Анатолий М. Тарасов^{1, 2}

¹Академия управления МВД России,
ул. Зои и Александра Космодемьянских, 8, г. Москва, 125993, Россия

²АО «Лаборатория Касперского»,
Ленинградское ш, 39А, строение 2, Москва, 125212, Россия
e-mail: Tarasov.tam@yandex.ru, <https://orcid.org/0000-0003-0000-408X>

ОКИНАВСКАЯ ХАРТИЯ И КОНГРЕССЫ ООН:
ВОПРОСЫ ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПНОСТИ

DOI: <http://dx.doi.org/10.26583/bit.2019.4.09>

Аннотация. Цель статьи – на основе анализа положений Окинавской хартии «Глобального информационного общества», решений Конгрессов ООН по предупреждению преступности и уголовному правосудию, а также соответствующих резолюций Генассамблеи ООН установить состояние организационного и нормативно-правового обеспечения противодействия кибервызовам и угрозам, а также киберпреступности в глобальном информационном пространстве. Об актуальности рассмотрения данной темы свидетельствует возрастающий уровень кибервызовов и угроз, рост их масштабности. Так, спецслужбами России в ходе проведения Чемпионата мира по футболу (2018 г.) было отражено около 25 млн различного рода кибератак. **Выводы:** Рассмотренные в статье вопросы и внесенные предложения по дальнейшему развитию норм международного права, особенно касающиеся разработки технологий искусственного интеллекта, а также использования робототехники, полагаем, могут быть учтены и найти отражение в проекте Конвенции ООН по информационной безопасности.

Ключевые слова: Окинавская хартия, конгрессы, международные акты, компьютерные преступления, киберпреступность, резолюции, правоохранительные органы.

Для цитирования: ТАРАСОВ, Анатолий М. ОКИНАВСКАЯ ХАРТИЯ И КОНГРЕССЫ ООН: ВОПРОСЫ ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПНОСТИ. Безопасность информационных технологий, [S.l.], v. 26, n. 4, p. 120–131, 2019. ISSN 2074-7136. Доступно на: <<https://bit.mephi.ru/index.php/bit/article/view/1237>>. Дата доступа: 05 dec. 2019. doi:<http://dx.doi.org/10.26583/bit.2019.4.09>.

Anatoly M. Tarasov^{1, 2}

¹Management Academy of the Ministry of the Interior of Russia,
Zoi and Alexandra Kosmodemianskikh str., 8, Moscow, 125993, Russia

²Joint stock company «Kaspersky Lab»,
Leningradskoe sh, 39A, building 2, Moscow, 125212, Russia
e-mail: Tarasov.tam@yandex.ru, <https://orcid.org/0000-0003-0000-408X>

**The Okinawa Charter and the Congress of the United Nations:
cybercrime countering issues**

DOI: <http://dx.doi.org/10.26583/bit.2019.4.09>

Abstract. The paper is based on the analysis of the provisions of the Okinawa Charter "Global information society", decisions of the UN Congresses on crime prevention and criminal justice, as well as relevant resolutions of the UN General Assembly to establish the state of organizational and regulatory support for countering cyber challenges and threats, as well as cybercrime in the global information space. The relevance of this topic is evidenced by the increasing level of cyber challenges and threats, and its scale growth. Thus, the Russian security services have repelled about 25 million cyber attacks of different kinds of during the World Cup (2018). In conclusion the discussed issues the proposals we made for the further development of international law, especially concerning the development of artificial intelligence technologies, as well as the use of robotics can be taken into account and reflected in the draft of UN Convention on information security.

Keywords: Okinawa Charter, congresses, international acts, computer crimes, cybercrime, resolutions, law enforcement.

For citation: TARASOV, Anatoly M. The Okinawa Charter and the Congress of the United Nations: cybercrime countering issues. IT Security (Russia), [S.l.], v. 26, n. 4, p. 120–131, 2019. ISSN 2074-7136. Available at: <<https://bit.mephi.ru/index.php/bit/article/view/1237>>. Date accessed: 05 dec. 2019. doi:<http://dx.doi.org/10.26583/bit.2019.4.09>.

Введение

Важность и актуальность рассмотрения данной темы связана с разобщенностью государств в создании и в обеспечении безопасности применения информационно-коммуникационных технологий (ИКТ), в недооценке важности применения на практике действующих норм международного права, в частности Окинавской хартии «Глобального информационного общества» (далее по тексту – Хартия), подписанной руководителями государств Большой восьмерки 22 июля 2000 г.¹ Положения данной Хартии нацелены на объединение политических и экономических усилий и ресурсов по созданию информационного общества в глобальном пространстве, а также по организации противодействия новым кибервызовам и угрозам, включая растущую компьютерную преступность.

Борьба с компьютерной преступностью с учетом её трансграничности и глобальности в международном аспекте, наряду с проблемами борьбы с терроризмом, незаконным оборотом оружия, боеприпасов, наркотиков, является одной из требующих наибольшего и постоянного внимания всех государств, поскольку вопрос: кто (киберпреступники и киберпреступность) – кого (производители технологических средств и государственные структуры, принимающие меры по её противодействию) стоит достаточно жестко и требует со стороны субъектов, осуществляющих борьбу с киберпреступностью [1], в том числе и во внутрироссийском формате, привлечения значительных кадровых, финансовых, правовых, организационных, технических, информационных, временных, научно-методических ресурсов.

