершения преступлений. Проблема т.н. киберпреступности актуализировалась в эпоху информационного общества, когда компьютеры и телекоммуникационные системы охватили все сферы жизнедеятельности человека и государства, а глобальная сеть Интернет является одной из наиболее быстрых областей развития телекоммуникационных технологий.

Сегодня жертвами преступников, орудующих в виртуальном пространстве, могут стать не только люди, но и целые государства. При этом безопасность тысяч пользователей может оказаться в зависимости от нескольких преступников. Количество преступлений, совершаемых в киберпространстве, растёт пропорционально числу пользователей компьютерных сетей. Сайт Internet Complain Center (IC3), созданный в мае 2000 года для регистрации заявлений пользователей сети Интернет о совершённых в отношении них киберпреступлениях, 11 июня 2007 года получил миллионную жалобу об интернет-преступлении. Растущий профессионализм киберпреступников и постоянное совершенствование информационных технологий, и, как следствие, постоянная эволюция возможностей для совершения

*** Виталий Анатольевич Номоконов** — доктор юридических наук, профессор кафедры уголовного права и криминологии Дальневосточного федерального университета (Владивосток, Россия). E-mail: nomokonov@rambler.ru.

**** Татьяна Львовна Тропина** — кандидат юридических наук, научный сотрудник Института зарубежного и международного уголовного права Макса Планка (Фрайбург, Германия). E-mail: tatiana.tropina@gmail.com.

преступлений, создают новые угрозы для пользователей глобальных информационных сетей.

Проблема использования достижений науки и техники в преступных целях связана с одним из наиболее важных направлений интегративных процессов — созданием интернациональной по сути и глобальной по форме сети Интернет, объединившей миллионы компьютеров, расположенных в разных точках Земли. Всемирная сеть Интернет, открывшая широчайшие возможности для получения информации и обмена ею, развивается очень быстрыми темпами. В конце 1990-х, по некоторым прогнозам, ожидалось, что в 2005 году около 1 млрд. компьютеров во всем мире будут подключены к Интернету, и это казалось действительно большой цифрой. Однако результаты даже превзошли ожидания — в 2008 году количество пользователей сети Интернет составило 1,5 млрд. человек — это почти четверть населения Земли, а в 2013-м выход в виртуальное пространство получит уже почти треть землян (2,2 миллиарда).[1]

Стремительное развитие компьютерных сетей и проникновение их в различные сферы человеческой деятельности, как уже было сказано, изменило характер преступных посягательств и породило новые их формы. При этом от того, в какие именно сферы деятельности проникали сети, зависели наиболее актуальные угрозы на текущий момент времени. Так, в 60-х годах XX века, когда компьютерные сети использовались в основном в военных и научных учреждениях, основной опасностью считалась утрата секретной информации, а также несанкционированный доступ к ней. В 70-е годы на первый план вышли проблемы экономической преступности в сфере компьютерных технологий — взломы банковских компьютерных сетей, промышленный шпионаж. В 80-х годах широко распространенными преступлениями стали взломы и незаконное распространение компьютерных программ. С появлением и развитием в 90-х годах сети Интернет появился целый спектр проблем, связанных с преступными посягательствами на секретность частной информации, распространением в сетях детской порнографии, функционированием виртуальных сетевых сообществ экстремистской направленности.[2] В 2005—2008 гг. появились новые угрозы, связанные с распространением сетей так называемых «ботов» — заражённых компьютеров, которые без ведома пользователей способны совершать атаки. Кроме того, интеграция телекоммуникационных сетей и их конвергенция, появление возможности «мобильного» доступа в Интернет и всё большее совершенствование устройств доступа к сети, в том числе «портативных» мобильных телефонов, коммуникаторов, создаёт новые возможности для злоупотребления информационными технологиями.

Для большинства преступлений, совершаемых в глобальных компьютерных сетях, характерны следующие особенности:

1) Повышенная скрытность совершения преступления, обеспечиваемая спецификой сетевого информационного пространства (развитые механизмы анонимности, сложность инфраструктуры и т.п.).

2) Трансграничный характер сетевых преступлений, при котором преступник, объект преступного посягательства, потерпевший могут находиться на территориях разных государств.

3) Особая подготовленность преступников, интеллектуальный характер преступной деятельности.

