

УДК 343.9 : 004

## **О МЕРАХ ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПНОСТИ В МЕЖДУНАРОДНОМ И РОССИЙСКОМ УГОЛОВНОМ ПРАВЕ**

**В. В. Харитошкин**

ФГБОУ ВО «Тверской государственный университет», г. Тверь

В статье рассматриваются различные аспекты взаимодействия российского и международного уголовного права по вопросам борьбы с киберпреступностью.

***Ключевые слова:** информационные технологии, киберпреступность, компьютерная безопасность, международное право, российское уголовное право, имплементация.*

Широкое внедрение информационных технологий во все сферы жизни, доступность использования информации стали неременным условием развития науки, техники и цифровой экономики. В этих условиях любые преступные проявления, направленные против компьютерной безопасности, создают реальную угрозу научно-техническому прогрессу и национальной безопасности государства в целом.

Принимая во внимание указанные обстоятельства, Указом Президента Российской Федерации от 5 декабря 2016 г. утверждена новая Доктрина информационной безопасности Российской Федерации<sup>1</sup>. В ней отмечается, что повышение эффективности профилактики правонарушений, совершаемых с использованием информационных технологий, и противодействие таким правонарушениям являются важной составляющей обеспечения информационной безопасности.

Действующее законодательство Российской Федерации предусматривает уголовную ответственность за различные виды преступлений в сфере киберпреступности (ст. 272–274 УК РФ). Аналогичный подход наблюдается и за рубежом. По различным экспертным оценкам в последние годы, в мире отмечается как рост количества компьютерных преступлений, так и объема ущерба, причиненного в результате их совершения<sup>2</sup>. При этом особенностью киберпреступности является то, что она носит трансграничный характер. Следовательно, изучение зарубежного законодательства в сфере информационной безопасности представляется не только

---

<sup>1</sup> Указ Президента РФ от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // СПС «Гарант».

<sup>2</sup> См. подробнее: Лацинская М. Group-IB предоставила отчет о хакерских атаках // Газета. RU. 13 октября 2016 г. URL: <https://www.gazeta.ru/tech/2016/10/13/10249697/cybercrimecon.2016>

полезным, но и необходимым. Учет подобного опыта позволит избежать возможных ошибок и поможет решить многие проблемы установления уголовной ответственности за информационные преступления.

Важную роль в консолидации усилий государств в деле решения проблем информационной безопасности призвана была сыграть Конвенция о киберпреступности, вступившая в силу 1 июля 2004 г. Ее участниками стали 38 государств-членов Совета Европы, а также США, Канада, Япония, ЮАР и ряд других государств. Данная Конвенция содержит подробную классификацию киберпреступлений. Кроме того в ней указан порядок взаимодействия государств, чьи интересы пострадали в результате действий киберпреступников, а также регулируются вопросы хранения и использования личной информации клиентов интернет-провайдеров при расследовании преступлений.

Следует отметить, что в подготовке Конвенции активное участие принимали и российские специалисты. Но подписав в 2005 г. данную Конвенцию, наша страна вскоре отозвала свою подпись<sup>3</sup>. Что же явилось причиной такого решения? Российская сторона посчитала неприемлемым отсутствие условий трансграничного доступа к компьютерным системам, а ряд положений Конвенции, по мнению экспертов, содержит непосредственную угрозу национальной безопасности и суверенитету нашей страны.

В сложившейся ситуации в России обратили внимание на малайзийскую инициативу ИМРАСТ<sup>4</sup>, цель которой – повышение способности глобального сообщества решать проблемы, связанные с информационной безопасностью. Для нашей страны, по мнению ряда экспертов, это направление международного сотрудничества представляется в настоящее время более перспективным.