В качестве иллюстрации реально усиливающихся киберугроз, роста их масштабности приведем один пример: спецслужбами России только в ходе проведения Чемпионата мира по футболу (2018 г.) было отражено около 25 млн различного рода кибератак, а также других попыток «пробить» систему информационной безопасности страны.² По данным Лаборатории Касперского, технологический ресурс созданных ею продуктов в настоящее время в течение суток выявляет и обезвреживает порядка 340 тыс. вредоносных объектов, еще пять-шесть лет назад таких объектов обнаруживалось и нейтрализовалось, можно сказать, в два и более раза меньше.

В выступлении Генсекретаря ООН А. Гутерреша на 27 сессии Комиссии по предупреждению преступности и уголовному правосудию (Вена, 14.05.2018 г.)³ было заявлено, что киберпреступность приносит злоумышленникам около 1,5 триллиона долларов дохода в год. В актуальные задачи, стоящие сегодня перед ООН, кроме объединения межгосударственных усилий по противодействию киберугрозам, он также включил необходимость широкого применения больших данных и аналитики, искусственного интеллекта и автоматизации, благодаря применению чего человечество вступает в эпоху 4-й промышленной революции, и это должно позволить ему создавать

¹ Дипломатический вестник. 2000. № 8. С. 51–56.

² <https://iz.ru/767273/2018-07-16/putin-soobshchil-o-predotvrashchenii-25-mln-kiberatak-vo-vremia-chm-2018>.

³ <https://www.unodc.org/unodc/en/press/releases/2018/May/secretary-generals-remarks-to-the-27th-session-of-the-commission-on-crime-prevention-and-criminal-justice.html>

условия для дальнейшего роста и развития, принести пользу, в том числе по минимизации последствий, связанных с изменением климата, а также защиты окружающей среды.

В целях решения задач, указанных в Хартии по созданию глобального информационного общества, в России были приняты важные решения. В частности, только в последние годы были изданы соответствующие указы Президента РФ. Так, Указом главы государства от 9 мая 2017 г. № 203 утверждена «Стратегия развития информационного общества в Российской Федерации на 2017 - 2030 годы».⁴ В п. 1 Стратегии определены цели и задачи, а также меры по реализации внутренней и внешней политики России, связанной с использованием ИКТ, направленных на обеспечение её интересов, развитие информационного общества, реализацию стратегических приоритетов и на формирование цифровой экономики в России. В части, касающейся противодействия компьютерной преступности, Президентом РФ издан Указ от 15 января 2013 г. № 31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации». Кроме того, постановлением Правительства РФ от 15 апреля 2014 г. № 313 утверждена государственная программа РФ «Информационное общество».

1. Окинавская хартия

Как показывает анализ, Окинавская хартия является первым значимым международным актом по вопросам применения информационных коммуникационных технологий,⁵ а также по вопросам противодействия компьютерным преступлениям.

Особое значение в Хартии имеет п. 3, которым уже в 2000 г. была указана достаточно амбициозная и перспективная цель, связанная с повсеместным получением всеми людьми возможности по использованию преимуществ глобального информационного общества, хотя, подчеркнем, на момент принятия Хартии само такое общество еще только начало формироваться и то это касалось, в первую очередь, передовых в экономическом и технологическом плане государств, например, США, ряда европейских стран, Японии и Канады.

Кроме того, в п. 8 Хартии установлено, что усилия всего международного сообщества должны быть направлены не только на создание и развитие информационного общества, но и на борьбу с преступностью в компьютерной сфере и сопрягаться в этой части с согласованными действиями со стороны государств, направленными на формирование глобального безопасного киберпространства. А решение таких проблем, как несанкционированный доступ, компьютерные вирусы, как указано в Хартии, вызывает особую озабоченность и необходимость принятия согласованных политических мер на межгосударственном уровне.

В Хартии также определено, что для защиты информационных инфраструктур необходимо привлекать представителей промышленности и других посредников. Таким образом, можно сделать вывод, для решения актуальных межгосударственных проблем по созданию глобального информационного общества, эффективного противодействия преступлениям в компьютерной сфере, необходимо сопряжение ресурсов и усилий не только различных государственных органов, но и промышленного потенциала, а также других посредников, в том числе бизнеса⁶ [2].

⁴ СПС КонсультантПлюс

⁵ ИКТ - совокупность программно-технических и технологических средств, а также методов по обеспечению сбора, обработки, накопления, хранения, представления и распространения данных (информации).

⁶ Тарасов А.М. Электронное правительство и информационная безопасность. Учебное пособие. М: Галарт, 2011. – 648 с.