4) Нестандартность, сложность, многообразие и частое обновление способов совершения преступлений и применяемых специальных средств.

5) Возможность совершения преступления в автоматизированном режиме в нескольких местах одновременно. Возможность объединять относительно слабые ресурсы многих отдельных компьютеров в мощное орудие совершения преступления.

[1] World Internet Usage. URL: http://www.internetworldstats.com/stats.htm (дата обращения: 31.10.2011).

[2] Подробнее см. *Бондаренко С.В.* Виртуальные сетевые сообщества девиантного поведения. URL: http: // www. cyberpolitics.ru/ content/view/ 256/34/ (дата обращения: 31.10.2011).

6) Многоэпизодный характер преступных действий при множественности потерпевших.

7) Неосведомленность потерпевших о том, что они подверглись преступному воздействию.

8) Дистанционный характер преступных действий в условиях отсутствия физического контакта преступника и потерпевшего.

9) Невозможность предотвращения и пресечения преступлений данного вида традиционными средствами.[3]

Термин «киберпреступность» в настоящее время часто употребляется наряду с термином «компьютерная преступность», причём нередко эти понятия используются как синонимы.

В русскоязычной литературе наибольшее предпочтение отдаётся понятию «компьютерная преступность». Возможно, это обусловлено тем, что в основном исследования ведутся в криминалистической или процессуальной плоскостях. Кроме того, единственная глава в Уголовном кодексе РФ, предусматривающая ответственность за преступления, объектом которых являются информация и информационные системы, называется «Преступления в сфере компьютерной информации».

Действительно, эти термины очень близки друг другу, но всё-таки не синонимичны. На наш взгляд, понятие «киберпреступность» (в англоязычном варианте — cybercrime) шире, чем «компьютерная преступность» (computer crime), и более точно отражает природу такого явления, как преступность в информационном пространстве. Так, Оксфордский толковый словарь определяет приставку «cyber-» как компонент сложного слова. Её значение — «относящийся к информационным технологиям, сети Интернет, виртуальной реальности».[4] Практически такое же определение даёт Кембриджский словарь: приставка «cyber-» означает «включающий в себя использование компьютеров или относящийся к компьютерам, *особенно к сети Интернет*». При этом в качестве примера Кембриджский словарь приводит слово «cybercrime» — киберпреступность (киберпреступление).[5] Таким образом, «cybercrime» — это преступность, связанная как с использованием компьютеров, так и с использованием информационных технологий и глобальных сетей. В то же время термин «computer crime» относится только к преступлениям, совершаемым против компьютеров или компьютерных данных.

Глобальное информационное пространство, информационная мегасреда нематериальны и по сути своей несводимы к физическому носителю, в котором воплощены. Поэтому термин «компьютерная преступность» всё-таки несколько уже по своей смысловой нагрузке, и сводит суть явления к преступлениям, совершённым 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. Более того, с развитием 3G сетей мобильные телефоны способны подключаться к глобальной сети по технологии HSPDA (сеть четвёртого поколения) или UMTS (сеть третьего поколения), что по скорости не намного уступает возможностям подключения к сети Интернет с помощью обычного компьютера, а в перспективе и превышает их. Телекоммуникационные инфраструктуры приспосабливаются к тому, чтобы максимально способствовать перемещению гигантских объёмов информации в самой удобной для потребителя форме.[6] Можно только гадать, какие коммуникационные решения будут предложены пользователям мобильной связи и Интернет в течение ближайшего десятилетия.

По пути разделения терминов «киберпреступность» и «компьютерная преступность» и использованию именно первого

[3] *Осипенко А.Л.* Сетевая компьютерная преступность. — Омск, 2009. — С. 109—110.

[4] Oxford English Dictionary [Electronic recourse]. URL: http:/ /www. askoxford.com/ (дата обращения: 31.10.2011).

[5] Cambridge Advanced Learner's Dictionary [Electronic recourse]. URL: http: // dictionary. cambridge. org (дата обращения: 31.10.2011).

[6] Подробнее см.: *Кашлев Ю.Б.* Становление глобального информационного общества и место России // Информация. Дипломатия. Психология. — М., 2002. — С. 18—20.

термина идёт также международное законодательство. Совет Европы в ноябре 2001 года принял Конвенцию о киберпреступности, употребив именно термин «cybercrime», а не «computer crime».

