УДК 343.9
ББК 67.51

DOI 10.22394/1682-2358-2022-2-24-30

D.A. Brekhov, *post-graduate student of the Criminology Department, Kikot Moscow University of the Ministry of Interior of Russia*

PREVENTION OF CRIMES COMMITTED WITH THE USE OF INFORMATION AND COMPUTER TECHNOLOGIES IN CIS COUNTRIES

The article focuses on cyberthreats as a topical type of modern criminal activity. Modern international agreements aimed at countering international cybercrime are analyzed. its prevention and prevention are analyzed. An analysis of the main provisions of the CIS agreements in the field of prevention of crimes committed using information and computer technologies that determine their normative content is carried out. Directions of improving the prevention of crimes committed using information and computer technologies in CIS countries are outlined.

Key words and word-combinations: information and computer technologies, information and telecommunications network, cybercrime, interstate cooperation in the fight against cybercrime, CIS, international crime.

Д.А. Брехов, адъюнкт кафедры криминологии Московского университета МВД России имени В.Я. Кикотя (email: 89266666634@mail.ru)

ПРЕДУПРЕЖДЕНИЕ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ НА ПРОСТРАНСТВЕ СНГ

Аннотация. Рассматриваются киберугрозы как актуальная разновидность современной преступной деятельности. Анализируются современные международные соглашения, направленные на противодействие международной киберпреступности. Проведен анализ основных положений соглашений СНГ в сфере предупреждения преступлений, совершаемых с использованием информационно-компьютерных технологий, определяющих их нормативное содержание. Обозначены направления по совершенствованию предупреждения преступлений, совершаемых с использованием информационно-компьютерных технологий на пространстве СНГ.

Ключевые слова и словосочетания: информационно-телекоммуникационная сеть, киберпреступления, межгосударственное сотрудничество в борьбе с киберпреступностью, СНГ, международная преступность.

Современные процессы глобализации и цифровизации, обусловленные существованием большого технического

потенциала, и безграничные возможности для доступа к любой информации способствуют широкому распространению такого явления, как киберпреступность.

Ввиду глобальности информационно-коммуникационных технологий (ИКТ) киберпреступность приобретает транснациональный характер, что определяет необходимость консолидации мирового сообщества для разработки международных правовых инструментов в борьбе с рассматриваемым явлением.

Впервые вопросы борьбы с преступлениями, совершаемыми с использованием ИКТ, обсуждались на VIII Конгрессе ООН в 1990 г. В 1994 г. было принято Руководство ООН по предупреждению преступлений, связанных с компьютерами, и борьбе с ними [1]. В 2002 г. была принята Резолюция 56 / 261 Генеральной Ассамблеи Организации Объединенных Наций с приложением «Планы действий по осуществлению Венской декларации о преступности и правосудии: ответы на вызовы XXI века» [2], в которой рекомендовалось международному сообществу оказывать интенсивное содействие государствам-участникам в борьбе с преступностью, совершаемой с использованием ИКТ. В частности, сформулированы рекомендации по предотвращению рассматриваемых преступлений на национальном и международном уровнях.

В 2005 и 2010 гг. проблемы предотвращения преступлений, совершаемых с использованием ИКТ, рассматривались на XI и XII конгрессах ООН по предупреждению преступности и обращению с правонарушителями. По их итогам Резолюцией 65 / 230 Генеральной Ассамблеи от 21 декабря 2010 г. была принята Сальвадорская декларация о комплексных стратегиях для ответа на глобальные вызовы: системы предупреждения преступности и уголовного правосудия и их развитие в изменяющемся мире [3].

На региональном уровне впервые вопросы межгосударственного сотрудничества в борьбе с преступлениями, совершаемыми с использованием ИКТ, рассматривались в Соглашении о сотрудничестве государств — участников Содружества Независимых Государств (СНГ) в борьбе с преступлениями в сфере компьютерной информации от 21 июня 2001 г. [4]. В числе важнейших задач была обозначена целесообразность формирования правовых основ сотрудничества государств — участников Соглашения в борьбе с рассматриваемыми преступлениями.

В соответствии со ст. 3 Соглашении составы преступлений в сфере ИКТ можно классифицировать определенным образом (рис. 1).