2. Отличие понятий компьютерная преступность и киберпреступность

В Окинавской хартии, как показывает её анализ, применяются словосочетания «преступность в компьютерной сфере» и «преступность в киберпространстве» (п. 8). В то же время в Европейской Конвенцией (принята 23 ноября 2001 г. в г. Будапеште (ETS N 185) применяется термин киберпреступность и сам этот базовый международный документ в переводе на русский язык называется «Конвенция о киберпреступности» или «Конвенция о противодействии киберпреступности».⁷

Анализируя структуру и способы совершения компьютерных и киберпреступлений важно отметить, что понятия компьютерные преступления (компьютерная преступность) и киберпреступления (киберпреступность) не тождественны, при этом понятие киберпреступность является более широким. Так, в Европейской Конвенции по киберпреступности⁸ к такому виду преступлений относятся, в том числе деяния, связанные с размещением, распространением порнографии в киберпространстве, то есть с содержанием контента, а также преступления, совершаемые с использованием ИКТ, нарушающие авторские и смежные права. При этом следует сказать, что киберпреступления в отличие от компьютерных совершаются не только с использованием таких технических устройств, как компьютеры (ЭВМ), компьютерные сети, компьютерные программы, но и с помощью мобильных (сотовых) коммуникационных технических устройств связи. Вместе с тем, справедливости ради заметим, что современные мобильные (сотовые) средства связи по техническим возможностям практически не отличаются от компьютеров.

Как обоснованно считает И.Г. Чекунов, к киберпреступлениям, как к общественно-опасным уголовно наказуемым деяниям, относятся любые преступления, совершенные с применением электронных средств и способов. При этом понятие киберпреступление не ограничивается рамками Интернета, оно распространяется на все виды преступлений, совершаемых в сфере ИКТ, на весь спектр преступлений в этой сфере, и структура киберпреступности шире структуры компьютерной преступности⁹ [3].

В то же время, говоря о понятии киберпреступность, важно учитывать употребляемые в этой связи и такие понятия, как «информационная преступность» (в сфере информации), преступность в сфере высоких технологий. Однако, поскольку некоторые различия в названных выше понятиях не имеют принципиального значения в части рассматриваемой нами темы, а также в связи с тем, что многие исследователи подобных вопросов в последнее время, все чаще применяют именно термин киберпреступность как универсальный, включающий в себя и вышеуказанные понятия, мы при рассмотрении данной темы в дальнейшем также воспользуемся именно термином киберпреступность.

3. Роль Конгрессов ООН по предупреждению преступности и уголовному правосудию

В результате широкого внедрения ИКТ в сферы жизни и деятельности человека международное сообщество столкнулось с серьезными вызовами и рисками, связанными с реально расширяющимся ростом как общих объемов киберугроз, так и их таргетированностью. Масштабность нарастающих и нерешенных в глобальном плане

⁷ URL: <http://www.pravo.ru/interpravo/legislative/view/27/> или СПС «Гарант».

⁸ Россия «не вошла» в Будапештскую Конвенцию, поскольку Конвенцией предусмотрена возможность зарубежных спецслужб без официального уведомления стороны проникать в компьютерные сети других стран, а это может угрожать безопасности и суверенитету страны.

⁹ И.Г. Чекунов. Киберпреступность: понятие и классификация». СПС КонсультантПлюс.

проблем, связанных с предупреждением и противодействием такого вида преступлений, является серьезным сигналом для различных государств, обязывающим их принять комплексные меры по объединению усилий, направленных как на реализацию уже принятых международных нормативных актов, так и на разработку и принятие новых норм, нацеленных на создание эффективных международных организационно-правовых механизмов по противодействию киберправонарушениям [4, 5].

Главенствующая координирующая роль в обеспечении взаимодействия государств, их ресурсов в этой сфере принадлежит Организации объединенных наций (ООН) и её различным институтам.

Особый статус в налаживании межгосударственного взаимодействия, включая формат Интерпола¹⁰ и национальных правоохранительных органов, осуществляющих борьбу с киберпреступностью в различных государствах, а также в области разработки международных стандартов в этой сфере, отводится Конгрессу ООН по предупреждению преступности и уголовному правосудию. Именно на заседаниях таких конгрессов, созываемых раз в пять лет, принимаются концептуальные решения, направленные на совершенствование международного и национальных законодательств, улучшение межгосударственного сотрудничества правоохранительных органов в борьбе с преступностью. Отметим, что принятые на заседаниях конгрессов рекомендации закрепляются в специальных резолюциях Генеральной Ассамблеи ООН.

Непосредственно, и можно сказать впервые, проблема компьютерных преступлений (киберпреступлений) была отмечена на VIII Конгрессе, прошедшем в Гаване в 1990 г. Развитие эта тема получила на IX Конгрессе (Каир, 1995 г.). На этом Конгрессе, в частности, было обращено внимание на рост компьютерных преступлений, причем в международном (глобальном) формате.

На X Конгрессе (Вена, 2000 г.), посвященном вопросам международного сотрудничества государств в борьбе с транснациональной организованной преступностью, в части, касающейся компьютерных преступлений, речь уже шла о том, что данный вид преступлений стал серьезной проблемой для многих развитых стран. При этом следует подчеркнуть, что п. 18 Венской Декларации была предусмотрена необходимость разработки и принятия программных рекомендаций (документов), направленных на предупреждение киберпреступлений и усиление борьбы с ними.

