УДК 351.341

ТРАНСНАЦИОНАЛЬНАЯ ОРГАНИЗОВАННАЯ ПРЕСТУПНОСТЬ В КОНТЕКСТЕ СОВРЕМЕННЫХ РИСКОВ, ВЫЗОВОВ И УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ГОСУДАРСТВ

В.В. Меркушин

Белорусский государственный университет,
пр. Независимости 4, Минск, 220030, Беларусь

В статье определяются и анализируются современные риски и иные деструктивные воздействия транснациональной организованной преступности на информационную безопасность государств. Предлагаются актуальные теоретико-прикладные и международно-правовые инициативы по противодействию транснациональной организованной преступности в данной сфере.

***Ключевые слова*:** транснациональная организованная преступность, информационная безопасность, угрозы информационной безопасность, международное право.

TRANSNATIONAL ORGANIZED CRIME IN THE CONTEXT OF MODERN RISKS, CHALLENGES AND THREATS TO INFORMATION SECURITY OF STATES

V.V. Merkushin

Belarusian State University,
4 Nezalezhnosti Avenue, Minsk, 220030, Belarus

The article defines and analyzes modern risks and other destructive effects of transnational organized crime on the information security of states. Topical theoretical, practical and international legal initiatives to counter transnational organized crime in this area are proposed.

Keywords: transnational organized crime, information security, threats to information security, international law.

«Кто владеет информацией, тот владеет миром»
Натан Майер Ротшильд

В современных условиях активной эволюции научно-технического прогресса, информатизации современного общества, широкомасштабного доступа к интернет-ресурсам (легальным и нелегальным) [1, с. 5], подключения пользователей большинства стран к глобальным электронным платежным системам и пр., объективизировалась в качестве самостоятельной

сфера высоких технологий, способствовавшая модернизации использования киберпространства и релевантно связанных с ним общественно-опасных деяний – киберпреступлений [2 (пп. 41-42); 3 (п. 6); 4 (п. 9 (b)); 5, с. 44; 6; 7]. Отсюда, «актуализирующаяся проблема борьбы с ними из внутригосударственной превратилась в международную» (А.Г. Волеводз) [8, с. 16], чему способствует перманентное увеличение числа данного рода преступлений, закономерно приобретающих организованный транснациональный характер [9, с. 5; 10; 11; 12].

Более того, как отмечено в Специальном докладе: кибервойны в C-Suite [13], опубликованном в журнале Cybercrime: «глобальные расходы на киберпреступность будут расти на 15% в год в течение следующих пяти лет, достигнув $10,5 трлн в год к 2025 г., по сравнению с $3 трлн в 2015 г. Это представляет собой крупнейшую передачу экономического богатства в истории, ставит под угрозу стимулы для инноваций и инвестиций, экспоненциально превышает ущерб, причиненный стихийными бедствиями за год, и будет более прибыльным, чем глобальная торговля всеми основными незаконными наркотиками вместе взятыми». При этом, С. Морган (главный редактор Cybercrime) особо подчеркивает, что оценка такого ущерба произведена на основе хронологии развития соответствующих статистических данных, включая недавний рост в годовом исчислении (за последние 10 лет – прим. автора), резкого увеличения хакерской деятельности, спонсируемой враждебными национальными государствами и организованными преступными группировками [13].

На сегодняшний день, одной из важнейших составляющих элементов сферы высоких технологий[2], способной напрямую испытать на себе риски воздействий данных противоправных деяний, является инфраструктура информационной безопасности. Особенно в тех случаях, когда антагонистическими субъектами (источниками) выступают коллективные образования, как собственно преступные, так и легальные, но потенциально способные стать таковыми. В данном случае, с одной стороны, речь идет о своеобразных симбиотических связях традиционных [транснациональных] преступных групп с аналогичными сетевыми группами киберпреступников[3]**.** Они, напрямую или анонимно могут сотрудничать в любой точке мира с целью совершения совместных криминальных операций. Причем, использование информационно-коммуникационных технологий (ИКТ) значительно

[2] От англ. *high technology, high tech, hi-tech.* Сфера высоких технологий включает: собственно электроника, программное обеспечение, IT-технологии, смежные с IT-сферой направления (микро-, опто- и наноэлектроника, мехатроника, передача данных, радиолокация, радионавигация, радиосвязь, информационно-коммуникационные технологии, и др.), а также защита информации и создание центров обработки данных (Источник: Парк высоких технологий сегодня. URL:https://www.park.by/htp/about/. - (accessed: 25.05.2022).

[3] Например, Anonymous, LulzSec, NSO Group Technologies, Chaos Computer Club, РедХак, Киберберкут, OurMine, Lizard Squad, Cult of the Dead Cow, Сирийская электронная армия, Power Racing Series, MilwOrm, Israeli Elite Force, Derp, и др.

