

УДК 341.24:342.97

**МЕЖДУНАРОДНОЕ СОТРУДНИЧЕСТВО В СФЕРЕ УГОЛОВНО-ПРАВОВОЙ БОРЬБЫ
С НЕПРАВОМЕРНЫМ ЗАВЛАДЕНИЕМ КОМПЬЮТЕРНОЙ ИНФОРМАЦИЕЙ****М.А. ДУБКО***(Белорусский государственный университет, Минск)*

Представлен краткий анализ международной конвенционной и институционной работы государств и организаций в сфере противодействия неправомерному завладению компьютерной информацией. Показан транснациональный характер современной компьютерной преступности, требующий от государств поиска точек сближения по проблемам сотрудничества в сфере борьбы с данными преступлениями. Определены некоторые перспективы такого международного сотрудничества.

Введение. Использование компьютерных, информационно-коммуникационных технологий имеет бесспорные преимущества, однако возможности быстро развивающихся технологий все чаще используются в преступных целях, о чем свидетельствует статистика компьютерных преступлений как в Республике Беларусь [1], так и в зарубежных странах [2 – 4].

Трансграничный характер киберпреступности требует от государств выработки единого подхода в вопросе криминализации общественно опасных деяний в сфере оборота компьютерной информации. Наличие различий в правовых системах и недостаточно развитое международное сотрудничество усложняют проведение расследований киберпреступлений и преследование за их совершение. В настоящее время закреплены некоторые международно-правовые основы сотрудничества в области борьбы с компьютерной преступностью. В частности, таковыми являются Конвенция Совета Европы о киберпреступности 2001 года [5], Меры по борьбе против преступлений, связанных с использованием компьютеров, принятые на Одиннадцатом Конгрессе Организации Объединенных Наций по предупреждению преступности и обращению с правонарушителями в Бангкоке 25 апреля 2005 года [6], Глобальная программа кибербезопасности, утвержденная Международным союзом электросвязи в 2007 году [7], Окинавская Хартия глобального информационного общества, принятая 23 июля 2000 года на Окинаве (Япония) [8] и др. В масштабе стран СНГ 17 февраля 1996 года на VII пленарном заседании Межпарламентской Ассамблеи был принят Модельный уголовный кодекс, в котором регламентируется ответственность за компьютерные преступления [9]; 1 июня 2001 года в Минске было заключено Соглашение о сотрудничестве государств-участников СНГ в борьбе с преступлениями в сфере компьютерной информации [10].

Основная часть. Кратко рассмотрим историческое изменение международной политики в вопросах криминализации компьютерных преступлений, в частности, неправомерного завладения информацией.

Первая попытка разработки понятия и определения видов компьютерных преступлений в Европе была предпринята в рамках Организации экономического сотрудничества и развития (ОЭСР). С 1983 по 1985 год Комитет ОЭСР обсудил возможность международной гармонизации уголовного законодательства отдельных государств с целью борьбы с экономическими компьютерными преступлениями. В 1986 году Комитетом был предложен единый список действий, которые должны рассматриваться как компьютерные преступления в законодательстве государств-членов [11].

В период с 1985 по 1989 год над проблемой компьютерных преступлений работал Отдельный комитет экспертов по компьютерным преступлениям Совета Европы. По итогам работы Комитета 13 сентября 1989 года Совет Европы принял Рекомендацию № R89(9) Комитета Министров стран-членов Совета Европы о преступлениях, связанных с использованием компьютера. В ней определены практически все преступления, связанные с использованием компьютерных технологий, а также дана классификация компьютерных преступлений с рекомендуемым и факультативным перечнем (Минимальный и Необязательный списки) для включения их в национальное законодательство [12].

«Минимальный список правонарушений» включает:

- 1) компьютерное мошенничество;
- 2) компьютерный подлог;
- 3) повреждение компьютерной информации или компьютерных программ;
- 4) компьютерный саботаж;
- 5) несанкционированный доступ к системе ЭВМ;
- 6) несанкционированный перехват информации;
- 7) несанкционированное использование защищенных компьютерных программ;
- 8) незаконное воссоздание схем.

«Необязательный список правонарушений» включает следующие четыре вида преступлений:

- 1) незаконное изменение компьютерной информации или компьютерных программ;
- 2) компьютерный шпионаж;

- 3) противозаконное использование компьютера (без соответствующего разрешения);
- 4) несанкционированное использование защищенных компьютерных программ.

В Конвенции ООН против транснациональной организованной преступности 2000 года, принятой Резолюцией 55/25 Генеральной Ассамблеи от 15 ноября 2000 года [13] косвенно рассматриваются проблемы киберпреступности, если они совершаются организованными преступными группировками.