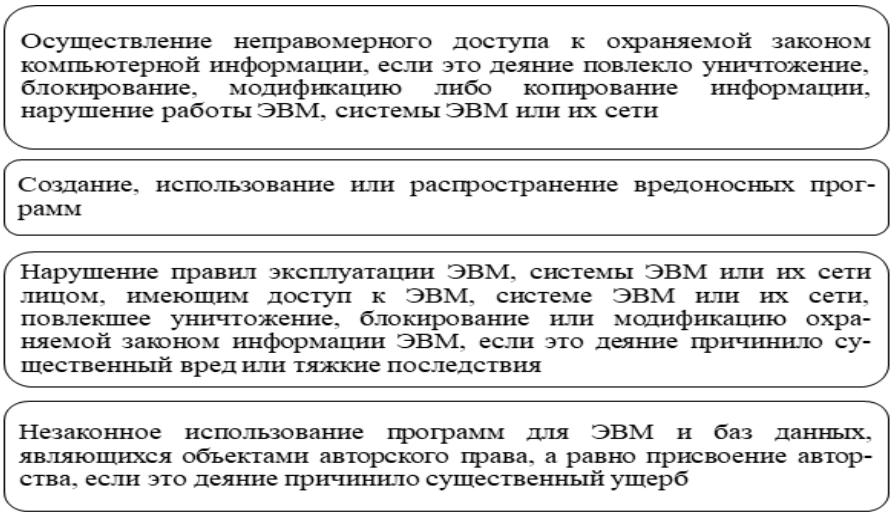

Рис. 1. **Классификация уголовно наказуемых составов преступлений в сфере ИКТ**

В Соглашении обозначены механизмы сотрудничества государств — участников СНГ в предупреждении преступлений, совершаемых с использованием ИКТ на пространстве СНГ (рис. 2).

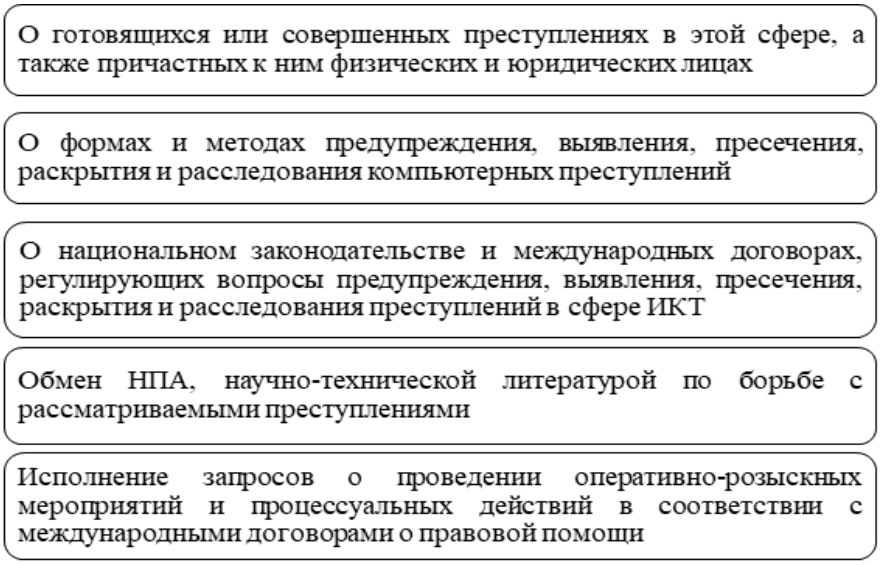

Рис. 2. **Механизмы сотрудничества государств — участников СНГ в предупреждении преступлений, совершаемых с использованием ИКТ**

Некоторые ученые к обозначенным механизмам относят следующие формы сотрудничества:

— планирование и проведение скоординированных мероприятий и операций по предупреждению, выявлению, пресечению, раскрытию и расследованию преступлений в рассматриваемой сфере;

— создание информационных систем, обеспечивающих выполнение задач по предупреждению, выявлению, пресечению, раскрытию и расследованию преступлений в сфере компьютерной информации [5, с. 38].

В Соглашении предусмотрена совместная подготовка и повышение квалификации кадров, например, посредством стажировки специалистов, организации конференций, семинаров и учебных курсов; совместных научных исследований и т.п.

В борьбе с преступлениями, совершаемыми с использованием ИКТ на пространстве СНГ, важное значение имеют модельные законодательные акты Содружества, принимаемые в рамках Межпарламентской Ассамблеи государств — участников СНГ. Например, модельный Уголовный кодекс [6].

В целях развития правовых и организационных основ сотрудничества государств — участников СНГ в борьбе с преступлениями, совершаемыми с использованием ИКТ, была разработана Концепция сотрудничества государств — участников СНГ в борьбе с преступлениями, совершаемыми с использованием ИКТ. В ней обозначены принципы, задачи, основные направления, формы и система обеспечения сотрудничества, направленные на развитие правовых и организационных основ сотрудничества в борьбе с преступлениями, совершаемыми с использованием ИКТ. Система международного информационного сотрудничества выступает базисом для разработки программ и планов совместных действий государств — участников СНГ в борьбе с преступлениями, совершаемыми с использованием ИКТ.