упрощает, а в иных случаях, устраняет, правовые и организационные «барьеры» для проникновения, как на легальные, так и нелегальные рынки товаров и услуг. С другой стороны, в определенных случаях, новые [квази]-субъекты транснациональной организованной преступности – транснациональные корпорации, частные военные и охранные компании и неправительственные международные организации [14, с. 3-10], используя свои ресурсы, возможности и опираясь окончательно неурегулированный свой [международно]-правовой статус, находятся в перечне рисков и потенциальных угроз информационной безопасности, устойчиво превалируя в сторону последних. Указанные субъекты могут выступать как автономно, в собственных корпоративных интересах, так и в форме соучастия особого рода (sui generis), формируя «теневые» бизнес-модели с использованием коррупционных связей в международных и национальных структурах.

На этом фоне, данные субъекты в той или иной степени, склонны к совершению таких уже достаточно распространенных противоправных деяний, как - мошенничество с электронной почтой и интернет-мошенничество, мошенничество с использованием личных данных (кража и злонамеренное использование личной информации), кража финансовых данных или данных банковских карт, кража и продажа корпоративных данных, кибершантаж (требование денег для предотвращения кибератаки), атаки программ-вымогателей (тип кибершантажа), криптоджекинг (майнинг криптовалюты с использованием чужих ресурсов без ведома их владельцев), кибершпионаж (несанкционированное получение доступа к данным государственных или коммерческих организаций) [15]. При этом, по мнению отдельных ученых-экспертов, современная проблема транснациональной организованной преступности еще усугубляется постоянно растущей глобальной связью, предоставляемой ИКТ, безграничной сферой киберпространства и низкими рисками раскрытия и привлечения к ответственности правоохранительными органами [16].

На сегодняшний день, проблематика противодействия транснациональной организованной киберпреступности, в том числе и в контексте обеспечения информационной безопасности, остается практически неизученной в отечественной и российской доктрине международного права, за исключением отдельных подходов и частно-научных точек зрения, обоснованных и разрабатываемых белорусскими, российскими и иными юристами-международниками Е.Ф. Довгань [17], Н.О. Мороз [18], А.Г. Волеводз [8], Д.М. Валеев [19], Е.Е. Королькова [20], О.В. Мозолина [21], Т.Б. Сеитов [22] и др.

Вместе с тем, вопросы информационной безопасности стала достаточно популярной в науке уголовного права, криминологии, криминалистики, а также оперативно-розыскной деятельности и теории обеспечения

национальной безопасности (например, Ю.Н. Жданов, С.К. Кузнецов, В.С. Овчинский [23], В.Е. Козлов [24], В.И. Третьяков [25], А.В. Варданян [26], Т.Л. Тропина [27], О.А. Степанов [28], А.В. Табаков [29], В.Г. Гавриленко [30] и др.), а также западными учеными-экспертами в рамках международных проектов исследований киберпреступности [31; 32].

Отсюда, заявленная проблематика, отражает цель настоящего исследования – изучение основных рисков транснациональной организованной преступности и иных факторов, воздействующих на информационную безопасность государств и их теоретико-правовое обоснование.

Основная часть

Проблематика угроз транснациональной организованной преступности на безопасность государств стала перманентной темой различных повесток дня, вызывающей наиболее пристальное внимание со стороны стран мирового сообщества, начиная с 90-х гг. XX – начала XXI вв. Этому послужили, во-первых, проведение IX Конгресса ООН по предупреждению преступности и обращению с правонарушителями (Каир, 29 апреля – 5 мая 1995 г.) и предшествовавшей ему Всемирной конференции на уровне министров по организованной транснациональной преступности (Неаполь, 21-23 ноября 2004 г.). Эти события актуализировали угрозы транснациональной организованной преступности, предложив их рассматривать в качестве международной в различных сферах межгосударственных отношений, в том числе и информационной. Во-вторых, принятие и подписание Конвенции ООН против транснациональной организованной преступности от 15 ноября 2000 г. зафиксировала рассматриваемое явление в качестве сформировавшегося международно-правового феномена, создав юридическую основу для его дальнейших комплексных научных исследований с различных сторон. Одна из них сфера информационной безопасности, степень рисков воздействия на которую со стороны транснациональной организованной преступности представляется достаточно высокой, а в некоторых случаях – угрожающей. В последнем случае, при условии взаимодействия организованных преступных групп с террористическими организациями, экстремистскими группами и радикально настроенными антиобщественными движениями и ассоциациями. Однако важно учитывать в качестве приоритетной все же экономическую ориентированность транснациональной организованной преступности и ее устойчивые корыстные интересы, направленные на получение максимальных прибылей в результате своей противоправной, латентной деятельности. Поэтому на данном этапе исследования было бы правильнее говорить о значительных рисках информационной безопасности [государств] от транснациональной организованной преступности, чем о непосредственных (экзистенциональных) угрозах. При этом, необходимо учитывать тот факт, что в международно-правовых документах, как правило, не проводят