Киберпреступность — это преступность в так называемом киберпространстве. Для того чтобы дать определение киберпреступности, необходимо прежде всего осмыслить такое понятие, как «киберпространство».

Авторы «модельного закона» о киберпреступности Международного Союза Электросвязи (2009 г.)[7] определяют киберпространство как «физическое и нефизическое 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, поскольку справочник был подготовлен под эгидой проекта ООН о киберпреступности, это определение можно считать наиболее официальным определением киберпространства для целей разработки уголовного законодательства.

Киберпреступность — 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 и компьютерных данных.

Это определение соответствует рекомендациям экспертов ООН. По их мнению, термин «киберпреступность» охватывает любое преступление, которое может совершаться с помощью компьютерной системы или сети, в рамках компьютерной системы или сети или против компьютерной системы или сети. Таким образом, к киберпреступлениям может быть отнесено любое преступление, совершённое в электронной среде.[8]

Приведённое определение распространяется на все виды преступлений, совершённых 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.[9]

Как соотносятся понятия «киберпреступность» и «компьютерные преступления»? Выше нами уже были приведены определения этих категорий специалистами ООН. Термин «киберпреступление» охватывает весь спектр преступлений в сфере информационных технологий, будь это преступления, совершённые с помощью компьютеров, или преступления, предметом которых являются компьютеры, компьютерные сети и хранящаяся на этих носителях информация. Компьютерное преступление — это только такое преступление, которое посягает на безопасное функционирование компьютеров и компьютерных сетей, а также на обрабатываемые ими данные. Таким образом, компьютерное преступление — разновидность киберпреступления.[10]

Виды киберпреступлений. Киберпреступления подразделяют на виды в зависимости от объекта, от предмета посягательства, в зависимости от способов совершения и т.п.

По объекту посягательства выделяются следующие группы киберпреступлений: экономические компьютерные преступления, компьютерные преступления против личных прав и неприкосновенности частной сферы, компьютерные преступления против общественных и государственных интересов.[11]

---

[7] ITU Toolkit For Cybercrime Legislation. ITU, 2009.

[8] Преступления, связанные с использованием компьютерной сети [Электронный ресурс] // Десятый конгресс ООН по предупреждению преступности и обращению с правонарушителями //A/CONF.187/10. URL: http: // www. un.org/ russian/ topics/crime/ docs10.htm (дата обращения: 31.10.2011).

[9] *Щетилов А.* Некоторые проблемы борьбы с киберпреступностью и кибертерроризмом // Информатизация и информационная безопасность правоохранительных органов. XI межд. конф. — М., 2002. — С. 187.

[10] См. подробнее: *Тропина Т.Л.* Киберпреступность. — Владивосток, 2009.

[11] См., напр.: *Бекряшев А.К., Белозеров И.П.* Теневая экономика и экономическая преступность / Электронный учебник. 2000.

По характеру использования компьютеров или компьютерных систем можно выделить три вида киберпреступлений: деяния, где компьютеры являются предметами преступлений (похищение информации, несанкционированный доступ, уничтожение или повреждение файлов и устройств и т.п.); действия, где компьютеры используются как орудия преступления (электронные хищения и т.п.); преступления, где компьютеры играют роль интеллектуальных средств (например, размещение в Интернете порносайтов).[12]

Самый распространённый способ — это подразделение на компьютерные преступления и преступления, совершаемые с помощью или посредством компьютеров, компьютерных сетей и иных устройств доступа к киберпространству. Эту классификацию использует ООН, подразделяя этот вид преступной деятельности на киберпреступления в «широком» и «узком» смысле.

Конвенция Совета Европы о киберпреступности изначально подразделяла киберпреступления на четыре группы (потом был принят дополнительный протокол, и теперь групп — пять), выделяя в первую группу «компьютерные преступления», называя их *преступлениями против конфиденциальности, целостности и доступности компьютерных данных и систем:*

• **незаконный доступ** — *ст. 2* (противоправный умышленный доступ к компьютерной системе либо её части);

• **незаконный перехват** — *ст. 3* (противоправный умышленный перехват не предназначенных для общественности передач компьютерных данных на компьютерную систему, с неё либо в её пределах);

• **вмешательство в данные** — *ст. 4* (противоправное повреждение, удаление, нарушение, изменение либо пресечение компьютерных данных);

• **вмешательство в систему** — *ст. 5* (серьёзное противоправное препятствование функционированию компьютерной системы путём ввода, передачи, повреждения, удаления, нарушения, изменения либо пресечения компьютерных данных).

