Журнал международного права и международных отношений. 2023. № 3 (106). С. 3—15.
Journal of International Law and International Relations. 2023. N 3 (106). P. 3—15.

УДК 351+341.1

# ПЕРСПЕКТИВНЫЕ НАПРАВЛЕНИЯ МЕЖДУНАРОДНО-ПРАВОВОГО УРЕГУЛИРОВАНИЯ ПРОБЛЕМ ПРОТИВОДЕЙСТВИЯ ТРАНСНАЦИОНАЛЬНОЙ ОРГАНИЗОВАННОЙ ПРЕСТУПНОСТИ В СФЕРЕ ВЫСОКИХ ТЕХНОЛОГИЙ И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

**Владимир Меркушин**

*Статья посвящена актуальным вопросам международно-правового противодействия транснациональной организованной преступности в сфере высоких технологий и информационной безопасности (киберпреступности). Сформулированы перспективные направления исследования данной проблематики, проанализированы ее место и роль в системе конструирования коллективной и региональной безопасности, предложены и обоснованы новые юридические инструментарии обеспечения национальных интересов Республики Беларусь в указанной области. Разработан и предложен на обсуждение проект Протокола о предотвращении и пресечении преступлений в сфере высоких технологий, особенно киберпреступлений, и наказаниях за них, дополняющего Конвенцию ООН против транснациональной организованной преступности 2000 г.*

*Ключевые слова: информационная безопасность; киберпреступность; международная безопасность; национальная безопасность; национальные интересы; правотворческие инициативы; сфера высоких технологий; транснациональная организованная преступность.*

***«Promising Directions of International Legal Regulation of the Problems of Countering Transnational Organised Crime in the Field of High Technology and Information Security» (Vladimir Merkushin)***

*The article is devoted to the topical issues of international legal counteraction to transnational organised crime in the field of high technologies and information security (cybercrime). Perspective directions of research of this problematic are formulated, its place and role in the system of constructing collective and regional security are analysed, new legal tools for ensuring national interests of the Republic of Belarus in this field are proposed and substantiated. The draft Protocol on Prevention, Suppression and Punishment of Crimes in the Sphere of High Technologies, Especially Cybercrimes, Supplementing the UN Convention against Transnational Organised Crime of 2000 has been developed and proposed for discussion.*

*Keywords: cybercrime; high technology; information security; international security; law-making initiatives; national interests; national security; transnational organised crime.*

Проблема противодействия транснациональной организованной преступности в сфере высоких технологий и информационной безопасности является одним из новейших и перспективных направлений формирования стратегии коллективной и региональной безопасности государств, непосредственно затрагивающей национальные интересы государств, в том числе и Республики Беларусь (пп. 9, 12, 14 Концепции национальной безопасности Республики Беларусь 2010 г. [19], п. 79 Концепции информационной безопасности Республики Беларусь 2019 г. [22]).

Актуальность угроз данной проблемы постоянно анализируется экспертами ООН, по оценкам которых, если в 2018 г. ущерб от киберпреступности составлял 1,5 трлн дол. США, то к 2025 г. это показатель может увеличиться уже до 9 трлн [4].

Важнейшую роль при этом играют, с одной стороны, революционные изменения технологий управления общественными институтами (использование систем искусственного интеллекта, развитие квантовых технологий, внедрение 5—6*G* технологий, достижения синтетической биологии и пр. [9]), которые могут быть как способом совершения преступлений,

*Автор:*
**Меркушин Владимир Владимирович** — кандидат юридических наук, докторант кафедры международного права факультета международных отношений Белорусского государственного университета, *e-mail: valdshin@mail.ru*
*Белорусский государственный университет. Адрес: 4, пр. Независимости, Минск, 220030, БЕЛАРУСЬ*

*Author:*
**Merkushin Vladimir** — Candidate of Law, Doctorant of the Department of International Law of the Faculty of International Relations, Belarusian State University, *e-mail: valdshin@mail.ru*
*Belarusian State University. Address: 4, Nezavisimosti ave., Minsk, 220030, BELARUS*