принципиальных различий между понятиями «угрозы», «опасности», «риски», «вызовы», используя их в комплексе и руководствуясь их близким смысловым содержанием. А применительно к рассматриваемой теме, например, существует еще термин «факторы уязвимости», способные создавать «новые проблемы в плане безопасности» [32]. А именно - преодоление «цифровой пропасти» для обеспечения универсального доступа к информационно-коммуникационным технологиям и для защиты важнейших информационных инфраструктур путем облегчения передачи информационных технологий развивающимся странам, особенно наименее развитым странам, и наращивания их потенциала в вопросах передовой практики и профессиональной подготовки в области кибербезопасности [32] и др. Учитывая при этом тот факт, что обеспечение защищенности важнейших информационных инфраструктур – это обязанность, которую правительства должны систематически выполнять, выступая с соответствующими инициативами на национальном уровне, в координации с заинтересованными сторонами, которые, в свою очередь, должны знать о соответствующих рисках, превентивных мерах и эффективных мерах реагирования [32] …

Так, например, вполне закономерно, Концепция информационной безопасности Республики Беларусь от 18 марта 2019 г. [33], базируясь на Концепции национальной безопасности Республики Беларусь от 9 ноября 2010 г. (п. 6) [34], рассматривает в качестве преступлений в информационной сфере преступления против информационной безопасности (киберпреступления) и иные преступления, предметом или средством совершения которых являются информация, информационные системы и сети (п. 8), не обходит стороной и транснациональный сегмент данных противоправных деяний. В том числе, совершаемых в составе преступных групп. В частности, говоря о мерах противодействия киберпреступности (гл. 19 Концепции) в рамках реализации международного и регионального сотрудничества в сфере кибербезопасности, Концепция акцентирует внимание на важности отслеживания деятельности преступных групп и отдельных преступников, действующих в киберпространстве (п. 74).

Это обосновывает определение в перечне основных источников угроз в области обеспечения безопасности информационных ресурсов «деятельность отдельных лиц, преступных групп, недобросовестных отечественных и иностранных организаций, объединений или сообществ, направленную на получение неправомерного доступа к этим ресурсам в политических, военных, коммерческих, личных и иных целях…» (п.79).

Идентичный подход присутствует и в Доктрине информационной безопасности Российской Федерации от 5 октября 2016 г. [35] В разделе III (Основные информационные угрозы и состояние информационной безопасности) данной Доктрины, с точки зрения исследуемой проблематики,

существенное значение имеет указание с одной стороны, на транснациональный характер незаконных деяний против информации, широкий спектр и масштаб их применения; с другой - возможности трансграничного оборота информации все чаще используются для достижения геополитических, противоречащих международному праву военно-политических, а также террористических, экстремистских, криминальных и иных противоправных целей в ущерб международной безопасности и стратегической стабильности (ст. 10). В нашем случае, еще немаловажна фокусировка Доктрины на криминальном аспекте такой деятельности, включающий: а) рост компьютерной преступности, прежде всего в кредитно-финансовой сфере, б) увеличение числа преступлений, связанных с нарушением конституционных прав и свобод человека и гражданина, в том числе в части, касающейся неприкосновенности частной жизни, личной и семейной тайны, при обработке персональных данных с использованием информационных технологий (ст. 14).

Причем, в новом правовом документе Российской Федерации в сфере обеспечения национальной безопасности – «Стратегии национальной безопасности Российской Федерации», от 2 июля 2021 г. [36] (раздел IV. «Обеспечение национальной безопасности» (п. 47 раздела: Государственная и общественная безопасность)), вполне оправдано то, что в качестве одной из специальных практических задач предусматриваются на федеральном уровне меры по предупреждению и пресечению правонарушений и преступлений, совершаемых с использованием информационно-коммуникационных технологий, в том числе легализации преступных доходов, финансированию терроризма, организации незаконного распространения наркотических средств и психотропных веществ, а также использованию в противоправных целях цифровых валют (пп.11).

Приведенные тезисы соответствует положениям Конвенции ООН против транснациональной организованной преступности 2000 г. В ней, частности, закреплены два важнейших системообразующих элемента в обозначении контура феномена транснациональной организованной преступности:

Квалификация преступления в качестве транснационального. Согласно п. 2 ст. 3 Конвенции, «преступление носит транснациональный характер, если: а) оно совершено в более чем одном государстве; б) оно совершено в одном государстве, но существенная часть его подготовки, планирования, руководства или контроля имеет место в другом государстве; в) оно совершено в одном государстве, но при участии организованной преступной группы, которая осуществляет свою преступную деятельность в более чем одном государстве; г) оно совершено в одном государстве, но его существенные последствия имеют место в другом государстве» [37].

Определение цели участия в организованной преступной группе. В соответствии с Конвенцией – это получение прямо или косвенно, в результате совершения какого-либо преступления, финансовой или иной материальной выгоды ((п.а) ст. 2).