Во вторую группу входят преступления, связанные с использованием компьютерных средств. Подлог с использованием компьютерных технологий Конвенция определяет как ввод, изменение, уничтожение или блокирование компьютерных данных, влекущие за собой нарушение аутентичности данных с намерением, чтобы они рассматривались или использовались в юридических целях в качестве аутентичных, независимо от того, поддаются ли эти данные непосредственному прочтению и являются ли они понятными. Мошенничество в киберпространстве, согласно Конвенции — это лишение другого лица его собственности путём любого ввода, изменения, удаления или блокирования компьютерных данных или любого вмешательства в функционирование компьютерной системы, с мошенническим или бесчестным намерением неправомерного извлечения экономической выгоды для себя или третьих лиц.

Третью группу составляют преступления, связанные с контентом (содержанием данных). Речь идёт о детской порнографии, причём в Конвенции достаточно подробно разъясняется, какие именно действия по распространению детской порнографии должны преследоваться.

В эту группу входят преступления, связанные с контентом — то есть с содержанием данных, размещённых в компьютерных сетях. Самый распространённый и наказуемый практически во всех государствах вид этих киберпреступлений — преступления, связанные с детской порнографией.

Детская порнография обычно считается тяжким преступлением, даже если лица, вовлечённые в её производство, не имели никакого физического контакта с детьми. Причиной этого является то, что для производства подобных порнографических материалов требуется сексуальная эксплуатация детей. Кроме того, потребители этих материалов зачастую не ограничиваются интересом к картинкам и сексуальными фантазиями, но и практикуют или стремятся практиковать педофилию в ре-

[12] Ю.М. Батурин и А.М. Жодзишский выделяют две группы компьютерных преступлений — связанные с вмешательством в работу компьютеров и использующие компьютеры как необходимые технические средства. См.: *Батурин Ю.М., Жодзишский А.М.* Компьютерная преступность и компьютерная безопасность. — М., 1991. — С. 11.

альной жизни, то есть имеют устойчивую асоциальную установку, что, безусловно, повышает общественную опасность этих деяний.

В четвёртую группу вошли преступления, связанные с нарушением авторского права и смежных прав. Виды таких преступлений в Конвенции не выделяются: установление таких правонарушений отнесено документом к компетенции национальных законодательств государств.

Пятая группа — преступления, посягающие на общественную безопасность. К этой категории относятся такие деяния, как кибертерроризм и использование киберпространства в террористических целях (например, вовлечение в совершение преступлений террористического характера или иное содействие их совершению). Глобализация информационных процессов обусловила появление новой формы терроризма — кибертерроризма. Кибертерроризм можно отнести к так называемым технологическим видам терроризма. В отличие от традиционного, этот вид терроризма использует в террористических акциях новейшие достижения науки и техники в области компьютерных и информационных технологий, радиоэлектроники, генной инженерии, иммунологии.

В 2007—2008 гг. экспертами Международного союза электросвязи с учётом новых деяний, появившихся в последние годы, также подготовлено несколько видов классификаций киберпреступлений, например, «Модельный закон» ITU содержит, помимо традиционно известной классификации, предложенной Конвенцией Совета Европы, также такие виды преступлений, как кибертерроризм — однако, они отнесены к подвидам других преступлений, например, к «неуполномоченному доступу» (неуполномоченный доступ с целью совершения террористических действий»).

2. Состояние, структура и динамика киберпреступности

Киберпреступность — явление по своей природе трансграничное. Поэтому анализ киберпреступности или её 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 имён, адресов, паролей и т.п.) создаёт ситуации, когда преступник находится на одном континенте, преступление непосредственно совершается на другом, а последствия преступления наступают на третьем. Более, того, в 2005—2009 гг. в связи с появлением возможности создания сети ботов — инфицированных компьютеров, проводящих атаки независимо от пользователей, ситуация усложнилась ещё больше: преступник, атакующий компьютер и потерпевший от преступления могут находиться в разных странах. Более того, сети «ботов» могут использоваться как прокси-серверы при совершении интернет-преступлений, поддерживающие анонимность преступника и затрудняющие его идентификацию. И если технически ещё возможно проследить «цепь» прокси и установить атакующий компьютер, то с точки зрения процессуальных действий по сбору доказательств, если компьютеры находились в разных странах, задача правоохранительных органов осложняется необходимостью делать официальные запросы в другие государства.