На состоявшемся в 2005 г. XI (Бангкокском) Конгрессе рассматривались вопросы, связанные с борьбой с терроризмом и организованной транснациональной преступностью, а также вопросы принятия мер, направленных на борьбу с организованной экономической преступностью и компьютерной преступностью (киберпреступностью). В отношении оценки качественной характеристики состояния компьютерной преступности было обращено внимание на возрастающее её распространение и охват ею уже большинства стран Мира, т.е. был сделан вывод о том, что компьютерная преступность становится все

¹⁰ Международная (межправительственная) организация уголовной полиции. В структуру Интерпола в настоящее время входят 194 государства. Главная задача Интерпола – осуществление межгосударственной координации в проведение общей политики в сфере борьбы с общеуголовной, в том числе киберпреступностью. Высшим коллегиальным органом является Генассамблея, заседания которой проводятся ежегодно под председательством избранного президента Интерпола. В целях координации борьбы с киберпреступностью Интерполом создано подразделение уголовной полиции, состоящее из 200 сотрудников для работы в сингапурском центре (Киберполиция).

Центральные органы Интерпола находятся в г. Лионе (Франция). Во всех входящих в Интерпол странах образованы государственные центральные бюро, в задачи которых входит взаимодействие с правоохранительными органами других стран, входящих в Интерпол, и с Ген. секретариатом Интерпола. В России создано Центральное национальное бюро Интерпола при МВД России.

более трансграничной, глобальной, и усилия по её противодействию должны быть более активными и соответствовать тенденциям её развития и распространения в международном масштабе.

Большое и предметное внимание проблемам борьбы с киберпреступностью было уделено на XII Конгрессе ООН (г.Сальвадор, Бразилия), прошедшем в апреле 2010 г.¹¹ с повесткой дня: «Комплексные стратегии для ответа на глобальные вызовы: системы предупреждения преступности и уголовного правосудия и их развитие в изменяющемся мире». Среди рассматриваемых вопросов Конгресса, в частности, стояли следующие: обеспечение действенности руководящих принципов ООН в области предупреждения преступности; последние тенденции в использовании научно-технических достижений правонарушителями и компетентными органами, ведущими борьбу с преступностью, в том числе совершаемых с использованием высоких технологий; практические подходы к укреплению международного сотрудничества в решении проблем, связанных с борьбой с преступностью. Таким образом, на данном Конгрессе вопрос борьбы с преступлениями, совершаемыми с использованием высоких технологий (киберпреступлениями), был впервые особо выделен в повестке дня и рассмотрен отдельно.

По результатам работы XII Конгресса была принята Сальвадорская декларация «О комплексных стратегиях для ответа на глобальные вызовы: системы предупреждения преступности и уголовного правосудия и их развитие в изменяющемся мире».¹² В п. 41 данной Декларации Управлению ООН по наркотикам и преступности, в сотрудничестве с государствами-членами, а также соответствующими международными организациями и частным сектором, рекомендовано оказывать государствам (по их просьбе) помощь в подготовке кадров и техническую помощь, а также помогать в деле совершенствования национального законодательства и усиления ресурса национальных правоохранительных органов в целях противодействия киберпреступности, в том числе в направлении предупреждения, выявления и расследования таких преступлений. Причем оказывать такую помощь в целях укрепления безопасности компьютерных сетей, как была поставлена задача в данном пункте Декларации, необходимо во всех формах, включая установление лиц, которые преследуются за их совершение.

Важное значение имеет п. 42 Декларации, в котором Комиссии по предупреждению преступности и уголовному правосудию ООН предложено провести всестороннее исследование проблемы киберпреступности, а также принимаемых со стороны государств-членов ООН, международного сообщества и частного сектора ответных мер. В целях обеспечения эффективности такого исследования был предусмотрен обмен информацией о национальном законодательстве, о имеющейся передовой практике, об оказании технической помощи при проведении исследования в рамках международного сотрудничества. Поскольку принятие решения по проведению исследования носило

¹¹ Конгрессы, являясь важнейшим форумом ООН, призваны служить укреплению международного сотрудничества в борьбе с преступностью, решению проблем, связанных с обеспечением прав правонарушителей, а также с уголовным правосудием во всем мире. Созывается Конгресс один раз в пять лет. Первый Конгресс прошел в 1955 году в Женеве (Швейцария); II-й - в 1960 г. в Лондоне (Великобритания); III-й - в 1965 г. в Стокгольме (Швеция); IV-й - в 1970 г. в Киото (Япония); V-й - в 1975 г. в Женеве (Швейцария); VI-й - в 1980 г. в Каракасе (Венесуэла); VII-й - в 1985 г. в Милане (Италия); VIII-й - в 1990 г. в Гаване (Куба); IX-й - в 1995 г. в Каире (Египет); X-й - в 2000 г. в Вене (Австрия); XI-й - в 2005 г. в Бангкоке (Таиланд); XII-й - в Сальвадоре (Бразилия); XIII-й - в 2015 г. в Дохе (Катар).

