УДК 343

НЕКОТОРЫЕ ПРОБЛЕМЫ БОРЬБЫ С КИБЕРПРЕСТУПНОСТЬЮ КАК САМЫХ ОПАСНЫХ ТРАНСНАЦИОНАЛЬНЫХ ПРЕСТУПЛЕНИЙ

Филимонов Сергей Александрович
канд. юр. наук
Кубанский государственный университет (филиал), Тихорецк
author@apriori-journal.ru

Аннотация. В настоящее время наблюдается значительный рост киберпреступлений, которые объективно являются самыми опасными транснациональными преступлениями. В связи с этим необходимо оценить эффективность имеющегося арсенала средств противодействия данным преступлениям. В статье анализируются некоторые проблемы борьбы с киберпреступностью, определяются перспективы дальнейшего развития нормативных предписаний по данной проблеме.

Ключевые слова: транснациональные преступления; киберпреступления; уголовное право; Европейский союз; Европол.

SOME PROBLEMS OF STRUGGLE WITH CYBERCRIMES AS MOST DANGEROUS TRANSNATIONAL CRIMES

Filimonov Sergey Aleksandrovich
candidate of jurisprudence
Kuban state university (branch), Tikhoretsk

Abstract. Significant growth cybercrimes which objectively are the most dangerous transnational crimes is observed. It is necessary to estimate efficiency of an available arsenal of means of counteraction to the given crimes. In article some problems of struggle with cybercrimes are analyzed, prospects of the further development of normative instructions on the given problem are determined.

Key words: transnational crimes; cybercrimes; criminal law; the European union; European police.

В настоящее время идет широкомасштабное формирование глобального информационного общества, при котором проблема обеспечения безопасности информации выходит на первый план. При этом от правоохранительных органов требуется грамотное и своевременное противодействие преступным посягательствам в сфере обращения цифровой информации.

Одними из наиболее опасных транснациональных преступлений, на наш взгляд, являются киберпреступления. Как следует из п. 2 Конвенции ООН «Против транснациональной организованной преступности» от 15 ноября 2000 года (ратифицирована РФ Федеральным законом от 26.04.2004 № 26-ФЗ и вступила в силу на территории России с 25 июня 2004 года) преступление носит транснациональный характер, если:

a) оно совершено в более чем одном государстве;

b) оно совершено в одном государстве, но существенная часть его подготовки, планирования, руководства или контроля имеет место в другом государстве;

c) оно совершено в одном государстве, но при участии организованной преступной группы, которая осуществляет преступную деятельность в более чем одном государстве;

или

d) оно совершено в одном государстве, но его существенные последствия имеют место в другом государстве [1].

По данным отчета Европола «The EU Serious and Organized Crime Threat Assessment» (SOCTA) 2013» только на территории Европейского союза обезврежено 3600 преступных группировок, осуществляющих свою деятельность в сети Internet, целью которых была личная финансовая выгода и подрыв экономической стабильности. Эксперты Европола вынуждены отметить, что в настоящее время выявляется порядка 30 % всех киберпреступлений и прогнозируют в будущем увеличение числа совершаемых в этой сфере преступных деяний, связывая рост

киберпреступности с увеличением значимости Интернета в повседневной жизни. Также данные эксперты отмечают, что увеличение значения мобильных устройств в качестве основного средства доступа к интернет-ресурсам может привести к более широкому использованию этих устройств преступниками [2].

Согласно Конвенции «О преступности в сфере компьютерной информации», заключенной в г. Будапеште в 2001 году и вступившей в силу с 01 июля 2004 года киберпреступлениями являются деяния, направленные против конфиденциальности, целостности и доступности компьютерных систем, сетей и компьютерных данных, а также злоупотребления такими системами, сетями и данными [3]. Согласно ст.12 данной Конвенции предусмотрено введение уголовной ответственности юридических лиц, что противоречит действующему российскому уголовному законодательству. Как обоснованно указывают С.С. Арбузов и С.П. Кубанцев, на настоящий момент существующие положения по введению уголовной ответственности юридических лиц в России носят поверхностный характер, игнорируют существующую доктрину уголовного права и в случае их реализации способны дезорганизовать систему уголовного судопроизводства и стать дополнительным источником коррумпированности правоохранительных и иных государственных органов [4].