Представляется очевидной возможность применения положений Конвенции и к киберпреступлениям, что в ряде случаев позволяет относить их к одним из [современных] форм собственно транснациональной [организованной] преступности. Последняя, как отмечалось, a priori представляя угрозу экономическому сектору безопасности государств [38], между тем интегрируется по обоснованному мнению профессора Е.Ф. Довгань еще и в систему современных вызовов и угроз в сфере военно-политической безопасности [17, с. 11], что с точки зрения другого белорусского ученого Н.О. Мороз свидетельствует уже о ее комплексном виде угроз [18, с. 7].

В подтверждение сказанному, приведем мнение одного из ведущих мировых специалистов в сфере информационной безопасности, являющегося также одним из учредителей, основным владельцем и действующим главой АО «Лаборатория Касперского», Е.В. Касперского. Он полагает: «Наиболее важным критерием любого бизнеса является прибыльность. И киберпреступление не является исключением» [39]. Е.В. Касперский также обосновано поддерживает опасения по поводу угрозы киберпреступности (ее кибератак) на критически важные объекты инфраструктуры, которая может привести к катастрофическим последствиям [40] и поддерживает идею (на наш взгляд несколько идеалистическую) о выработки и заключения межгосударственного соглашения о нераспространении кибероружия, считая, что мировое сообщество должно положить конец гонке кибервооружений и противодействовать эскалации киберугроз на глобальном уровне [41].

В целом соглашаясь с мнением Е.В. Касперского, отметим тот факт, что на сегодняшний день в международном праве по вопросам противодействия киберпреступности, особенно ее транснациональным, организованным структурам, отмечается адресно-целевая неурегулированность. В первую очередь, об этом свидетельствует отсутствие единого специализированного международно-правового документа с одной стороны, региональным характером и ограниченным кругом участников существующих конвенций, соглашений – с другой (например, Конвенция Совета Европы о преступности в сфере компьютерной информации ETS №185 (Будапешт, 23 ноября 2001 г.) и Дополнительный протокол к ней «О введении уголовной ответственности за правонарушения, связанные с проявлением расизма и ксенофобии, совершенные посредством компьютерных сетей» от 21 января 2003 г., Соглашение о сотрудничестве государств-участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации от 1 июня 2001 г., Конвенция Африканского союза о

кибербезопасности и защиты персональных данных от 27 июня 2014 г. (вступила в силу 3 июня 2019 г.) и др.).

Приведем некоторые обоснованные точки зрения. Так, на сегодняшний день, в международном праве выделяют 21 состав преступлений в сфере высоких технологий, содержащихся в различных международных соглашениях, 20 относятся к преступлениям международного характера и одно к международным преступлениям [42, с. 7]. В частности, по мнению отдельных экспертов, совершение акта международного терроризма при помощи информационно-коммуникационных технологий («кибертерроризма» или «информационно-электронного терроризма» [43, с. 3]) является международным преступлением, поскольку объектом такого преступления является международный мир и безопасность [42, с. 15]. Вместе с тем, преступления международного характера (в иной трактовке – транснациональные преступления [44, p. 56]) не что иное, как основные формы деятельности (проявления) самой транснациональной организованной преступности (например, торговля людьми, незаконная торговля оружием, наркотиками, «отмывание» денег, коррупция, преступления против правосудия и т.д.).

Руководствуясь вышеприведенными данными и наращиванием международно-правового потенциала по противодействию [транснациональной организованной] киберпреступности в целом, а в нашем случае - в сфере информационной безопасности, отметим еще некоторые, имеющие достаточно важное значение, положения международно-правовых документов. В первую очередь, стоит отметить Глобальную Программу ООН по киберпреступности 2017 г. [45]. Ее принятие было обусловлено, во-первых, сложным характером киберпреступности, действующей в неограниченном киберпространстве и усугубляемом ростом организованных преступных групп. Во-вторых, необходимостью гибкого реагирования на выявленные потребности в развивающихся странах (в первую очередь, Центральной Америки, Восточной Африки, БВСА, Юго-Восточной Азии и Тихого океана). В-третьих, достижением ее основных целей: 1) повышение эффективности и действенности расследования, судебного преследования и судебного разбирательства по делам о киберпреступлениях, особенно о сексуальной эксплуатации детей в Интернете и надругательствах над ними, в рамках надежной системы прав человека; 2) эффективное и действенное общегосударственное реагирование на киберпреступность в долгосрочной перспективе, включая национальную координацию, сбор данных и эффективную правовую базу, что ведет к устойчивому реагированию и усилению сдерживания; 3) укрепление национальных и международных связей между правительством, правоохранительными органами и частным сектором с повышением осведомленности общественности о рисках киберпреступности.