¹² Принята резолюцией 65/230 Генеральной Ассамблеи ООН от 21 декабря 2010 года.
http://www.un.org/ru/documents/decl_conv/declarations/salvador_declaration.shtml
http://www.un.org/ru/documents/decl_conv/conventions/tokyo_rules.shtml

прикладной характер, то по его результатам было предусмотрено внесение предложений по применению (укреплению) не только уже действующих нормативных правовых документов, но и по предстоящим принятию новым национальным и международным правовым актам, а также по принятию других мер, касающихся противодействия киберпреступности.

При этом следует также обратить внимание на один процедурный момент, касающийся обсуждения проекта и принятия самой Сальвадорской Декларации. Так, при её принятии на практике был реализован принцип учета мнения различных сторон, то есть принцип всеобъемлющего и сбалансированного подхода.

Кстати, на XII Конгрессе делегации России и Китая предложили внести в проект Декларации пункт по разработке международной универсальной конвенции по киберпреступности. Однако многие европейские и страны других континентов выступили против этого предложения и сфокусировали внимание не на разработке в рамках ООН нового, имеющего универсальный характер международного правового акта, а на расширении формата участников названной выше Будапештской конвенции о киберпреступности (Россия, как отмечалось, не является стороной данной Конвенции).

В результате согласования двух принципиально различающихся позиций в п. 42 Декларации была включена компромиссная рекомендация об учреждении Комиссией ООН по предупреждению преступности и уголовному правосудию Межправительственной рабочей группы экспертов по проблематике киберпреступности с правом разработки предложений, касающихся вопросов противодействия киберпреступности в международном формате. В целом, можно сказать, что в Сальвадорской декларации впервые были определены основные (стратегические) направления международного сотрудничества в сфере предупреждения киберпреступности.

Очередной (XXIII) Конгресс по предупреждению преступности и уголовному правосудию ООН прошел 12–19 апреля 2015 г. в г. Доха (Катар).¹³ В ходе него были рассмотрены, в частности, следующие вопросы, в том числе касающиеся новых вызовов и угроз, борьбы с киберпреступностью:

- успехи и вызовы в реализации комплексной политики и стратегий в области предупреждения преступности и уголовного правосудия в целях содействия обеспечению верховенства права на национальном и международном уровнях и поддержки устойчивого развития;
- международное сотрудничество, в том числе на региональном уровне, в целях борьбы с транснациональной организованной преступностью;
- всеобъемлющие и сбалансированные подходы в целях предупреждения новых и появляющихся форм транснациональной преступности и надлежащего реагирования на них;
- национальные подходы к участию общественности в укреплении систем предупреждения преступности и уголовного правосудия.

На одном из семинаров, прошедших в рамках Конгресса, обсуждался вопрос укрепления мер реагирования систем предупреждения преступности и уголовного правосудия на развивающиеся формы преступности, включая киберпреступность. Вопросы, связанные с предупреждением новых, появляющихся и видоизменяющихся форм преступности, в том числе в сфере киберпространства, нашли отражение в подпунктах «а» и «b» пункта 9 Декларации, одобренной Конгрессом [6].

¹³ <https://www.un.org/ru/events/crimecongress2015/about.shtml>

Так, в подп. «а» Декларации заявляется о стремлении разрабатывать и осуществлять всеобъемлющие меры реагирования в области предупреждения преступности и уголовного правосудия, в том числе направленные на укрепление потенциала судебных и правоохранительных органов, и принимать, при необходимости, законодательные и административные меры для эффективного предупреждения новых, появляющихся и видоизменяющихся форм преступности и борьбы с ними на национальном, региональном и международном уровнях.

В подп. «b» декларируется необходимость апробирования конкретных мер, направленных на создание защищенной и устойчивой киберсреды, предупреждение и пресечение преступной деятельности, осуществляемой с помощью Интернета.

При этом особое внимание в Декларации в части, касающейся международного противодействия киберпреступности, было предложено уделять:

- краже личных данных, вербовке с целью торговли людьми и защите детей от эксплуатации и надругательства через Интернет;

- укреплению сотрудничества между правоохранительными органами на национальном и международном уровнях, в том числе с целью выявления и защиты жертв, в частности, посредством удаления из Интернета детской порнографии, изображений сексуального надругательства над детьми;

- повышению защищенности компьютерных сетей и обеспечению защиты соответствующей инфраструктуры;

- оказанию долгосрочной технической помощи и содействия наращиванию потенциала для укрепления способности национальных ведомств противодействовать киберпреступности, в том числе посредством профилактики, выявления, расследования и уголовного преследования таких преступлений (преступников) во всех их формах.

Отметим также, что в подпункте «b» п. 8 Декларации XIII Конгресса указывается на необходимость продолжения поддержки программ, направленных на предупреждение и противодействие использованию Интернета в террористических целях, а также на создание в этих целях потенциала и важности подготовки должностных лиц системы уголовного правосудия.

Анализируя содержание рассмотренных выше деклараций конгрессов ООН, следует обратить внимание на то, что положения принятых деклараций не являются обязательными для исполнения сторонами, а носят только рекомендательный характер. Вместе с тем сам факт проведения таких конгрессов и одобренных ими деклараций являются важными политическими решениями, оказывающими влияние на формирование, развитие и стимулирование политики в области предупреждения преступности и уголовного правосудия в мировом значении, а также на формирование политики и создание профессиональной практики на национальных уровнях.