так и их объектом. С другой стороны, данные процессы создают предпосылки столкновения национальных интересов государств, способствующих возникновению конкурирующей и, особенно, «недружественной» юрисдикции [11; 20]. Это, по нашему мнению, с высокой степенью вероятности может вызвать объективные трудности обеспечения интересов Республики Беларусь, поскольку «наша страна находится на пути движения транснациональных угроз как с западной стороны, так и при их перемещении в сторону Западной Европы» [8, л. 206]. Нарастающие вызовы и угрозы правам и интересам субъектов информационного взаимодействия существенно влияют на безопасность государств и их союзов [16, с. 3] и требуют принятия более жестких мер против «преступности без границ» [48, с. 24].

Традиционное отнесение указанных и иных релевантно связанных вопросов к компетенции ряда соответствующих международных, особенно региональных, организаций, участником которых является Республика Беларусь, представляется пока небезусловным с точки зрения международной правотворческой практики, однако востребованным и в то же время весьма дискуссионным в доктринальных источниках. Особенно, когда в фокусе внимания постоянно находится вопрос научного осмысления проблем реализации новых документов стратегического планирования, развития системы принципов обеспечения международной информационной безопасности в условиях цифровой трансформации [30, с. 47].

Подробное исследование отдельных, но системообразующих международно-правовых аспектов данной проблематики осуществлялось в указанных и иных работах отечественных и иностранных авторов, таких как А. Л. Баньковский, П. И. Савков [2], Д. М. Валеев [3], Е. Ф. Довгань [7; 8], О. С. Макаров [16], О. В. Мозолина [17], Н. О. Мороз [18], В. С. Овчинский, Ю. Н. Жданов [21], Т. А. Полякова [30], Т. Б. Сеитов [33], а также Э. Верхелст и Я. Ваутерс [5], Жу Цичао [9], Ф. Кальдерони [37], К. Андреассон [45], А. Крамер [47], Т. Крюссманн [48], Р. МакКаскер [49], С. Шольберг и С. Гернаути-Хели [52] и др.

Обращаясь к Конвенции ООН против транснациональной организованной преступности 2000 г. как основополагающему и инклюзивно ориентированному документу, особенно в рамках рассматриваемой тематики, отметим, что согласно пункту 1 статьи 34 указанной Конвенции «каждое Государство-участник принимает в соответствии с основополагающими принципами своего внутреннего законодательства необходимые меры, включая законодательные и административные меры, для обеспечения осуществления своих обязательств согласно настоящей Конвенции» [13].

При этом, руководствуясь инструментарием оценки потребностей, документально зафиксированным Управлением Организации Объединенных Наций по наркотикам и преступности по осуществлению Конвенции ООН против транснациональной организованной преступности, обратим внимание на цель данной инициативы — дать методические указания по оценке того, какие меры необходимо принять государствам-участникам для обеспечения *полной реализации потенциала* (курсив наш. — *В. М.*) данной Конвенции. В частности, при оценке потребностей государств-участников в оказании технической помощи акцентируется особое внимание на разработке законодательства, нацеленного на осуществление положений Конвенции [28, с. 7].

В этой связи в другом документе — резолюции Генеральной Ассамблеи ООН 74/173 от 18 декабря 2019 г. 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», а также то, 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» [35].

В целом надо отметить, что деятельность органов и учреждений системы ООН была стратегически определяющей, во-первых, в подготовке и принятии собственно Конвенции ООН против транснациональной организованной преступности 2000 г. и трех дополнительных протоколов к ней, подписанных и ратифицированных Республикой Беларусь [24; 26; 27]; во-вторых, в формировании единой правовой платформы, касающейся работы над проектом новой Международной (Всеобъемлющей) конвенции ООН о противодействии использованию информационно-коммуникационных технологий в преступных целях [38], и в-третьих, последовательном интегрировании результатов региональных систем безопасности во всеобщую архитектуру коллективной безопасности.