Европейским комитетом по проблемам преступности и комитетом экспертов по преступности в киберпространстве 25 июня 2001 года был разработан проект Конвенции о киберпреступности. Конвенция была открыта для подписания 23 ноября 2001 года; ее подписали 26 стран-членов Совета Европы, а также США, Канада, Япония и ЮАР. Этот документ обязывает государства, являющиеся его сторонами, гармонизировать национальные законы в отношении определения основных преступлений, указанных в документе.

В разделе 1 Конвенции «Материальное уголовное право» содержится 4 подраздела, таким образом, устанавливающих четыре группы киберпреступлений:

- 1) преступления против конфиденциальности, целостности и доступности компьютерных данных и систем;
- 2) преступления, связанные с использованием компьютерных средств;
- 3) преступления, связанные с содержанием данных;
- 4) преступления, связанные с нарушением авторского права и смежных прав [5].

Следует отметить, что Конвенция выходит за рамки сугубо законодательных вопросов; она в большей степени устанавливает основы для международного сотрудничества правоохранительных органов стран-участниц в борьбе с компьютерной преступностью.

Базируясь на Конвенции и рекомендациях региональных организаций, мировое сообщество могло бы выработать единые подходы к определению понятия компьютерного преступления и его видам, однако Конвенция Совета Европы 2001 года основана на преступном поведении 90-х годов прошлого века и не совсем подходит для борьбы с новыми вызовами (видами компьютерных преступлений) последнего времени. К тому же Конвенции как предполагаемому универсальному механизму сотрудничества в борьбе с компьютерной преступностью не достает мирового масштаба распространения в связи с тем, что такие страны, как Россия, Китай, страны Латинской Америки, Арабские государства, по разным причинам не являются ее участниками.

Главным органом в области межгосударственной борьбы с преступностью является Организация Объединенных Наций (ООН). С 1950 года эта деятельность включена в число ее приоритетов. Проблеме борьбы с компьютерными преступлениями серьезное внимание уделяют Конгрессы ООН.

Начиная с восьмого Конгресса по предупреждению преступности и обращению с правонарушителями, состоявшегося в 1990 году, ООН активно занимается рассмотрением различных аспектов процессов в сферах, связанных с использованием компьютеров. Уже в 1994 году было опубликовано Руководство ООН по предупреждению преступлений, связанных с компьютерами, и борьбе с ними [14]. В 2000 году в рамках десятого Конгресса был проведен семинар-практикум по преступлениям, связанным с использованием компьютерных сетей.

В 2002 году Генеральная Ассамблея ООН призвала международное сообщество усилить помощь государствам-членам в борьбе с преступностью, связанной с использованием компьютеров. В документе «Планы действий по осуществлению Венской декларации о преступности и правосудии: ответы на вызовы XXI века», прилагавшемся к резолюции 56/261 Генеральной Ассамблеи от 31 января 2002 года, имеется особый раздел под названием «Меры по борьбе с преступлениями, связанными с использованием высоких технологий и компьютеров». В нем содержатся ориентированные на принятие конкретных мер программные рекомендации по предотвращению такого рода преступлений и борьбе с ними.

В апреле 2010 года в Бразилии прошел очередной 12-й Конгресс ООН по предупреждению преступности и уголовному правосудию, на котором обсуждались и вопросы борьбы с компьютерными преступлениями и действия государств по обеспечению кибербезопасности. Выступавшие представители государств призвали руководства стран принять меры по повышению эффективности оказания взаимной правовой помощи и сотрудничеству в правоохранительной области. Также на Конгрессе была рассмотрена рекомендация, относительно необходимости тщательного изучения и принятия решения по разработке глобальной конвенции о борьбе с киберпреступностью.

По итогам Конгресса была принята Сальвадорская декларация о комплексных стратегиях для ответа на глобальные вызовы, в которой, в частности, рекомендуется Управлению ООН по наркотикам и преступности (ЮНОДК), в сотрудничестве с государствами-участниками, соответствующими международными организациями и частным сектором, оказывать государствам, по их просьбе, техническую помощь и помощь в подготовке кадров в деле совершенствования национального законодательства и наращивания потенциала национальных органов в целях противодействия киберпреступности.

Проанализировав имеющийся опыт международного сотрудничества в сфере уголовно-правовой борьбы с компьютерной преступностью, можно сделать вывод, что данный процесс довольно динамичен и протекает в двух направлениях: правительственное (межгосударственное) сотрудничество и неправительственное (осуществляется посредством деятельности международных организаций).