Важное значение для правоприменительной практики имели решения на международном уровне вопросов юридической техники, а также разработка целого ряда юридических понятий. В качестве одного из примеров можно привести разработанное ЮНЕСКО определение информационных технологий, под которыми понимаются «комплекс взаимосвязанных научных, технологических, инженерных дисциплин, изучающих методы эффективной организации охраны труда людей, занятых обработкой и хранением информации; вычислительная техника

---

<sup>3</sup> См.: Распоряжение Президента РФ «О подписании Конвенции о киберпреступности» от 15.11.2005 г. № 557-рп // СЗ РФ. 2005. № 47. Ст. 4929; Распоряжение Президента РФ «О признании утратившим силу Распоряжение Президента РФ от 15.11.2005 г. "О подписании Конвенции о киберпреступности" от 22.03.2008 г. № 144-рп» // СЗ РФ. 2008. № 13. Ст. 1295.

<sup>4</sup> ИМРАСТ – Международное многостороннее партнерство против кибер-угроз.

и методы организации и взаимодействия с людьми и производственным оборудованием, их практические приложения, а также социальные, экономические и культурные проблемы»<sup>5</sup>.

В этой связи следует отметить, что появлению в действующем УК РФ отдельной главы о преступлениях в сфере компьютерной безопасности (гл. 28), включающей нормы об ответственности за неправомерный доступ к компьютерной информации (ст. 272 УК РФ); создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ); нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК РФ); неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (ст. 274.1 УК РФ), во многом способствовало введению в правовую систему России целого ряда понятий в сфере информационной безопасности, разработанных и принятых на международном уровне.

Говоря о совершенствовании российского уголовного законодательства в сфере борьбы с киберпреступностью нельзя не отметить и Модельный уголовный кодекс для стран-участниц СНГ, принятый 17 февраля 1996 г. В гл. 30 раздела «Преступления против информационной безопасности», наряду с известными российскому уголовному праву составами преступлений в сфере компьютерной информации, упоминается также об изготовлении с целью сбыта, а равно сбыте специальных программных или аппаратных средств для получения неправомерного доступа к защищенной компьютерной системе или сети (ст. 290). Представляет интерес и ст. 289, рассматривающая как преступление небольшой тяжести несанкционированное копирование или иное неправомерное завладение информацией, хранящейся в компьютерной системе, сети или на машинных носителях, а равно перехват информации, передаваемой с использованием средств компьютерной связи<sup>6</sup>.

В последние годы информационные технологии все чаще используются организованной преступностью в самых разнообразных сферах. С появлением новых информационных возможностей все более острыми становятся проблемы борьбы с незаконным оборотом наркотических и психотропных веществ, а также распространением

---

<sup>5</sup> См.: Федотова Е.Л. Информационные технологии и системы: учеб. пособие. М.: Форум: Инфра-М, 2011. С. 66.

<sup>6</sup> См.: Модельный Уголовный кодекс государств-участников СНГ (принят постановлением Межпарламентской Ассамблеи государств-участников СНГ 17 февраля 1996 г.) // Приложение к Информационному бюллетеню Межпарламентской Ассамблеи государств-участников СНГ. 1997. № 10.

порнографических материалов. Так, по мнению эксперта ООН С. Шоула, являющегося координатором Программы ООН по контролю за оборотом наркотиков, Интернет стал тайной лабораторией для их изготовления, а его сеть оказалась заполненной сайтами пронаркотического содержания<sup>7</sup>.

Учитывая транснациональный характер преступности, связанной с наркобизнесом, в качестве юридической основы для создания национального законодательства на международном уровне была признана необходимой разработка конвенций по борьбе с этим злом. Важную роль в развитии российского уголовного законодательства в данной сфере сыграли Единая конвенция о наркотических средствах (Нью-Йорк, 1961 г.), Конвенция о психотропных веществах (Вена, 1971 г.) и Конвенция ООН о борьбе против незаконного оборота наркотических средств и психотропных веществ (Вена, 1988 год). В конвенциях указаны все виды преступлений, охватываемых понятием «наркобизнес». В действующем российском уголовном законе установлена ответственность практически за все эти деяния. После вступления в силу УК РФ было внесено около 70 поправок, касающихся установления либо усиления уголовной ответственности за преступления, связанные с незаконным оборотом наркотических и психотропных веществ, включая появление новых составов. Все это говорит о том, что Российская Федерация осуществляет последовательную имплементацию норм международных конвенций по борьбе с наркобизнесом в отечественное законодательство.