Авторами данной работы с 2001 года ведётся сбор информации о состоянии киберпреступности. За прошедшие одиннадцать лет эксперты остались единодушны: в настоящее время не существует ни релевантной статистики, отражающей реальную картину состояния киберпреступности, ни надёжных методов сбора таких данных.[13] 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, например, до какой степени достоверна статистика об экономических потерях в результате киберпреступности.

[13] *Gercke, M.* Understanding Cybercrime: A Guide for Developing Countries. ITU, 2009.

По некоторым данным, ежегодные потери от киберпреступности в мире составляют примерно 750 млрд. — 1 трлн. долларов. Растут и доходы преступников. С 2004 по 2009 год доходы от киберпреступности возросли в десять раз, до 1 трлн. долларов.[14]

Наибольшая часть киберпреступности остаётся за рамками статистики — можно с уверенностью утверждать, что в официальную статистику попадает лишь десять, в лучшем случае двадцать процентов совершённых деяний. По некоторым оценкам, латентность киберпреступности в России составляет более 90 %, в США — 80 %, в Великобритании — до 85 %, в ФРГ — 75 %.[15]

Структура киберпреступности. Она различается заметно в разных странах в зависимости, прежде всего, от характера и степени развития информационных технологий, погружённости пользователей в Интернет и т.п. Структура киберпреступности, например, в США, выглядит следующим образом. По данным одного из изучений, 44 % составили кражи денег с электронных счетов, 16 % — повреждения программного обеспечения, столько же — похищение секретной информации, 12% — фальсификация информации, 10 % — заказ услуг за чужой счёт.[16]

Проблема киберпреступности также 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 телекоммуникационых сетей, которые не могут выдержать подобной нагрузки. Структура и динамика киберпреступности, а также её масштабы зависят от культуры кибербезопасности пользователей в отдельном государстве, что также имеет разные аспекты в зависимости от степени развития экономики той или иной страны.

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 «облегчили» 130 банкоматов в 49 городах Америки. При этом вся операция заняла у злодеев не более 30 минут, а общий куш составил около 9 млн. долларов, которые затем были переведены на счета в различные государства.

Недавние тенденции, отмеченные экспертами ООН и МСЭ в 2008 году, говорят об изменении структуры наиболее распространённых посягательств, что связано с развитием телекоммуникационных технологий и ростом количества пользователей сети Интернет. Можно привести десять наиболее опасных угроз, отмечаемых специалистами: сети ботов; «целенаправленные» атаки на правительственные сайты, частные предприятия, и конечных пользователей; финансовое мошенничество, потерпевшими от которого являются банки, частные предприятия и конечные пользователи; мошенничество с удостоверением личности; спам и фишинг; шпионаж — экономический и в государственных органах; Web-атаки; социальные сети; неправильное или злонамеренное использование внутренних сетевых ресурсов; вирусы и черви.[17]

К 2011 году в связи с развитием информационных технологий и ростом количества пользователей сети Интернет появились новые возможности использования киберпространства в целях совершения преступлений. Основные тенденции, которые, как отмечается, будут представлять наибольшую угрозу: рост количества пользователей социальных сетей (таких, как MySpace, Facebook и прочих), сервисы по определению местонахождения (так называемые geo-location services), рост популярности доступа в Интернет с мобильных телефонов, и, как следствие, эксплуатация преступниками «брешей» в программном

[14] См. напр.: www.crime-research.ru (дата обращения: 31.10.2011).

[15] *Kabay M.* Studies and Surveys of Computer Crime. — Northfield, 2001. — P. 2.

[16] *Селико Ю., Прохоров А.* Internet — отмычка для компьютера // Компьютер-пресс. — 2002. — № 3. — С. 38.

[17] *Ifrah, L.* Cybercrime: current threats and Trends. COE, 2008.