Большинство государств имеют двусторонние или многосторонние договоры с другими странами о сотрудничестве по выявлению, пресечению или расследованию компьютерных преступлений, либо данные вопросы разрешаются путем применения традиционных межгосударственных соглашений о взаимной помощи по гражданским, административным и уголовным делам.

На международном уровне такие организации, как Управление ООН по наркотикам и преступности (ЮНОДК), Международная уголовная полиция (Интерпол), Организация международного сотрудничества и развития (ОЭСР) и «Группа Восьми», а также такие региональные организации, как Европейский союз, Совет Европы, Организация американских государств, Ассоциация государств Юго-Восточной Азии и Азиатско-Тихоокеанская ассоциация экономического сотрудничества (АТЭС) обеспечивают политические и технические знания и опыт, необходимые для развития международного сотрудничества. Однако необходимо заметить, что данное сотрудничество осуществляется в основном в сфере информационно-правового обеспечения процессуального взаимодействия правоохранительных органов стран по предупреждению и расследованию компьютерных преступлений, а исследования ведутся в плоскости криминологической науки. Тем временем уголовно-правовые вопросы определения понятия и видов компьютерных преступлений, особенностей их криминализации в национальных уголовных законах, уголовной ответственности за совершение данных деяний остаются без ответа.

Республика Беларусь принимает активное участие в деле международной борьбы с компьютерной преступностью. Не являясь участницей Конвенции о киберпреступности 2001 года, Беларусь предпринимает решительные меры в сфере борьбы с компьютерными преступлениями как на национальном, так и международном уровне.

Национальное законодательство устанавливает основы регулирования в области компьютерной и информационной безопасности, а также содействует дальнейшему развитию информационной сферы в стране. Наиболее значимые нормативные акты, наряду с Уголовным кодексом Республики Беларусь, следующие: Концепция национальной безопасности, утвержденная Указом Президента Республики Беларусь от 09.11.2010; Закон Республики Беларусь «Об информации, информатизации и защите информации» от 10.11.2008; Закон Республики Беларусь «О государственных секретах» от 19.07.2010; Стратегия развития информационного общества в Республике Беларусь на период до 2015 года и план первоначальных мер по реализации Стратегии развития информационного общества в Республике Беларусь на 2010 год от 9 августа 2010 года, утвержденной Постановлением Совета Министров Республики Беларусь № 1174; Указ Президента Республики Беларусь от 01.02.2010 № 60 «О мерах по совершенствованию использования национального сегмента сети Интернет»; Национальная программа ускоренного развития услуг в сфере информационно-коммуникационных технологий на 2011 – 2015 годы и др.

В качестве самостоятельного направления выделяют борьбу с данными преступлениями межправительственные соглашения, среди которых можно выделить: Соглашение между Правительством Республики Беларусь и Правительством Республики Узбекистан о сотрудничестве в области борьбы с преступностью от 19 июня 2008 года; Меморандум о взаимопонимании между Правительством Республики Беларусь и Правительством государства Катар по вопросам сотрудничества в области безопасности от 24 августа 2008 года; Соглашение между Правительством Республики Беларусь и Правительством Исламской Республики Иран о сотрудничестве в сфере безопасности от 10 сентября 2004 года и др. Соглашение о сотрудничестве между Министерством внутренних дел Республики Беларусь и Министерством общественной безопасности Китайской Народной Республики от 22 апреля 2001 года предусматривает осуществление сторонами сотрудничества в предупреждении, пресечении и раскрытии преступлений, связанных с использованием компьютерной техники [15].

Заключение. Возможно, что присоединение Республики Беларусь в Конвенции Совета Европы о киберпреступности способствовало бы положительной оценке международным сообществом деятельности нашего государства в сфере обеспечения информационной безопасности и противодействия компьютерной преступности. Однако, на наш взгляд, существующая на данный момент в Республике Беларусь правовая база в отношении правонарушений и преступлений в информационном пространстве значительно приближена к требованиям и стандартам, принятым на международном уровне, в том числе к Конвенции Совета Европы о киберпреступности.

Заключение универсального международного договора о борьбе с компьютерными преступлениями, который бы учитывал уже накопившийся опыт международных соглашений в данной области и особенности национального законодательства стран-участниц, – довольно сложная и трудоемкая задача. Таким универсальным регулятором могла бы стать отдельная Конвенция ООН о компьютерных преступлениях.

Представляется, что международное сотрудничество в сфере борьбы с компьютерной преступностью должно идти по пути расширения форм правовой помощи между государствами посредством заключения новых соглашений или внесения изменений в уже существующие, а также создания совместных институтов по взаимодействию в сфере борьбы с компьютерной преступностью и урегулированию разногласий, возникающих в процессе применения таких соглашений.