Принимая во внимание рекомендации об усилении уголовной ответственности за злоупотребление в сфере телекоммуникаций и высоких технологий при совершении преступлений, содержащиеся в Международном пакте о гражданских и политических правах (ч. 3 ст. 19) и Европейской конвенции по защите прав человека и основных свобод (п. 2 ст. 10), в ряд составов УК РФ был включен квалифицирующий признак «с использованием средств массовой информации, либо электронных или информационно-телекоммуникационных сетей (включая сеть Интернет)». Так, с принятием Федерального закона от 1 марта 2012 г. №18 ФЗ этот квалифицирующий признак появился в ч. 2 ст. 228.1 УК РФ. В настоящее время на рассмотрении в Государственной Думе РФ находится законопроект о введении уголовного наказания за пропаганду и рекламу в сети Интернет наркотических средств. Ответственность за пропаганду наркотических средств, психотропных веществ и их

---

<sup>7</sup> См.: Гузеева О. Ответственность за распространение информации пронаркотического характера в российском сегменте в сети Интернет // Законность. 2007. № 7. С. 41 – 43.

прекурсоров предусмотрена в ч. 1 ст. 46 ФЗ РФ от 8 января 1998 г. «О наркотических средствах и психотропных веществах»<sup>8</sup>, ст. 4 Закона РФ от 27 декабря 1991 г. «О средствах массовой информации»<sup>9</sup>, ст. 6.13 Кодекса об административных правонарушениях, а также ст. 230 УК РФ.

В меньшей степени в международно-правовых актах регулируются вопросы ответственности за распространение в сети Интернет порнографических материалов. Так, в том же Международном Пакте о гражданских и политических правах и Европейской конвенции о защите прав человека и основных свобод содержится ряд положений, касающихся вопросов нравственных критериев при оценке материалов, размещаемых в различных информационных источниках.

При этом особое внимание обращается на распространение, публичную демонстрацию или рекламирование порнографических материалов с изображением несовершеннолетних. Учитывая имеющийся международный опыт борьбы с такого рода преступлениями, в 2012 г. в УК РФ были внесены редакционные изменения и дополнения в ст. 242 УК РФ, а также появились две новые статьи: 242.1 и ст. 242.2. В 2013 г. Россия ратифицировала Конвенцию Совета Европы о защите детей от сексуальной эксплуатации и сексуальных злоупотреблений (CETS № 201) от 25 октября 2007 г.<sup>10</sup>. Данная конвенция содержит перечень деяний, которые государству-участнику необходимо криминализировать: производство детской порнографии, распространение или передача детской порнографии, преднамеренное получение к доступу детской порнографии при помощи информационно-коммуникационных технологий. Соответствующее положение также было включено в европейскую Конвенцию о борьбе с киберпреступностью 2001 г. (ETS № 185)<sup>11</sup>. Эта Конвенция предусматривает для государств-участников установить в своем внутреннем законодательстве в качестве уголовно-наказуемых следующие деяния: изготовление материалов, связанное с детской порнографией, с целью распространения их через компьютерную систему; предложения или предоставление материалов, связанных с детской порнографией, через компьютерную систему; получение

---

<sup>8</sup> См.: СЗ РФ. 1998. № 2. Ст. 219.

<sup>9</sup> См.: Ведомости Съезда народных депутатов Российской Федерации и Верховного Совета Российской Федерации. 1992. № 7. Ст. 300.

<sup>10</sup> См.: Конвенция Совета Европы о защите детей от сексуальной эксплуатации и сексуальных злоупотреблений (CETS № 201) от 25 октября 2007 г. // СЗ РФ. 2014. № 7. Ст. 632.