Кроме того, важным аспектом в части оценки значения таких международных форумов, как конгрессы ООН, является предоставление в ходе проведения форума реальной возможности по обмену информацией между различными государствами и специалистами-экспертами в области борьбы с киберпреступностью, по укреплению международной кибербезопасности в целом.

Проведение четырнадцатого Конгресса по предотвращению преступности и уголовному правосудию запланировано на 2020 год в Японии. На заседании Конгресса будут обсуждаться вопросы, связанные с усовершенствованием мер по предупреждению преступности и основ правосудия [7].

В заключение отметим, что одобренные Конгрессом декларации представляются сессии Комиссии ООН по предупреждению преступности и уголовному правосудию.

4. Россия и международное сотрудничество в области противодействия кибервызовам и угрозам

Являясь, начиная со II Конгресса ООН постоянным их участником, Российская Федерация целенаправленно привлекает внимание всех государств-участников конгрессов на решение стратегически-значимых задач в области предупреждения кибервызовов, эффективного противодействия киберпреступности в глобальном масштабе.

После принятия Окинавской хартии МИД России активно и неоднократно призывало государства не применять ИКТ в качестве способа оказания политического давления, угрозы нанесения экономического ущерба, то есть вмешательства во внутренние дела других государств. Предлагала нацеливать ресурс ООН на разработку и принятие специальных правил по ответственному поведению государств в Интернете, в том числе по предотвращению конфликтов при использовании новых технологий, включая цифровую сферу.

Для достижения таких целей в практической плоскости Россией в 2017 г., например, был внесен в ООН проект резолюции по обеспечению информационной безопасности и предложено провести международную дискуссию по данному вопросу.¹⁴ Проект резолюции «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» 5 декабря 2018 г. был обсужден на заседании Генеральной Ассамблеи ООН и была принята резолюция по образованию в рамках ООН специальной рабочей группы по разработке правил информационной безопасности. Кстати, за принятие данной резолюции проголосовало 119 государств, 46 стран её не поддержали и 14 стран воздержались. Против принятия этой резолюции, выступили, в частности, США, Великобритания, Грузия, Украина.

При этом отметим, что в первом комитете Генассамблеи ООН одновременно также был поддержан проект резолюции по данному вопросу, внесенный США. Сущностное различие этих проектов заключается в том, что Российская Федерация предложила разработать и дополнительно к уже действующим принять новые правовые нормы, регламентирующие правила поведения всех государств, в том числе по воздержанию от любых вредоносных действий в глобальном киберпространстве, а также обязательство по соблюдению Устава ООН. По мнению же США, международные отношения, касающиеся использования киберпространства, в правовом плане уже достаточно урегулированы и необходимость принятия других нормативных документов, включая некие правила поведения, нецелесообразна.

В этой связи считаем, что в части, касающейся масштабного роста и видоизменения новых кибервызовов и угроз, сегодня человечество во многом подошло к черте, переступать за которую крайне опасно. Вопрос кто кого стоит реально, в том числе на межгосударственном уровне. Поэтому все возможные меры по минимизации международных киберпроблем, обеспечению глобальной информационной безопасности, включая совершенствование правового поля, должны быть государствами предприняты своевременно и в должном объеме. Такая востребованность связана также и с необходимостью правового регулирования вопросов по применению искусственного интеллекта (ИИ) [8] при использовании ИКТ, а также ответственности за его применение в негативных государственных целях.

Кроме того, и в этой связи отметим, что Россией в сентябре 2017 г. было внесено предложение США по формированию двусторонней российско-американской группы по вопросам кибербезопасности.¹⁵ Однако США до настоящего времени не принято решение

¹⁴ <https://iz.ru/648864/2017-09-21/lavrov-predlozhil-obsudit-na-ga-oon-vzaimodeistvie-v-kiberprostranstve>

¹⁵ <https://iz.ru/645476/2017-09-14/rf-prizyvaet-ssha-izuchit-initiativu-o-gruppe-po-kiberbezopasnosti>

о поддержке данного предложения Российской Федерации, очередной раз в позициях России и США проявилась турбулентность.

В развитие актуальности данной темы важно также сказать и о том, что в выступлении 28 сентября 2019 г. Министра иностранных дел России на 74-й сессии Генассамблеи ООН в очередной раз было подчеркнуто, что выработка общеприемлемых подходов (правил) по регулированию цифровой сферы, осмысление процессов, связанных с созданием искусственного интеллекта являются важнейшими задачами, стоящими перед Миром, что для обеспечения международной информационной безопасности важно принять юридически значимые и обязывающие межгосударственные договоренности,¹⁶ то есть на сегодняшний день реально необходима дальнейшая гармонизация международного законодательства, его актуализация, с учетом транспарентности межгосударственного подхода, а также характера и возрастающих объемов современных кибервызовов и угроз, в основе создания которых все больше участвуют технологии ИИ.