Кроме того, в соответствии с резолюцией 65/230 Генеральной Ассамблеи [46] и резолюциями 22/7 и 22/8 Комиссии по предупреждению преступности и уголовному правосудию соответственно [47; 48], Глобальная программа по киберпреступности уполномочена оказывать помощь государствам-членам в их борьбе с преступлениями, связанными с киберпреступностью, посредством наращивания потенциала и оказания технической помощи [45].

В этой связи, фокусируясь на исследуемой проблематике, отметим, что в резолюции, принятой Генеральной Ассамблеей ООН 74/173 от 19 декабря 2019 г. с удовлетворением отмечались «усилия Управления Организации Объединенных Наций по наркотикам и преступности, направленные на реализацию Глобальной программы борьбы с киберпреступностью в целях выполнения его мандата по оказанию технической помощи и наращиванию потенциала в области борьбы с киберпреступностью», и что Конвенция ООН против транснациональной организованной преступности 2000 г. «представляет собой инструмент, который могут использовать государства-участники для налаживания международного сотрудничества в деле предупреждения транснациональной организованной преступности и борьбы с ней и который для ряда государств-участников может быть использован в рамках некоторых дел о киберпреступности» [49].

В этой связи нам видится оптимальным и практически целесообразным, исходя из анализированной выше специфики исследуемой проблемы, разработать и принять на обсуждение проект Протокола против использования информационно-коммуникационных технологий в преступных целях, особенно киберпреступлений, дополняющий Конвенцию Организации Объединенных Наций против транснациональной организованной преступности 2000 г.

Однако, учитывая тот факт, что в настоящий момент в рамках Специального комитета [50] по разработке Всеобъемлющей Международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях идет плановая работа (1 сессия, Нью-Йорк, 28 февраля-11 марта 2022 г., 2 сессия, Вена, 30 мая-10 июня 2022 г., 3 сессия, Нью-Йорк, 29 августа-9 сентября 2022 г.) строить иллюзии относительно ее окончательной разработки и своевременного принятия заинтересованными государствами представляется, на наш взгляд, преждевременным. Не смотря на то, что, например, Российская Федерация разработала и внесла в Специальный комитет ООН свой проект конвенции о борьбе с киберпреступностью [51]. Предложение озаглавлено «Конвенция ООН о противодействии использованию информационно-коммуникационных технологий в преступных целях». Это предложение, как сообщается, призывает государства-члены сконструировать внутреннее законодательство для

наказания за ряд конкретных преступлений, связанных с киберпреступностью. Причем, их перечень намного шире, чем те, которые признаны международным правом на данный момент времени. Российский проект представляет собой 55-страничный документ, который охватывает целый ряд вопросов, включая определение 23 видов киберпреступлений, описание процедур между различными странами по выдаче преступников (хакеров), а также оказание правовой помощи по уголовным делам, таким как выявление преступлений, арест и возвращение активов.

Высказанное сомнение обусловлено, с одной стороны, происходящими в настоящее время глобальными общественными трансформациями в странах мирового сообщества, вызванные возрастающим противостоянием стран НАТО под лидерством США против Российской Федерации и ее союзников. С другой стороны, используемые США и их союзниками информационно-коммуникационные технологии умышленно ставятся вне правового поля, подменяя их приоритетностью собственных интересов в сфере квази-национальной безопасности, а латентно – в интересах бенефициаров различного рода корпоративных структур и их аффилированных негосударственных субъектов. Это однозначно нивелирует значимость концепции примата международного права в разрешении любых межгосударственных споров и конфликтов.

Вместе с тем, наше предложение о внесении соответствующего проекта Протокола, дополняющего Конвенцию против транснациональной организованной преступности 2000 г., не противоречит цели самой Конвенции (ст.1), соответствует сферам ее применения (ст. 3), а по состоянию на 19 сентября 2017 года она насчитывает 190 участников, что свидетельствует о ее юридической состоятельности. Разумеется, предлагаемый проект Протокола будет направлен на решение только на определенную часть проблем в рассматриваемой области, однако проблем весьма значимых, актуальных и уже имеющих устойчивую юридическую основу.

Заключение

Предпринятая попытка исследования проблем транснациональной организованной преступности в контексте рисков информационной безопасности безусловно является актуальной, малоизученной и требующей дальнейших предметных исследований с точки зрения международного права, в первую очередь, основываясь на его таких отраслях как право международной безопасности, международное уголовное право и международное гуманитарное право.

В целях придания системности и наполнения определенным смысловым содержанием понятий: «вызовы», «угрозы», «опасности», «риски», «факторы уязвимости», представляется целесообразным их закрепление в разрабатываемом в настоящее время проекте Всеобъемлющей

международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях в силу ее в большей степени ожидаемого декларативного характера.

В качестве практических шагов по противодействию транснациональной организованной преступности в данной сфере, устойчивости и обоснованности международно-правовой позиции Республики Беларусь, предлагается разработка проекта Протокола против использования информационно-коммуникационных технологий в преступных целях, особенно киберпреступлений, дополняющий Конвенцию Организации Объединенных Наций против транснациональной организованной преступности 2000 г.