обеспечении мобильных устройств, рост использования прикладного программного обеспечения для смартфонов и портативных устройств, и невозможность обеспечить надежность источников их разработки, а также эксплуатация уязвимостей в этом программном обеспечении.[18]

Фишинг. Слово «фишинг» происходит от английского термина phishing (искаженное fishing — рыбалка). Этим термином называют мошенничество, в ходе которого злоумышленники заманивают доверчивых пользователей на свои сайты, замаскированные под сайты заслуживающих доверия организаций, например, банков, и выведывают у них персональные данные, включая номера счетов и кредитных карт. Чтобы заманить пользователя на такой сайт, ему отправляют письмо с поддельным обратным адресом с просьбой подтвердить или заново сообщить какую-либо информацию, перейдя по указанной в письме ссылке. Эта ссылка часто очень похожа на ссылку на настоящий сайт банка, но ведёт прямо в логово мошенников.

Спам. По оценкам ведущих компаний-производителей антивирусных программ, около 87 % от всех электронных писем, отправленных в 2009 году, являлись спамом, а в некоторые месяцы этот показатель зашкаливал за 95 %. В 2008 году виртуального мусора было меньше — ему принадлежали лишь около 70 % общего объёма электронной корреспонденции. В целом за 2009 год количество отправленных сообщений, содержащих спам, перевалило за 40 триллионов. Таким образом, на каждого жителя Земли (включая младенцев и неподключенных к Сети) в среднем пришлось около 5 тысяч подобных писем.[19]

В России в последнее время количество компьютерных преступлений неуклонно увеличивается, возрастает их удельный вес по размерам похищаемых сумм и другим видам ущерба в общей доле материальных потерь от обычных видов преступлений. По данным Министерства внутренних дел РФ, в 2009 году россияне совершили более 17,5 тысяч компьютерных преступлений, что на четверть больше чем в 2008 году. Правда, в 2010 году было зарегистрировано лишь 7398 преступлений в сфере компьютерной информации.

По мнению авторов, официальная статистика о компьютерных преступлениях в России весьма мало информативна, поскольку с учётом того, что с 1996 года не менялось законодательство о киберпреступлениях, а также высокой латентности подобных деяний, оперировать официальными статистическими данными и говорить о том, что количество киберпреступлений удвоилось или утроилось — совершенно бессмысленно.

Как показал специальный анализ преступлений, совершённых хакерами-гражданами РФ на территории России, финансовые показатели преступников в 2010 г. составили 1,3 млрд. долларов. В 2011 году российские хакеры заработают около 3,7 млрд., а в 2013 г. удвоят данный показатель. При обзоре актуальных услуг и типовых цен на них, существующие 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 платёжных поручений с целью хищения денежных средств; спам — массовая рассылка нежелательных сообщений электронной почты; продажа трафика — услуги по установке программ на большое количество компьютеров и услуги по перенаправлению посетителей на определённые веб-сайты (услуга относится к внутреннему рынку киберпреступности); партнёрские программы — нелегальная продажа медикаментов, продажа контрафактного ПО, загрузок и т.п. (услуга относится к внутреннему рынку киберпреступности).[20]

Сегодня практически все исследователи и специалисты признают, что ситу-

[18] McAfee, 2011 Threats Predictions. Available. URL: http://www.mcafee.com/us/resources/reports/rp-threat-predictions-2011.pdf (дата обращения: 31.10.2011).

[19] См.: Воры в паутине. URL: http://www.tribuna.ru (дата обращения: 31.09.2011).

[20] За 2010 г. русские хакеры заработали около $2,5 млрд. URL: http: // www. cnews.ru /news/line/index.shtm l?2011/03/28/ 433836 (дата обращения: 31.09.2011).

ация с киберпреступностью пока имеет тенденцию к ухудшению. Ещё одна опасная тенденция — всё большая связь 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.

Более того, в течение последних лет отмечается «профессионализация» киберпреступности: не только компьютерные атаки становятся всё 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.[21]

Еще одна тенденция — использование сети Интернет организованными преступными группами для *отмывания денег*. Интернет представляет огромные возможности для махинации со счетами. Он-лайн аукционы позволяют произвести перемещение денег в связи с якобы легальными поставками, развитие электронных платежей и он-лайн банков предоставляет множество способов скрыть движение преступных доходов и производить незаконные сделки.