В последнем случае важно подчеркнуть, что на сегодняшний день вопросы противодействия транснациональной преступности в сфере высоких технологий и информационной безопасности наиболее систематизированы и практически отрегулированы в рамках международных региональных организаций (например, Содружества Независимых Государств

[34; 36] (далее — СНГ), Организации Договора о коллективной безопасности [25] (далее — ОДКБ), Совета Европы [12], Шанхайской организации сотрудничества [29] (далее — ШОС) и др.). Однако вопрос о правовых мерах по борьбе с транснациональной организованной преступностью, по мнению австрийского ученого Т. Крюссманна, вряд ли был подготовлен с использованием сравнительного регионального опыта [48, p. 24]. Данная ситуация, на наш взгляд, несколько принижает потенциал универсального механизма сотрудничества в этой области (в первую очередь, ООН и Интерпола [56]). При том, что в ряде соответствующих резолюций Генеральной Ассамблеи ООН (например, 75/10 [39], 71/19 [40], 77/20 [41], 73/11 [42]) отмечается необходимость укрепления международного сотрудничества на глобальном, региональном и субрегиональном уровнях в различных областях, связанных с предупреждением и борьбой с транснациональной преступностью, в частности с транснациональной организованной преступностью, предупреждением и противодействием терроризму. А практическая роль того же Интерпола закреплена еще более чем в 50 резолюциях Совета Безопасности ООН [55]. И это не случайно. Поскольку на данный момент опубликованные данные о работе Интерпола [54] свидетельствуют о достаточно эффективной координации сотрудничества государств-членов в противодействии как организованной преступности [51], так и релевантно связанным с ней киберпреступлениям [44; 46].

Вышесказанное позволяет предположить, что основным маркером эффективной деятельности универсальных международных организаций, особенно ООН, является дальнейшая разработка базовых стандартов и общего юридического инструментария по реализации противодействия транснациональной организованной преступности и связанным с ней преступлениям в сфере высоких технологий и киберпреступлениям.

Здесь, с одной стороны, подписание и ратификация Конвенции против транснациональной организованной преступности 2000 г. большинством стран достаточно решает проблематику транснациональной организованной преступности на универсальном уровне, а с другой — объективно демонстрирует правовую лакуну в части, касающейся киберпреступности, которая относительно полно заполнена на региональном (субрегиональном) уровне, но «требует выработки адекватного правового обеспечения безопасности субъектов в процессе совместных действий» [18, с. 3], в том числе и при применении санкций к государствам и негосударственным акторам, принятии мер по борьбе с современными вызовами и угрозами [7, с. 9].

В связи с фактическим отсутствием каких-либо универсальных международных документов в рассматриваемой области заметен определенный диссонанс на региональном и межрегиональном уровне. По нашему мнению, это особенно прослеживается по линии стран НАТО и аффилированных с ней иных организаций, в первую очередь Организации по безопасности и сотрудничеству в Европе, Европейского союза, Совета Европы и др., в условиях снижающихся темпов их партнерства с некоторыми государствами — участниками СНГ (например, Россией и Республикой Беларусь) и практически отсутствия такового со странами ОДКБ, ШОС, Евразийского экономического союза и др.

Разрешение данной ситуации на универсальном уровне видится в ходе предпринимаемой работы над проектом Всеобъемлющей конвенции ООН о противодействии использованию информационно-коммуникационных технологий в преступных целях. Однако для ряда стран здесь возникают определенные сложности.