Библиографический список

1. Арчаков, В.Ю. Даркнет в контексте рисков национальной безопасности / В.Ю. Арчаков, А.Л. Баньковский, Е.В. Зенченко // Право.by. – 2021. – №6(74). – С. 5-10.

2. Сальвадорская декларация ООН о комплексных стратегиях для ответа на глобальные вызовы: системы предупреждения преступности и уголовного правосудия и их развитие в изменяющемся мире [Электронный ресурс]: принята резолюцией Генер. Ассамблеи ООН, 21 дек., 2010 г. №65/230 // Организация Объединенных Наций. – Режим доступа: https://www.un.org/ru/documents/decl_conv/declarations/salvador_declaration.shtml. - Дата доступа: 08.11.2022.

3. Предварительная повестка дня двадцатой сессии Комиссии ООН по предупреждению преступности и уголовному правосудию: «Мировые тенденции в области преступности и новые проблемы в области предупреждения преступности и уголовного правосудия и способы их решения» [Электронный ресурс]: 11-15 апреля 2011 г., E/CN.15/2022/1 // Организация Объединенных Наций. – Режим доступа: https://www.unodc.org/documents/commissions/CCPCJ/CCPCJ_Sessions/CCPCJ_24/resolutions/L11_Rev1/ECN152015_L11_r_V1503512.pdf. - Дата доступа: 08.11.2022.

4. Дохинская декларация ООН о включении вопросов предупреждения преступности и уголовного правосудия в более широкую повестку дня Организации Объединенных Наций в целях решения социальных и экономических проблем и содействия обеспечению верховенства права на национальном и международном уровнях, а также участию общественности [Электронный ресурс]: 12-19 апреля 2015 г., A/CONF.222/L.6 // Организация Объединенных Наций. – Режим доступа: https://www.unodc.org/documents/congress/Declaration/V1504153_Russian.pdf. - Дата доступа: 08.11.2022.

5. Руководство для дискуссий: док. ООН A/CONF.234/PM.1 // Четырнадцатый Конгресс Организации Объединенных Наций по предупреждению преступности и уголовному правосудию, Киото, Япония, 20-27 апреля 2020 г. [Электронный ресурс] // Организация Объединенных Наций. –Режим доступа: https://undocs.org/pdf?symbol=ru/A/CONF.234/PM.1. – Дата доступа: 07.11.2022.

6. Конвенция Совета Европы о киберпреступности (в отдельных источниках трактуется как Конвенция о преступности в сфере компьютерной информации) [Электронный ресурс]: 23 ноября 2001 г., ETS № 185. – Режим доступа: http://base.garant.ru/4089723/. - Дата доступа: 08.11.2022.

7. Доклад межправительственной группы экспертов открытого состава о всестороннем исследовании проблемы киберпреступности и ответных мер со стороны государств-членов, международного сообщества и частного сектора. Двадцатая сессия

Комиссии Организации Объединенных Наций по предупреждению преступности и уголовному правосудию [Электронный ресурс]: 11-15 апреля 2011 г., E/CN.15/2011/19 // Организация Объединенных Наций. – Режим доступа: https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/UNODC_CCPCJ_EG4_2013_2_R.pdf. – Дата доступа: 07.11.2022.

8. Волеводз, А.Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества / А.Г. Волеводз. – М.: ООО «Юрлитинформ», 2001. – 496 с.

9. Глобальная программа кибербезопасности [ГПК] МСЭ: Основа для международного сотрудничества в области кибербезопасности. Международный союз электросвязи. Отдел корпоративной стратегии. Place des Nations. CH-1211 Geneva 20 [Электронный ресурс]. – Режим доступа: https://ifap.ru/pr/2008/080908aa.pdf. – Дата доступа: 07.11.2022.

10. Межгосударственная программа совместных мер по борьбе с преступностью на 2019-2023 [Электронный ресурс]. - Режим доступа: https://e-cis.info/cooperation/3192/83381/. - Дата доступа: 08.11.2022.

11. Kramer, A.E. Cyberweapon Warning From Kaspersky, a Computer Security Expert /A.E. Kramer. The New York Times (3 June 2012).

12. The Globalization of Crime: A Transnational Organized Crime Threat Assessment (United Nations Office on Drugs and Crime) [Electronic resource]. – Mode of access: https://www.unodc.org/documents/data-and-analysis/tocta/TOCTA_Report_2010_low_res.pdf. - Date of access: 08.11.2022.

13. Cybercrime to cost the world $10.5 trillion annually by 2025: special report: cyberwarfare in the c-suite. Sausalito, Calif. – Nov. 13, 2020 [Electronic resource]. – Mode of access: https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025// - Date of access: 08.11.2022.

14. Меркушин, В.В. О некоторых проблемах международно-правового регулирования противодействия транснациональной организованной преступности в контексте обеспечения безопасности государств / В.В. Меркушин // Журнал международного права и международных отношений. 2021. 3(98). С. 3–10.