<sup>11</sup> См.: Конвенция о преступности в сфере компьютерной безопасности (ETS № 185): заключена в г. Будапеште 23 ноября 2001 г. // СПС «Консультант Плюс».

материалов, связанных с детской порнографией, через компьютерную систему для самого себя или для другого лица; обладание материалами, связанными с детской порнографией, в компьютерной системе или на носителе компьютерных данных.<sup>12</sup>

В целом сравнение отечественного уголовного права и международно-правовых источников по вопросам обеспечения эффективного и безопасного использования информационных технологий позволяет сделать вывод, что наша страна является активным участником многих соглашений в этой сфере и придерживается большинства рекомендаций, выдвигаемых международным сообществом.

### **Список литературы**

1. Конвенция Совета Европы о защите детей от сексуальной эксплуатации и сексуальных злоупотреблений (СЕТС № 201) от 25 октября 2007 // СЗ РФ. 2014. № 7. Ст. 632.

2. Конвенция о преступности в сфере компьютерной безопасности (ETS № 185): заключена в г. Будапеште 23 ноября 2003 // СПС «Консультант Плюс».

3. Модельный Уголовный кодекс государств-участников СНГ (принят постановлением Межпарламентской Ассамблеи государств-участников СНГ 17 февраля 1996 г.) // Приложение к Информационному бюллетеню Межпарламентской Ассамблеи государств-участников СНГ. 1997. № 10.

4. Указ Президента РФ от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // СПС «Гарант».

5. Распоряжение Президента РФ «О подписании Конвенции о киберпреступности» от 15.11.2005 г. № 557-рп // СЗ РФ. 2005. № 47. Ст. 4929.

6. Распоряжение Президента РФ «О признании утратившим силу Распоряжение Президента РФ от 15.11.2005 г. "О подписании Конвенции о киберпреступности" от 22.03.2008 г. № 144-рп» // СЗ РФ. 2008. № 13. Ст. 1295.

11. Заирная М.М. Преступления в сфере оборота порнографических материалов и предметов: монография. М: Юрлитинформ, 2017.

7. Ведомости Съезда народных депутатов Российской Федерации и Верховного Совета Российской Федерации. 1992. № 7. Ст. 300.

---

<sup>12</sup> См.: Заирная М.М. Преступления в сфере оборота порнографических материалов и предметов: монография. М: Юрлитинформ, 2017. С. 22.

8. Гузеева О. Ответственность за распространение информации пронаркотического характера в российском сегменте в сети Интернет // Законность. 2007. №7. С. 41–43.

9. Лацинская М. Group-IB предоставила отчет о хакерских атаках // Газета. RU. 13 октября 2016 г. URL: <https://www.gazeta.ru/tech/2016/10/13/10249697/cybercrimecon.2016>

10. Федотова Е.Л. Информационные технологии и системы: учеб. пособие. М.: Форум: Инфра-М, 2011.

## ON MEASURES AGAINST CYBER CRIME IN INTERNATIONAL AND RUSSIAN CRIMINAL LAW

**V. V. Haritoshkin**

Tver State University

The article discusses various aspects of the interaction of Russian and international criminal law in the fight against cybercrime.

**Keywords:** *information technology, cybercrime, computer security, international law, Russian criminal law, implementation.*

### *Об авторе*

ХАРИТОШКИН Валерий Вячеславович – кандидат юридических наук, профессор, заведующий кафедрой уголовного права и процесса Тверского государственного университета (170100, г. Тверь, ул. Желябова, 33); e-mail: [jurfaktver\\_nauka@mail.ru](mailto:jurfaktver_nauka@mail.ru)

HARITOSHKIN Valery – PhD, Professor, head. department of criminal law and procedure of the Tver State University (170100, Tver, ul. Zhelyabova, 33); e-mail: [jurfaktver\\_nauka@mail.ru](mailto:jurfaktver_nauka@mail.ru)

Харитошкин В.В. О мерах противодействия киберпреступности в международном и российском уголовном праве // Вестник ТвГУ. Серия: Право. 2019. № 3 (59). С. 111 – 117.