3. Особенности борьбы с киберпреступностью

Как уже указывалось выше, киберпреступность имеет по определению транснациональный характер. Борьба же с преступностью в области международных компьютерных сетей усложняется, по оценкам экспертов ООН, по трём основным причинам. 1) Для расследования преступлений в электронной среде требуются специальные знания и опыт. 2) Интернет представляет собой открытую среду, дающую пользователям возможности совершать определённые действия за пределами границ государства, в котором они находятся. В то же время следственные действия правоохранительных органов в целом ограничиваются пределами собственного государства. 3) Открытые структуры международных компьютерных сетей позволяют пользователям выбирать такую правовую среду, которая оптимальным образом соответствует их целям. Т.е. пользователи могут выбирать такие страны, в которых определённые деяния, совершаемые в электронной среде, не влекут за собой уголовную ответственность. Наличие подобных «информационных убежищ» может сдерживать усилия других государств по борьбе с преступностью с использованием компьютерных сетей.[22]

Анализ показывает, что в решении проблемы предупреждения преступлений в киберпространстве наибольшую отдачу могут дать технологический, организационный и правовой подходы. Первый предусматривает предотвращение преступлений главным образом за счёт мероприятий технического характера. Второй связан с осуществлением разнообразных организационных мероприятий. Третий опирается на совершенствование правовых механизмов: улучшение правовой базы борьбы с данным видом преступлений, оптимальное решение проблем криминализации общественно опасных деяний, закрепление процессуальных механизмов и т.п. Практика показала бесполезность попыток обеспечения безопасности компьютерных сетей исключительно за счёт защитных организационно-технических мероприятий.

Для борьбы с угрозой киберпреступности, которая, безусловно, будет расти с дальнейшим расширением сферы использования информационных технологий, предоставляя всё большие возможности

[21] URL: BSI, Die Lage der IT-Sicherheit in Deutschland 2011, S. 4, available at: https://www.bsi-fuer-buerger.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2011.pdf?__blob=publicationFile (дата обращения: 31.09.2011). Tropina, T. Cybercrime and Organized Crime, Freedom from Fear Magazine. – 2010. — Issue 3.

[22] См.: Преступления, связанные с использованием компьютерной сети // Десятый конгресс ООН по предупреждению преступности и обращению с правонарушителями //A/CONF.187/10.

для противоправной деятельности, как отдельным лицам, так и преступным группам, необходимо постоянное международное сотрудничество. Контролировать киберпреступность и бороться с ней на уровне отдельного государства практически невозможно. Важную роль в борьбе с киберпреступностью поэтому играют международные соглашения в соответствующей области. Так, Конвенция Совета Европы 2001 г. обязывает стороны установить уголовную ответственность за содействие либо подстрекательство, а также за попытку совершения деяний, предусмотренных статьями 2—10.

Закон также предусматривает установление сторонами уголовной, гражданской либо административной ответственности юридических лиц за преступления, совершённые любым физическим лицом, действующим индивидуально либо как представитель органа данного юридического лица и занимающим в нём руководящую должность. Последнее означает, что такое физическое лицо уполномочено представлять юридическое лицо, имеет право принимать решения в его интересах и осуществлять контроль внутри юридического лица.

Глава 2 второго раздела Конвенции посвящена процессуальным мерам, которые должны принять стороны Конвенции.

Представляется, что принятие данной Конвенции Совета Европы было весьма важным и своевременным шагом. К сожалению, Россия не присоединилась к указанной конвенции. Мировое же сообщество пока не располагает ни международным органом, специально занимающимся интернет-преступностью, ни общемировым кодексом, определяющим масштабы ответственности за соответствующие преступления. В целом ООН пока не выработала какой-то целостной политики в области криминализации киберпреступлений.

Тем не менее, в мире предпринимаются определённые шаги в направлении более решительного противодействия новой глобальной угрозе. Так, Россия выступила в последние годы с инициативой принятия специальной Конвенции ООН, полагая, что назрела потребность в разработке и принятии универсальной международной конвенции по борьбе с киберпреступностью, а также общего кодекса принципов поведения государств в мировом информационном пространстве. В Совете безопасности и МИДе РФ подготовлен проект конвенции ООН «Об обеспечении международной информационной безопасности». Документ (на принятие его Россия рассчитывает уже в 2012 году) запрещает использование Интернета в военных целях и для свержения режимов в других странах, но при этом оставляет властям полную свободу действий внутри национальных сегментов сети.