В связи с острой необходимостью борьбы с киберпреступностью 01 июня 2001 года в г. Минске было заключено Соглашение о сотрудничестве государств – участников содружества независимых государств в борьбе с преступлениями в сфере компьютерной информации (ратифицировано РФ с оговоркой Федеральным законом от 01.10.2008 № 164-ФЗ и вступило в силу на территории России с 17.10.2008 года) [5]. Как следует из ст. 1 вышеуказанного Соглашения преступление в сфере компьютерной информации – уголовно наказуемое деяние, предметом посягательства которого является компьютерная информация.

С учетом того факта, что вышеуказанные международные правовые акты по борьбе с киберпреступностью обладают явной противоречивостью в том числе в самом понятии киберпреступления это может привести к уводу от уголовной ответственности преступника только потому, что государство, в котором было совершено киберпреступление и государство, в котором было задержано виновное лицо ориентируются на разные международные договора о борьбе с кибепреступлениями. Необходимо также отметить, что не все страны мира криминализировали киберпреступления. То есть совершение киберпреступлений в некоторых странах вообще уголовно не наказуемо, что приводит к появлению безнаказанных профессиональных интернет – преступников.

Как обоснованно указывает Р.В. Амелин появление главы 28 в УК РФ в 1996 г. было крайне обоснованным и весьма своевременным в связи с интенсивным развитием информационных технологий. В то же время в силу относительной новизны регулируемых данной главой правоотношений она страдает многочисленными недостатками – главным образом в понятийной сфере, начиная от отсутствия нормативной дефиниции самого понятия компьютерной информации и заканчивая множеством спорных моментов, связанных с объективной частью каждой из включенных в нее статей [6].

Для совершения киберпреступлений достаточно лишь приобрести портативное средство спутниковой связи. Время, в течение которого совершается этот вид преступлений, может занимать менее одной минуты и преступник не ограничен в выборе страны, на территории которой он это устройство будет использовать. У правоохранительных органов на поиск и привлечение к уголовной ответственности такого лица, как правило, уходит значительное количество времени, в течение которого преступник имеет реальную возможность уничтожить следы преступления, чем затруднить или сделать невозможным привлечение киберпреступника к уголовной ответственности. В данной ситуации только путем объединения

усилий правоохранительных органов всех государств возможно эффективное пресечение этой категории транснациональных преступлений.

В связи с открытым доступом к сети Интернет большинство киберпреступлений совершается именно с использование данной сети, ведь отследить лицо, совершившее преступление весьма затруднительно. Одним из факторов, приводящих к росту данной категории преступлений в России, является отсутствие необходимого взаимодействия правоохранительных органов в вопросах расследования этих преступлений. В этой связи особое значение приобретает необходимость постоянного повышения профессиональной подготовки сотрудников правоохранительных органов по вопросам расследования данных преступлений.

Говоря о данной проблеме нельзя не указать на высокую латентность киберпреступлений. Мы согласны с М.В. Старичковым, который называет уровни латентности порядка 99,7 % по ст. 272 УК РФ и 99,8 % по ст. 273 УК РФ как для всех преступлений в сфере компьютерной информации, так и для преступлений, совершенных посредством Интернета, хотя замечает, что полученные данные вряд ли могут претендовать на абсолютную достоверность [7]. Как обоснованно указывает А.А. Комаров высокая латентность и безнаказанность киберпреступников может повлечь переход традиционных форм мошенничества в интернет и приведет к снижению выявляемости и раскрываемости деяний, совершенных данным способом [8]. Потерпевшие по данной категории преступлений вряд ли захотят обращаться в правоохранительные органы, поскольку вероятность поймать киберпреступника минимальна, а время, потраченное на подачу заявления в порядке ст. 141 УПК РФ и дачу объяснения при проведении проверки по ст. 144 УПК РФ никем материально компенсировано не будет, как и ущерб, причиненный киберпреступлением.

В настоящее время в целях пресечения киберпреступности необходимо принимать более действенные и жесткие меры. Так, в действующий УК РФ необходимо ввести дополнительную статью об ответствен-

ности руководителя компаний интернет – провайдеров и сотовых операторов за бездействие, позволившее совершить киберпреступление. При этом также необходимо распределить и гражданско-правовую ответственность исходя из степени вины киберпреступника и интернет-провайдера (оператора сотовой связи).

Как обоснованно указывает П.В. Костин, преступления в сфере компьютерной информации редко встречаются в обособленном виде, как правило, они совершаются в совокупности с иными общественно опасными деяниями и имеют факультативный характер. Это обусловлено тем, что при использовании компьютерной информации в качестве средства совершения другого преступления она сама становится предметом общественно опасного деяния [9].