15. Советы по защите от киберпреступников [Электронный ресурс]. - Режим доступа: https://www.kaspersky.ru/resource-center/threats/what-is-cybercrime. - Дата доступа: 08.11.2022.

16. Овчинский, В. Организованная киберпреступность / В. Овчинский, Ю. Жданов [Электронный ресурс]. - Режим доступа: https://zavtra.ru/blogs/organizovannaya_kiber-prestupnost_ - Дата доступа: 08.11.2022.

17. Довгань, Е.Ф. Международные организации и поддержание международного мира и безопасности: моногр. / Е.Ф. Довгань. – Минск: Междунар. ун-т «МИТСО», 2016. – 262 с.

18. Мороз, Н.О. Международно-правовое сотрудничество в борьбе с преступностью в сфере высоких технологий: моногр. / Н.О. Мороз. – Минск: Междунар. ун-т «МИТСО», 2017. – 266 с.

19. Валеев, Д.М. Международно-правовые основы сотрудничества по борьбе с транснациональной организованной преступностью: дис. канд. юрид. наук: 12.00.10 / Д.М. Валеев. – Казань, 2016. – 227 с.

20. Королькова, Е.Е. Международно-правовое регулирование деятельности частных военных и охранных компаний: дис. … канд.юрид. наук: 12.00.10 / Е.Е. Королькова. – М., 2019. – 212 с.

21. Мозолина, О.В. Публично-правовые аспекты международного регулирования отношений в Интернете: автореф. дисс. … канд. .юрид. наук: 12.00.10 / О.В. Мозолина. – М., 2008. – 26 с.

22. Сеитов, Т.Б. Международно-правовое сотрудничество государств в борьбе с компьютерной преступностью: автореф. дисс. … канд. юрид. наук: 12.00.10 / Т.Б. Сеитов. – Алматы, 2002. – 23 с.

23. Жданов, Ю.Н. COVID-19: преступность, кибербезопасность, общество, полиция / Ю.Н. Жданов, [и др.]. – М.: Междунар. отношения, 2020. – 448 с.

24. Козлов, В.Е. Противодействие компьютерной преступности: проблемы и пути их разрешения: монография / В.Е. Козлов. – Минск: Акад. МВД Респ. Беларусь, 2006. – 256 с.

25. Третьяков, В.И. Организованная преступность и легализация криминальных доходов: автореф. дис. ... доктора юрид. наук: 12.00.08 / В.И. Третьяков. – Ростов-на-Дону, 2009. – 56 с.

26. Варданян, А.В. Расследование преступлений в сфере высоких технологий и компьютерной информации / А.В. Варданян, Е.В. Никитина. – М.: Юрлитинформ, 2007. – 307 с.

27. Тропина, Т.Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы / Т.Л. Тропина. – Владивосток: Изд-во Дальневосточного ун-та, 2009. – 237 с.

28. Степанов, О.А. Теоретико-правовые аспекты безопасного функционирования и развития информационно-электронных систем: автореф. дис. ... доктора юрид. наук: 12.00.01 / О.А. Степанов. – М., 2005. - 53 с.

29. Табаков, А.В. Современное состояние и основные тенденции развития транснациональной организованной наркопреступности: моногр. / А.В. Табаков; СПбГАСУ. – СПб., 2018. – 259 с.

30. Гавриленко, В.Г. Правовые основы и механизмы обеспечения национальной безопасности и суверенитета Республики Беларусь / В.Г. Гавриленко. – Минск: Право и экономика, 2019. – 1104 с.

31. Всестороннее исследование проблемы киберпреступности: проект, февраль [Электронный ресурс]: Вена, 2013 г. // Управление ООН по наркотикам и преступности. - Режим доступа: https://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime_Study_Russian.pdf. – Дата доступа: 08.11.2022.

32. Создание глобальной культуры кибербезопасности и защита важнейших информационных структур [Электронный ресурс]: резолюция Генер. Ассамблеи ООН, 23 дек. 2003 г., №58/199 // Организация Объединенных Наций. – Режим доступа: https://undocs.org/ru/A/RES/58/199. - Дата доступа: 08.11.2022.

33. О Концепции информационной безопасности Республики Беларусь от 18 марта 2019 г. [Электронный ресурс]: Постановление Совета Безопасности Республики Беларусь № 1/ - Режим доступа: https://www.sb.by/articles/kontseptsiya-informatsionnoy-bezopasnosti-respubliki-belarus.html. - Дата доступа: 08.11.2022.

34. Об утверждении Концепции национальной безопасности Республики Беларусь [Электронный ресурс]: Указ Президента Респ. Беларусь, 9 нояб. 2010 г., № 575 // КонсультантПлюс. Беларусь / ООО «ЮрСпектр», Нац. центр правовой информ. Респ. Беларусь. - Минск, 2020.