Сегодня уже однозначно можно утверждать, что ресурс ИИ систематически наращивается, причем как его создателями и заказчиками со стороны государств и бизнеса для решения важнейших национальных социально-экономических проблем, а также обеспечения безопасности государства, общества, личности, так и со стороны враждебных сторон, криминального мира.

5. Искусственный интеллект и киберугрозы

Рассматривая данный вопрос, целесообразно отметить, что его актуальность и важность в межгосударственных отношениях проявились, в частности, в принятии Европейской этической хартии об использовании искусственного интеллекта в судебных системах (принята Европейской комиссией по эффективности правосудия (CEPEJ) Совета Европы 04.12.2018).¹⁷ Принятию Хартии послужила необходимость объективной и качественной обработки судебных решений сертифицированными цифровыми моделями, разработанными на междисциплинарной основе в безопасной технологической среде и на основе нематериальных данных. Для этого были задействованы интеллектуальные системы, выполняющие творческие функции, ранее считающиеся прерогативой человека. Расширяющаяся востребованность развития и применения ИИ особенно в сфере роботизации связана и с тем, что ИИ решает вопросы без эмоций, эффективно.

Задачи развития и широкого применения ИИ является для России также достаточно значимыми, о чем, например, свидетельствует утверждение Указом Президента РФ от 10 октября 2019 года № 490 «Национальной стратегии развития искусственного интеллекта на период до 2030 года». Согласно п. 1 Указа целями его издания являются: ускорение развития ИИ в России, повышение для пользователей доступности вычислительных ресурсов и информации, совершенствование системы подготовки кадров, проведение в этой области научных исследований.

Таким образом, изданием данного Указа государство показало свою заинтересованность не упустить ситуацию по применению ИИ в решении политических и социально-экономических вопросов в стране, а также своевременного обеспечения безопасности институтов государственной власти, общества, личности и бизнеса. Государство также продемонстрировало, что не хочет быть отстающим или догоняющим в

¹⁶ <https://www.discred.ru/2019/09/28/vystuplenie-sergeya-lavrova-na-74-j-sessii-ga-onn-polnyj-tekst-video/>

¹⁷ Council of Europe adopts first European Ethical Charter on the use of artificial intelligence in judicial systems. <https://www.coe.int/en/web/artificial-intelligence/-/council-of-europe-adopts-first-european-ethical-charter-on-the-use-of-artificial-intelligence-in-judicial-systems>

сфере разработок и применения ИИ, что оно не заинтересовано допустить использование ИИ в разрушительных целях, в том числе как средства (ресурса) для киберугроз и проведения кибератак на критически-важные объекты промышленной инфраструктуры, особенно на межгосударственном уровне, а также как средства усиления криминального ресурса для злоумышленников в глобальном киберпространстве.

Кстати, угрозы использования технологий ИИ и его продуктов (робототехники), например, в военных целях постоянно возрастают. Достаточно вспомнить недавние бомбардировки неустановленными дронами-самолетами (роботами) нефтяных объектов в Саудовской Аравии или атаки неопознанными морскими объектами, оснащенными технологиями ИИ, на нефтеналивное судно Ирана. При этом можно сделать обоснованный вывод: чем больше у государства или у криминала интеллектуальных и экономических ресурсов, тем проще разрабатывать и совершенствовать технологии создания продуктов ИИ и наоборот. В этой связи определяющее значение имеет цель разработки технологий и продуктов ИИ, а она, к сожалению, не всегда может быть гуманной.

Итак, как показывает анализ ряда международных актов, в которых нашли отражение вопросы кибербезопасности, на сегодняшний день конкретных норм, регламентирующих разработку и применение ИИ и его продуктов только в мирных целях, а также предусматривающих ограничение их применения, не установлено.

Заключение

В случае отсутствия механизмов противодействия нарастающим киберугрозам, противоборство с применением автоматизации, роботизации, использованием возможностей ИИ в киберпространстве, особенно на межгосударственном уровне, будет нарастать и создавать все большую напряженность в отношениях между многими государствами, усиливая опасность сохранения цивилизации на Земле.

Одним из путей минимизации негативных последствий от разработки и использования ИИ и его продуктов в межгосударственных отношениях (в международном формате) является выработка дополнительных общеприемлемых правил, регулирующих цифровую сферу и связанных с созданием, развитием и применением технологий ИИ и его продуктов (робототехники). Таким образом, для противодействия новым вызовам и угрозам в рамках ООН на основе транспарентного подхода необходимо принять юридически обязывающий межгосударственный акт, направленный на актуализацию международного законодательства, с учетом возрастающих угроз от технологий создания ИИ и его продуктов. Основой для принятия такого международного нормативного акта, считаем, является внесенный Россией в ООН проект конвенции по вопросам информационной безопасности. При рассмотрении и принятии данного акта важно, чтобы государства-участники руководствовались такими международными принципами, как: невмешательство в информационное пространство друг друга (не использование ИТ-технологий для решения вопросов, относящихся к внутренней компетенции другого государства), а также неделимости безопасности киберпространства (его безопасность – общая цель и задача).