В Концепции определены задачи, основные направления и формы сотрудничества государств — участников СНГ в борьбе с преступлениями, совершаемыми с использованием ИКТ (рис. 3).

В Концепции закреплены следующие формы сотрудничества:

во-первых, предусматривающие обмен оперативной, статистической, научно-методической и иной информацией для пополнения единого банка данных о транснациональных преступных группах и преступных организациях, совершающих преступления с использованием ИКТ;

во-вторых, проведение согласованных следственных действий, комплексных совместных профилактических оперативно-розыскных мероприятий и специальных операций;

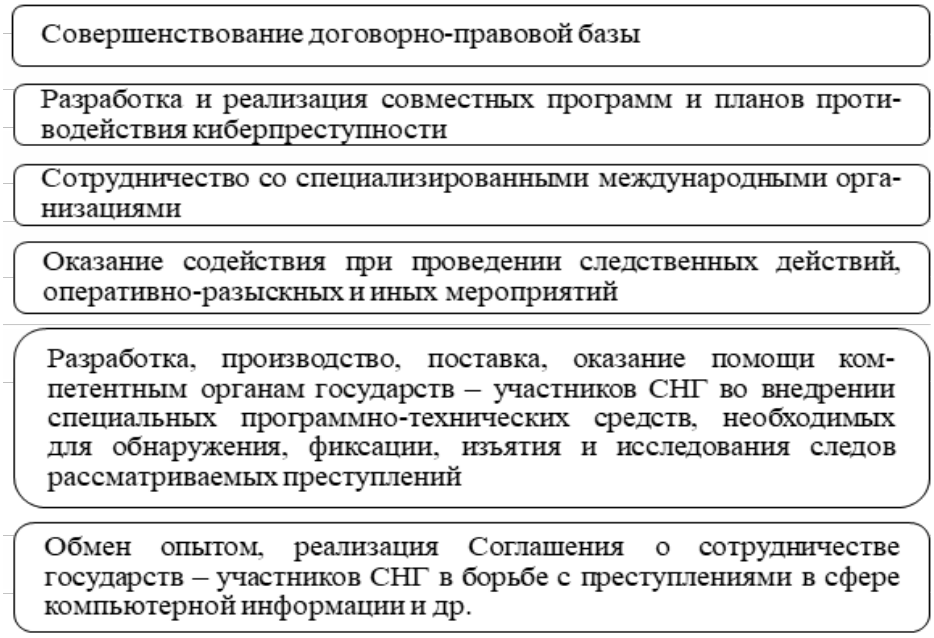

Рис. 3. **Основные направления сотрудничества государств — участников СНГ в борьбе с преступлениями, совершаемыми с использованием ИКТ**

в-третьих, создание и укрепление специализированных подразделений по борьбе с киберпреступностью и оснащение их современными аппаратно-программными и научно-техническими средствами и другое.

В Соглашении уделяется особое значение информационному и научному обеспечению сотрудничества в сфере международной безопасности. Формированию единого специализированного автоматизированного банка данных государств — участников СНГ о транснациональных преступных группах, специализирующихся на совершении преступлений с использованием ИКТ, нераскрытых транснациональных преступлениях, участниках транснациональных преступных групп и отдельных лицах, привлеченных к ответственности за совершение преступлений данного вида [7, с. 74].

Главным направлением совершенствования предупреждения преступлений, совершаемых с использованием ИКТ, является развитие сотрудничества государствами — членами Организации Договора о коллективной безопасности и другими международными организациями.

В качестве примера эффективного взаимодействия в предупреждении преступлений, совершаемых с использованием ИКТ, можно привести специальные операции под кодовым названием «ПРОКСИ» (против криминала в социальной сети), проходящие под официальной

международной эгидой Организации Договора о коллективной безопасности [8, с. 92].

Полагаем, что особую актуальность в рамках совершенствования предупреждения преступлений, совершаемых с использованием ИКТ на территории СНГ, представляет более плотное сотрудничество с Международным многосторонним партнерством против киберугроз (International Multilateral Partnership Against Cyber Threats, IMPACT). Партнерство предоставляет доступ к технической экспертизе, оборудованию и ресурсам для обеспечения эффективной защиты от киберугроз, а также помогает учреждениям ООН обеспечить защиту их ИТ-инфраструктур [9, с. 123].

Проведенный анализ позволил определить тенденции предупреждения преступлений, совершаемых с использованием ИКТ на территории СНГ, представленные на рис. 4.