Так, в условиях перманентной конфронтации Российской Федерации и Республики Беларусь со странами НАТО (особенно в информационной сфере) и, как следствие, со странами Европейского региона (в частности, Европейского союза, Совета Европы) вопросы совместного противодействия киберпреступлениям и преступлениям в сфере высоких технологий остаются актуальными, но перестают быть среди приоритетных. Тем не менее даже такая ситуация нисколько не снижает интереса Республики Беларусь к данной проблематике. Особенно следует подчеркнуть ее деятельное участие наряду с Россией [32; 53] в разработке указанного проекта Всеобъемлющей конвенции ООН о противодействии использованию информационно-коммуникационных технологий в преступных целях. Причем, несмотря на то, что ряд соответствующих региональных документов, разработанных в рамках Совета Европы и открытых для присоединения (за исключением Конвенции о противодействии торговле людьми от 16 мая 2005 г. [43], вступила в силу 1 февраля 2008 г. и ратифицирована Республикой Беларусь [23]), по различным причинам находится вне возможностей присоединения к ним Республики Беларусь (например, Конвенция о преступности в сфере компьютерной информации *ETS* № 185 от 23 ноября 2001 г. [12] 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., Конвенция об отмывании, выявлении, изъятии конфискации доходов от преступной деятельности от 8 ноября 1990 г. [14], Конвенция о защите детей от сексуальной эксплуатации и сексуального насилия от 25 октября 2007 г. [15] и др.).

В то же время оценка результатов деятельности Управления ООН по наркотикам и преступности (далее — УНП ООН) по оказанию

содействия и поддержки осуществлению Протокола о предупреждении и пресечении торговли людьми, особенно женщинами и детьми, и наказании за нее, дополняющего Конвенцию ООН против транснациональной организованной преступности, представленная на Конференции участников Конвенции ООН против транснациональной организованной преступности (Вена, 12—16 октября 2020 г.), выглядит более прогрессивно. Об этом свидетельствуют увеличившееся до 185 количество участников Протокола по итогам проведения Конференции и акцентирование внимания на практическом сегменте УНП ООН — осуществлять комплексную стратегию борьбы с торговлей людьми, оказывая содействие и поддержку путем реализации Протокола своей нормотворческой деятельностью и определения политики, формирования корпуса знаний, межучрежденческого сотрудничества и взаимодействия и технического сотрудничества [6]. В этом контексте выборочное и необоснованное конструирование региональной (европейской) системы безопасности, в обход возможностей универсальных инструментариев безопасности, выглядит достаточно амбивалентно.

В целях выработки устойчивой правовой позиции Республики Беларусь в системе ООН и укрепления ее межгосударственного авторитета предлагаем в рамках собственной правотворческой инициативы *проект Протокола о предотвращении и пресечении преступлений в сфере высоких технологий, особенно киберпреступлений, и наказаниях за них, дополняющего Конвенцию ООН против транснациональной организованной преступности 2000 г.* (см. приложение).

В пользу принятия указанного проекта можно пояснить следующее.

1. Несмотря на серьезную работу над проектом Международной (Всеобъемлющей) конвенции ООН о противодействии использованию информационно-коммуникационных технологий в преступных целях, вопрос о ее своевременном принятии остается пока проблематичным. Это вызвано, на наш взгляд, высокой степенью политизации «неконструктивного международно-правового вакуума» [1, с. 9—10], сложившегося в результате усиливающейся политической конъюнктуризации в отношении правотворческих инициатив, предлагаемых Россией и поддерживающей ее Республикой Беларусь в данной сфере. В частности, предлагаемый Российской Федерацией проект Всеобъемлющей конвенции ООН по обеспечению международной информационной безопасности [53], одобряемый Республикой Беларусь, необоснованно и безальтернативно блокируется западными странами.

2. Возможность использования юридического инструментария, содержащегося в Будапештской конвенции Совета Европы 2001 г., представляется ограниченной в силу, с одной стороны, ее определенного территориального характера, а с другой — неприемлемости статьи 32*b*) данной Конвенции, на основании которой ее участники получают трансграничный доступ к данным, которыми располагает другая сторона, без уведомления властей данного государства, располагающего соответствующей информацией. По авторитетному мнению некоторых российских экспертов [31], это дает возможность зарубежным спецслужбам вмешиваться без официального уведомления в деятельность компьютерных сетей (в частности, России), угрожать ее безопасности и суверенитету, нарушать фундаментальные гражданские права (особенно это касается личных (персональных) данных).