СПИСОК ЛИТЕРАТУРЫ:

1. Минин А.Я. О специфике противодействия киберпреступности // Российский следователь. 2013. № 8. С. 37–39.
2. Тарасов А.М. Электронное правительство и информационная безопасность. Учебное пособие. М: Галарт, 2011. – 648 с.
3. Чекунов И.Г. Киберпреступность: понятие, классификация, современные вызовы и угрозы // Молодые ученые. Издательство: Московский институт государственного управления и права (Москва). 2012. № 3. С. 178–186. URL: <https://elibrary.ru/item.asp?id=21944441> (дата обращения: 10.10.2018).
4. Минаев В.А., Дворянкин С.В. и др. Кибербезопасность и глобальные геодинамические риски // Вопросы кибербезопасности, № 3 (31), 2019. С. 11–17. DOI: 10.21681/2311-3456-2019-3-11-17. URL: <https://elibrary.ru/item.asp?id=38654901> (дата обращения: 28.11.2019).
5. Карцхия А.А., Макаренко Г.И., Сергин М.Ю. Современные тренды киберугроз и трансформация понятия кибербезопасности в условиях цифровизации системы права // Вопросы кибербезопасности, № 3 (31), 2019. С. 18–23. DOI: 10.21681/2311-3456-2019-3-18-23. URL: https://cyberrus.com/wp-content/uploads/2019/07/18-23-331-19_4.-Karzhia-1.pdf (дата обращения: 28.11.2019).
6. Проект Дохийской декларации 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. A/CONF.222/L.6. Distr.: Limited 31 March 2015 Russian Original: English. Доха, 12–19 апреля 2015 года. URL: <https://undocs.org/ru/A/CONF.222/L.6> (дата обращения: 28.11.2019).
7. Четырнадцатый Конгресс Организации Объединенных Наций по предупреждению преступности и уголовному правосудию. Киото, Япония, 20–27 апреля 2020 года. URL: <http://www.unodc.org/congress/ru/about.html> (дата обращения: 28.11.2019).
8. Васильев А.А., Шпопер Д. Искусственный интеллект: правовые аспекты // Известия Алтайского государственного университета. Юридические науки. 2018. №6 (104). С. 23–26. DOI: 10.14258/izvasu(2018)6-03. URL: <https://cyberleninka.ru/article/n/iskusstvennyy-intellekt-pravovye-aspekty/viewer> (дата обращения: 28.11.2019).

REFERENCES:

- [1] Minin A.Ya. On the specifics of combating cybercrime. Rossijskij sledovatel'. 2013. № 8. P. 37–39 (in Russian).
- [2] Tarasov, A.M. E - government and information security. Textbook. M: Galart, 2011. – 648 p. (in Russian).
- [3] Chekunov, I.G. Cybercrime: concept, classification, modern challenges and threats. Molodye uchenye. Publisher: Moscow Institute of public administration and law (Moscow). 2012. № 3. С. 178–86. URL: <https://elibrary.ru/item.asp?id=21944441> (accessed: 10.10.2018) (in Russian).
- [4] Minaev V.A., Dvoryankin S.V. and and others. Cybersecurity and Global Geodynamic Risks. Voprosy kiberbezopasnosti. Tom 3 (31), 2019. P. 11–17. DOI: 10.21681/2311-3456-2019-3-11-17. URL: https://cyberrus.com/wp-content/uploads/2019/07/11-17-331-19_3.-Minaev-1.pdf (accessed: 28.11.2019) (in Russian).
- [5] Karzhia A.A., Makarenko G.I., Sergin M.Yu. Modern trends of cyber-threats and transformation of the concept of cybersecurity in the conditions of digitalization of the system of law. Voprosy kiberbezopasnosti. Tom 3 (31), 2019. P. 18–23. DOI: 10.21681/2311-3456-2019-3-18-23. URL: https://cyberrus.com/wp-content/uploads/2019/07/18-23-331-19_4.-Karzhia-1.pdf (accessed: 28.11.2019) (in Russian).
- [6] Draft Doha Declaration on integrating crime prevention and criminal justice into the wider United Nations agenda to address social and economic challenges and to promote the rule of law at the national and international levels, and public participation. A/CONF.222/L.6. Distr.: Limited 31 March 2015 Original: English. Doha, 12–19 April 2015. URL: <https://undocs.org/en/A/CONF.222/L.6> (accessed: 28.11.2019).
- [7] 14th United Nations Congress on crime prevention and criminal justice. Kyoto, Japan, April 20–27, 2020. URL: <http://www.unodc.org/congress/en/about.html> (accessed: 28.11.2019).
- [8] Vasilev A.A., Szpopper D. Artificial Intelligence: Legal Aspects. Proceedings of the Altai state University. Legal science. 2018. Tom 6 (104). P. 23–26. DOI: 10.14258/izvasu(2018)6-03. URL: <https://cyberleninka.ru/article/n/iskusstvennyy-intellekt-pravovye-aspekty/viewer> (accessed: 28.11.2019) (in Russian).

Поступила в редакцию – 05 ноября 2019 г. Окончательный вариант – 05 декабря 2019 г.

Received – November 05, 2019. The final version – December 05, 2019.