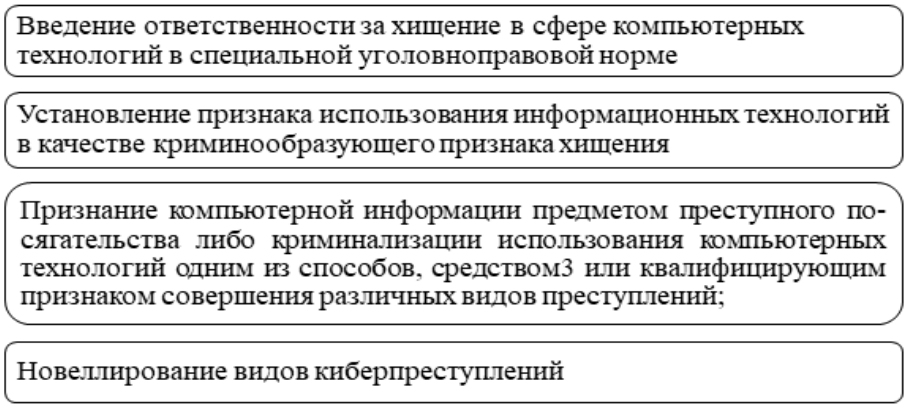

Рис. 4. **Тенденции предупреждения преступлений, совершаемых с использованием ИКТ на территории СНГ**

По нашему мнению, для совершенствования предупреждения преступлений, совершаемых с использованием ИКТ на территории СНГ, необходимы следующие меры:

— на национальном и региональном уровнях совершенствовать правовые конструкции и признаки составов преступлений;

— предусмотреть в национальных уголовных законодательствах компьютерные преступления, перечисленные в рассматриваемом Соглашении государств — участников СНГ, и рекомендуемые модельным законодательным актом Содружества.

Кроме того, целесообразно принять в рамках СНГ новое Соглашение в борьбе с преступлениями, совершаемыми с использованием ИКТ, где предусмотреть следующие аспекты: во-первых, перечень преступлений, связанных с распространением детской порнографии; во-вторых, новые

виды киберпреступлений, получающие распространение при использовании таких методов, как «облачные технологии» (Bluetooth, беспроводные сети связи Wi-Fi, WiMAX, пиринговые файлообменные сети, спам); в-третьих, новые виды преступлений, отражающие современные проблемы обеспечения безопасности в сфере компьютерной информации.

Для дальнейшего эффективного предупреждения преступлений, совершаемых с использованием ИКТ на территории СНГ, следует совершенствовать работу по формированию организационных и правовых основ межгосударственного информационного сотрудничества, пресечению преступлений, совершаемых с использованием ИКТ.

Библиографический список

1. Руководство Организации Объединенных Наций по предупреждению преступлений, связанных с применением компьютеров, и борьбе с ними // Международный обзор уголовной политики. 1994. № 43, 44.

2. Планы действий по осуществлению Венской декларации о преступности и правосудии: ответы на вызовы: Резолюция Генеральной Ассамблеи ООН 56 / 261 от 15 апр. 2002 г. Приложение XI: Меры по борьбе с преступлениями, связанными с использованием высоких технологий и компьютеров. URL: http://www.un.org/ru/documents/ods.asp?m=A/RES/56/261

3. Сальвадорская декларация о комплексных стратегиях для ответа на глобальные вызовы: системы предупреждения преступности и уголовного правосудия и их развитие в изменяющемся мире / принята Резолюцией 65 / 230 Генеральной Ассамблеи ООН от 21 дек. 2010 г. URL: http://www.un.org/ru/documents/decl_conv/declarations/salvador_declaration.shtml

4. Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации от 21 июня 2001 г. // Единый реестр правовых и других актов Содружества Независимых Государств. URL: http://www.un.org/russian/news/fullstorynews.asp?newsID=14417.

5. *Волеводз А.Г.* Уголовное законодательство об ответственности за компьютерные преступления: опыт разных стран // Правовые вопросы связи. 2004. № 1. С. 37–48.

6. Модельный Уголовный кодекс, рекомендательный законодательный акт / принят на седьмом пленарном заседании Межпарламентской Ассамблеи государств – участников Содружества Независимых Государств 17 февр. 1996 г. // Единый реестр правовых и других актов Содружества Независимых Государств. URL: http://www.un.org/russian/news/fullstorynews.asp?newsID=14417

7. *Зинина У.В.* Преступления в сфере компьютерной информации в российском и зарубежном уголовном праве. М., 2017.

8. Киберпреступность: риски и угрозы: материалы Всероссийского студенческого круглого научно-практического стола с международным участием (Санкт-Петербург, 11 февр. 2021 г.) / Северо-Западный филиал ФГБОУВО «Российский государственный университет правосудия»; под ред. Е.Н. Рахмановой. СПб., 2021.

9. Развитие и деятельность Содружества Независимых Государств в 2013 г.: сборник информационно--аналитических материалов / Исполнительный комитет СНГ; под ред. А.К. Заварзина. Минск, 2014. № 2.