3. Недостаточная эффективность Конвенции ООН против транснациональной организованной преступности 2000 г. по урегулированию вопросов противодействия вновь возникающим видам киберпреступлений, особенно носящих системный, организованный и трансграничный характер (например, сетевого мошенничества, спамерской деятельности, легализации (отмывания) денег и финансирования терроризма, создания и распространения программ и методов, направленных на подрыв нормального функционирования критической инфраструктуры государств [10, с. 6—7] и пр.).

Представляется, что предлагаемый авторский проект протокола к Конвенции ООН 2000 г. может стать отправной точкой и своего рода компромиссным вариантом урегулирования вопросов противодействия киберпреступности и информационной безопасности на универсальном уровне.

Таким образом, опираясь на значительную эмпирическую и научно-теоретическую базу, раскрывающую отдельные, но немаловажные стороны рассматриваемой проблематики, подчеркнем настоятельную необходимость ее дальнейшего совершенствования, особенно с точки зрения прогрессивного развития международного права в данной области, в противовес внеконвенциональной деятельности отдельных международных неправительственных организаций (например, *Internet Corporation for Assigned Names and Numbers (ICAAN)*, *Society for Worldwide Interbank Financial Telecommunications (SWIFT)*, *International Organization for Standardization (ISO)*), иных негосударственных акторов (например, западных частных военных и охранных компаний), обоснованно рассматриваемых в ряде случаев в качестве квазисубъектов транснациональной организованной преступности [50].

Предлагаемый проект протокола, дополняющего Конвенцию против транснациональной организованной преступности 2000 г., не противоречит цели самой Конвенции (ст. 1), соответствует сферам ее применения (ст. 3),

подтверждается статьей 37 Конвенции (взаимосвязь с протоколами), предусматривающей возможность дополнения Конвенции одним или несколькими протоколами. Поскольку Конвенция против транснациональной организованной преступности 2000 г. насчитывает к настоящему времени 190 участников, можно констатировать ее безусловную юридическую состоятельность, что, если не предопределяет, то и не исключает определенное внимание к предлагаемому проекту дополнительного протокола к ней.

Данный проект протокола направлен на решение, хотя только и определенной части специфических проблем в рассматриваемой области, однако уже имеющих устойчивую юридическую основу в формате действующей Конвенции против транснациональной организованной преступности 2000 г., особенно важных при реализации функциональных возможностей системы коллективной (региональной) безопасности, в том числе и в части обеспечения интересов национальной безопасности Республики Беларусь.