35. Доктрина информационной безопасности Российской Федерации, утверждена Указом Президента РФ от 5 декабря 2016 г. № 646 [Электронный ресурс]: - Режим доступа: http://kremlin.ru/acts/bank/41460/page/1. - Дата доступа: 08.11.2022.

36. О Стратегии национальной безопасности Российской Федерации: Указ Президента Российской Федерации от 2 июля 2021 г. №400 [Электронный ресурс]: - Режим доступа: https://www.garant.ru/products/ipo/prime/doc/401325792/. - Дата доступа: 08.11.2022.

37. Конвенция Организации Объединенных Наций против транснациональной организованной преступности: принята резолюцией Генеральной Ассамблеи 15 ноября 2000 г. [Электронный ресурс] // Организация Объединенных Наций. – Режим доступа: https://www.un.org/ru/documents/decl_conv/conventions/orgcrime.shtml. – Дата доступа: 08.11.2022.

38. Edie, E. Economics of crime / E. Edie [et oth.] // Foundations and Trends in Microeconomics. – 2006. – №3, Vol. 2. Emory Law and Economics Research Paper №11-114, Available at SSRN [Electronic resource]. – Mode of access: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1912073. – Date of access: 08.11.2022.

39. Официальный сайт Евгения Касперского [Электронный ресурс]. – Режим доступа: https://e-kaspersky.livejournal.com/. – Дата доступа: 07.11.2022.

40. Новый, В. Если будут "валить" регион, город или страну целиком – до свиданья / В. Новый [Электронный ресурс]. – Режим доступа: kommersant.ru (28 марта 2013). - Дата доступа: 08.11.2022.

41. Kramer, Andrew E. Cyberweapon Warning From Kaspersky, a Computer Security Expert (англ.), The New York Times (3 June 2012).

42. Мороз, Н.О. Международно-правовое сотрудничество в борьбе с преступностью в сфере высоких технологий: автореф. дис. ... канд. юрид. наук: 12.00.10 / Н.О. Мороз. – Минск, 2014. – 23 с.

43. Степанов, О.А. Теоретико-правовые аспекты безопасного функционирования и развития информационно-электронных систем: автореф. дис. ... доктора юрид. наук: 12.00.01 / О.А. Степанов. – М., 2005. – 53 с.

44. Bassiouni, M.Ch. A draft international criminal code and draft statute for an international criminal tribunal / By M. Cherif Bassiouni. - Dordrecht et al.: Nijhoff, 1987. P. 56-57.

45. Global Programme on Cybercrime [Electronic resource] // United Nations Organization. – Mode of access: https://www.unodc.org/unodc/en/cybercrime/global-programme-cybercrime.html. – Date of access: 08.11.2022.

46. Twelfth United Nations Congress on Crime Prevention and Criminal Justice: General Assembly resolution 65/230 [21 December 2010] [Electronic resource] // United Nations Organization. – Mode of access: https://www.unodc.org/documents/commissions/CCPCJ/Crime_Resolutions/2010-2019/2010/General_Assembly/A-RES-65-230.pdf. – Date of access: 08.11.2022.

47. The Commission on Crime Prevention and Criminal Justice [Electronic resource]: Res. 22/7 “Strengthening international cooperation to combat cybercrime”. – Mode of access: https://www.unodc.org/documents/commissions/CCPCJ/Crime_Resolutions/2010-2019/2013/CCPCJ/Resolution_22-7.pdf. – Date of access: 08.11.2022.

48. The Commission on Crime Prevention and Criminal Justice [Electronic resource]: Res. 22/8 “Promoting technical assistance and capacity-building to strengthen national measures and international cooperation against cybercrime” [Electronic resource]. – Mode of access: https://www.unodc.org/documents/commissions/CCPCJ/Crime_Resolutions/2010-2019/2013/CCPCJ/Resolution_22-8.pdf. – Date of access: 08.11.2022.

49. Резолюция Генеральной Ассамблеей от 18 декабря 2019 г. [по докладу Третьего комитета (A/74/400)]: содействие оказанию технической помощи и наращиванию

потенциала для усиления национальных мер и укрепления международного сотрудничества в целях борьбы с киберпреступностью, включая обмен информацией [A/RES/74/173] [Электронный ресурс] // Организация Объединенных Наций. – Режим доступа: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N19/429/95/PDF/N1942995.pdf?OpenElement. – Дата доступа: 07.11.2022.

50. Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes. Organizational session. New York, 10–12 May 2021. Agenda item 6. [A/AC.291/L.1] [Electronic resource] // United Nations Organization. – Mode of access: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Organizational_session/V2200692.pdf. – Date of access: 08.11.2022.

51. Russia gives the UN draft convention to fight cybercrime [Electronic resource]. – Mode of access: https/previewtech.net/russia-gives-the-un-draft-convention-to-fight-cybercrime/. – Date of access: 08.11.2022.