По мнению И.Г. Чекунова в современных условиях широкое распространение получили случаи организации Doss-атак на компьютеры коммерческих организаций, основной целью которых является последующее требование вознаграждения за их прекращение.

С позиций уголовного права отмеченные деяния, несомненно, подпадают под действие ст. ст. 272 (неправомерный доступ к компьютерной информации) и 273 (создание, использование и распространение вредоносных программ для ЭВМ) УК РФ. Однако следует обратить внимание на санкции данных норм уголовного законодательства. Если описанные деяния не влекут за собой тяжкие последствия, а они, как правило, не влекут такие последствия, то в соответствии с указанными статьями они признаются преступлениями всего лишь средней тяжести, что явно не соответствует степени их общественной опасности. По механизму своего совершения они крайне схожи с таким составом преступления, как вымогательство и, с нашей точки зрения, должны наказываться не менее строго.

Применить к организаторам Doss-атак положения норм ст. 163 УК РФ нельзя. Помимо угроз, связанных с применением насилия, диспозиция ч. 1 ст. 163 УК РФ в качестве способов совершения вымогательства преду-

сматривает только угрозы уничтожения или повреждения чужого имущества, а также шантаж. Таким образом, действия организаторов Doss-атак находятся за рамками действия ст. 163 УК РФ. Такие атаки всего лишь блокируют работу программного обеспечения компьютеров коммерческих организаций или отдельных пользователей или осуществляют массовую рассылку пользователям электронных сообщений, что затрудняет или делает невозможным их работу в компьютерных сетях, но все эти действия нельзя отождествлять с уничтожением или повреждением чужого имущества, а тем более с шантажом потерпевшего [10]. При таких обстоятельствах в настоящее время необходимо ввести квалифицирующий признак в ст. ст. 272, 273 УК РФ за организацию Doss-атак на компьютеры коммерческих организаций, основной целью которых является последующее требование вознаграждения за их прекращение.

В 28-й главе УК РФ угрозы для компьютерной информации рассматриваются не с точки зрения ее свойств, которые нарушаются в результате неправомерных действий (бездействия), а с точки зрения самих этих действий. Нам становится понятно, что указать исчерпывающий перечень действий, направленных на угрозу правоотношениям в сфере компьютерной информации, практически невозможно, поскольку наблюдается стремительное развитие компьютерных технологий. Данный факт также является проблемой при расследовании этой категории преступлений.

Так, например, формально чтение информации с экрана монитора не подпадает ни под одно из перечисленных выше понятий (уничтожение, блокирование, копирование, модификация), однако нарушает права владельца информации (например, если эта информация составляет личную или коммерческую тайну) [11].

Подводя итог нашему исследованию необходимо прийти к выводу о том, что в действующих международных правовых актах по борьбе с киберпреступностью необходимо внести ряд изменений направленных на унификацию составов киберпреступлений и понуждению всех стран мира к криминализации всех видов киберпреступлений.

Список использованных источников

1. СПС «Консультант плюс». 2014.
2. Отчет Европола «The EU Serious and Organized Crime Threat Assessment (SOCTA) 2013» [Электронный ресурс]. URL:ttps://www.europol.europa.eu/sites/default/files/publications/socta2013.pdf
3. СПС «Консультант плюс». 2014.
4. Арбузов С.С., Кубанцев С.П. О перспективе введения в России института уголовной ответственности юридических лиц // Журнал российского права. 2012. № 10. С. 106.
5. СПС «Консультант плюс». 2014.
6. Амелин Р.В. О возможном решении неполноты главы 28 УК РФ // Уголовно-исполнительная система: право, экономика, управление. 2009. № 5. С.27.
7. Старичков М.В. Умышленные преступления в сфере компьютерной информации: уголовно-правовая и криминологические характеристики: дис. …канд. юр. наук. Иркутск, 2006. С. 109-112.
8. Комаров А.А. Криминологические аспекты мошенничества в глобальной сети Интернет: автореф. дис. …канд. юр. наук. Саратов, 2011. С. 16.
9. Костин П.В. Исследование машинных носителей информации, используемых при совершении преступлений в сфере экономики: автореф. дисс. ...канд. юр. наук. Н.Новгород, 2007. С. 6.
10. Чекунов И.Г. Некоторые особенности квалификации преступлений в сфере компьютерной информации // Российский следователь. 2012. № 3. С. 13.
11. Расследование неправомерного доступа к компьютерной информации / под ред. Н.Г. Шурухнова. М., 2004. С. 95.