ЛИТЕРАТУРА

1. Статистика. Управление по раскрытию преступлений в сфере высоких технологий [Электронный ресурс]. – Режим доступа: <http://www.mvd.gov.by/ru/main.aspx?guid=3311>. – Дата доступа: 07.02.2012.
2. Официальная статистика компьютерных преступлений, совершенных в российской федерации (по данным Главного информационно-аналитического центра (ГИАЦ) МВД России) [Электронный ресурс]. – Режим доступа: http://www.cyberpol.ru/statcrime.shtml#p_00. – Дата доступа: 06.05.2011.
3. Жмыхов, А.А. Компьютерная преступность за рубежом и ее предупреждение: автореф. дис. ... канд. юрид. наук: 12.00.08 / А.А. Жмыхов. – М., 2003. – 26 с.
4. Число несанкционированных взломов компьютеров Правительства США возросло на 50 % [Электронный ресурс]. – Режим доступа: <http://www.crime-research.ru/news/06.05.2011/7234/>. – Дата доступа: 06.05.2011.
5. Convention on Cybercrime. The Council of Europe. Hungary, 2001 [Электронный ресурс]. – Режим доступа: <http://cyber-crime.com/legislative>. – Дата доступа: 17.12.2011.
6. Бангкокская декларация «Взаимодействие и ответные меры: стратегические союзы в области предупреждения преступности и уголовного правосудия» [Электронный ресурс]. – Режим доступа: http://www.un.org/russian/events/11thcongress/a_conf203_18.pdf. – Дата доступа: 12.02.2012.
7. Глобальная программа кибербезопасности (ГПК) МСЭ [Электронный ресурс]. – Режим доступа: www.ifap.ru/pr/2008/080908aa.pdf. – Дата доступа: 21.02.2012.
8. Окинавская Хартия глобального информационного общества [Электронный ресурс]. – Режим доступа: federalbook.ru/files/SVAYZ/saderzhanie/Tom%206/I/hartia.pdf. – Дата доступа: 17.02.2012.
9. Модельный Уголовный кодекс СНГ [Электронный ресурс]. – Режим доступа: <http://www.cisatc.org/135/154/241>. – Дата доступа: 22.02.2012.
10. Соглашение о сотрудничестве государств-участников СНГ в борьбе с преступлениями в сфере компьютерной информации, 1 июня 2001 г. // Содружество. Информ. вестн. Совета глав гос-в и Совета глав Правительств СНГ. – № 1. – 2001. – С. 23 – 31.
11. Понимание кибербезопасности: руководство для развивающихся стран [Электронный ресурс]. – Режим доступа: http://www.itu.int/dms_pub/itu-d/oth/01/0B/D010B0000073301PDFR.pdf. – Дата доступа: 04.02.2012.
12. Широков, В.А. Киберпреступность: история уголовно-правового противодействия / В.А. Широков, Е.В. Беспалова [Электронный ресурс]. – Режим доступа: <http://rudocs.exdat.com/docs/index-161949.html>. – Дата доступа: 17.01.2012.
13. Конвенция ООН против транснациональной организованной преступности, 15 ноября 2000 г. // Междунар. право и борьба с преступностью: сб. докл. / сост.: А.В. Змеевский, Ю.М. Колосов, Н.В. Прокофьев. – М.: Междунар. отношения, 2004. – 720 с.
14. UN Manual on the Prevention and Control of Computer-Related Crime (United Nations publication, Sales No. E.94.IV.5) [Electronic resource]. – Mode of access: <http://www.uncjin.org/Documents/EighthCongress.html>. – Date of access: 01.02.2012.
15. Сборник международных соглашений (конвенций) и национальных нормативных правовых актов по вопросам международного сотрудничества в борьбе с преступностью / сост. С.И. Мукашев, И.И. Полетило: в 2 т. – Минск: Акад. МВД Респ. Беларусь, 2005. – Т. 2. – С. 512 – 515.

Поступила 09.08.2012

**INTERNATIONAL COOPERATION IN THE SPHERE OF CRIMINAL STRUGGLE AGAINST
ILLEGAL COMPUTER INFORMATION MISAPPROPRIATION**

M. DUBKO

The article carries out a short analysis of international conventional and institutional collaboration of countries and organizations in the sphere of counteraction to the illegal computer information misappropriation. Besides, it is underlined that the modern computer criminality has an international character, which obliges governments to look for the possibility of cooperation in the sphere of struggle against these crimes. Some perspectives of such an international cooperation are defined.