Основные угрозы, на борьбу с которыми направлен продвигаемый Россией документ, подробно перечислены в его четвёртой статье. Среди них «использование информационных технологий для враждебных действий и актов агрессии», «подрыв политической, экономической и социальной систем» одного государства другим, «манипулирование потоками в информационном пространстве других государств с целью искажения психологической и духовной среды общества», а также «массированная психологическая обработка населения для дестабилизации общества и государства». Россия считает подобные действия составными частями «информационной войны» и требует признать их преступлением против международного мира и безопасности.

Нормы, которые должны помочь России бороться с этими угрозами, подробно изложены в ключевой, пятой статье конвенции. «Государства будут руководствоваться принципом неделимости безопасности и не будут укреплять свою безопасность в ущерб безопасности других, — говорится в документе. — Ни одно государство не будет предпринимать попыток добиться господства в информационном пространстве над другими государствами».

Шестая статья проекта конвенции обязывает государства «воздерживаться от разработки и принятия планов, способных спровоцировать возрастание угроз в информационном пространстве», «не использовать информационно-коммуникационные технологии для вмешательства в дела, относящиеся к внутренней компе-

тенции другого государства» и, наконец, «воздерживаться от клеветнических утверждений, оскорбительной или враждебной пропаганды для осуществления интервенции или вмешательства во внутренние дела других государств».

Проект конвенции также предлагает государствам сотрудничать друг с другом при расследовании кибератак и в некоторых случаях допускать иностранных следователей к соответствующим системам на своей территории.[23]

В уголовном законодательстве России ответственность за преступления в сфере компьютерной информации регламентируется главой 28 УК РФ, в которую включены три статьи: 272 (Неправомерный доступ к компьютерной информации), 273 (Создание, использование и распространение вредоносных программ для ЭВМ), 274 (Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети). Существующее уголовное законодательство об ответственности за преступления в сфере компьютерной информации говорит только о компьютерных преступлениях, т.е. преступлениях, которые совершаются в отношении компьютеров и компьютерной информации (преступлениях против компьютерной безопасности), но не касается других преступлений, совершаемых с их использованием.

Модельный кодекс государств-участников СНГ, также содержащий главу о преступлениях в сфере компьютерной информации, является, на наш взгляд, гораздо более проработанным документом в отношении компьютерных преступлений, чем УК РФ. Раздел XII этого Кодекса — «Преступления против информационной безопасности» — содержит 7 статей:

- «Несанкционированный доступ к компьютерной информации»;
- «Модификация компьютерной информации»;
- «Компьютерный саботаж»;
- «Неправомерное завладение компьютерной информацией»;
- «Изготовление и сбыт специальных средств для получения неправомерного доступа к компьютерной системе или сети»;
- «Разработка, использование и распространение вредоносных программ»;
- «Нарушение правил эксплуатации компьютерной системы или сети».[24]

Представляется целесообразным ввести в УК РФ помимо других новелл, также норму о «приобретении права на чужое имущество, совершённое путём ввода, изменения, удаления или блокирования компьютерных данных либо любого другого вмешательства в функционирование компьютера или компьютерной системы» («компьютерное хищение»). По сути, эта норма будет охватывать деяния, называемые «компьютерными кражами», но не подпадающие под действие статьи 158 УК РФ.

В настоящее время всё чаще говорится о необходимости криминализации спама. Ещё в 2004 году на рассмотрение в Государственную Думу РФ был внесён проект Федерального закона «О внесении изменений в Федеральный закон «О рекламе», Уголовный кодекс Российской Федерации и Кодекс Российской Федерации об административных правонарушениях (о рекламе в сети электросвязи)», предусматривающий дополнение УК РФ статьёй об уголовной ответственности за спам. Данный законопроект в декабре 2004 года был отозван авторами законодательной инициативы.

С таким явлением, как спам, можно и нужно бороться, но его общественная опасность — одно из основных оснований для криминализации деяния, — вряд ли такова, что необходимо предусматривать уголовную ответственность за совершение таких действий.

Вполне достаточно было бы внесения норм об ответственности за незапрашиваемые рассылки в Кодекс РФ об административных правонарушениях.

[23] См.: *Черненко Е., Габуев А.* Россия указала выход для Интернета // Коммерсантъ. — 2011. — 23 сентября.