## Список использованных источников


1. Арчаков, В. Ю. К вопросу о международных коррупционных рейтингах / В. Ю. Арчаков, А. Л. Баньковский, И. В. Щеглов // Законность и правопорядок. — 2021. — № 3. — С. 9—15.
2. Баньковский, А. Л. Концептуальные взгляды стран запада на кибервойны / А. Л. Баньковский, П. И. Савков // Современный мир и национальные интересы Республики Беларусь: материалы Междунар. науч. конф., Минск, 17 дек. 2021 г. / редкол.: Е. А. Достанко (гл. ред.) [и др.]. — Минск: БГУ, 2021. — С. 40—45.
3. Валеев, Д. М. Международно-правовые основы сотрудничества по борьбе с транснациональной организованной преступностью: дис. ... канд. юрид. наук: 12.00.10 / Д. М. Валеев. — М., 2016. — 227 л.
4. В Вене проходят переговоры по разработке конвенции о борьбе с киберпреступностью [Электронный ресурс] // Новости ООН. — 17.01.2023. — Режим доступа: <https://news.un.org/ru/story/2023/01/1436692>. — Дата доступа: 26.09.2023.
5. Верхелст, Э. Глобальное управление в сфере кибербезопасности: взгляд с позиции международного права и права ЕС / Э. Верхелст, Я. Ваутерс // Вестн. междунар. организаций. — 2020. — Т. 15, № 2. — С. 141—172.
6. Деятельность Управления Организации Объединенных Наций по наркотикам и преступности по оказанию содействия и поддержки осуществлению Протокола о предупреждении и пресечении торговли людьми, особенно женщинами и детьми, и наказании за нее, дополняющего Конвенцию Организации Объединенных Наций против транснациональной организованной преступности: доклад Секретариата: док. ООН CTOC/COP/2020/2 [Электронный ресурс] // Управление ООН по наркотикам и преступности. — Режим доступа: <https://www.unodc.org/documents/treaties/UNTOC/COP/SESSION_10/Website/CTOC_COP_2020_2/CTOC_COP_2020_2_R.pdf>. — Дата доступа: 26.09.2023.
7. Довгань, Е. Ф. Международные организации и поддержание международного мира и безопасности / Е. Ф. Довгань. — Минск: Междунар. ун-т «МИТСО», 2016. — 262 с.
8. Довгань, Е. Ф. Региональный механизм системы коллективной безопасности в современном международном праве: дис. ... д-ра юрид. наук: 12.00.10 / Е. Ф. Довгань. — Минск, 2014. — 333 л.
9. Жу Цичао. Влияние развития технологий искусственного интеллекта на кибербезопасность / Жу Цичао [Электронный ресурс] // Сборник докладов участников пятнадцатого международного форума «Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности», Москва, 27—29 сент. 2021 г. — С. 142—143. — Режим доступа: <https://namib.online/wp-content/uploads/2021/12/%D0%A1%D0%91%D0%9E%D0%A0%D0%9D%D0%98%D0%9A-%D0%94%D0%9E%D0%9A%D0%9B%D0%90%D0%94%D0%9E%D0%92-%D0%A3%D0%A7%D0%90%D0%A1%D0%A2%D0%9D%D0%98%D0%9A%D0%9E%D0%92-XV-%D0%9C%D0%95%D0%96%D0%94%D0%A3%D0%9D%D0%90%D0%A0%D0%9E%D0%94%D0%9D%D0%9E%D0%93%D0%9E-%D0%A4%D0%9E%D0%A0%D0%A3%D0%9C%D0%90.pdf>. — Дата доступа: 02.01.2023.
10. Информационная безопасность личности и государства в современном международном праве: материалы «круглого стола» каф. гос. управления юрид. фак. Белорус. гос. ун-та, Минск, 12 апр. 2022 г. / редкол.: В. С. Михайловский (гл. ред.), Е. Ф. Довгань, Н. О. Мороз. — Минск: БГУ, 2022. — 298 с.
11. К «недружественным» отнесли все страны ЕС и еще 12 государств [Электронный ресурс] // Экономическая газета. — 08.04.2022. — Режим доступа: <https://neg.by/novosti/otkrytj/k-nedruzhestvennym-otnesli-vse-strany-es-i-eshche-12-gosudarstv/>. — Дата доступа: 02.01.2023.
12. Конвенция о преступности в сфере компьютерной информации ETS N 185 (Будапешт, 23 нояб. 2001 г.) [Электронный ресурс] // Информационно-правовой портал «ГАРАНТ.РУ». — Режим доступа: <http://base.garant.ru/4089723/>. — Дата доступа: 08.02.2023.
13. Конвенция Организации Объединенных Наций против транснациональной организованной преступности: принята резолюцией Генеральной Ассамблеи 15 нояб. 2000 г. [Электронный ресурс] // Организация Объединенных Наций. — Режим доступа: <https://www.un.org/ru/documents/decl_conv/conventions/orgcrime.shtml>. — Дата доступа: 02.01.2023.
14. Конвенция Совета Европы об отмывании, выявлении, изъятии и конфискации доходов от преступной деятельности ETS N 141 (Страсбург, 8 нояб. 1990 г.). [Электронный ресурс] // Информационно-правовой портал «ГАРАНТ.РУ». — Режим доступа: <https://base.garant.ru/2541079/>. — Дата доступа: 08.02.2023.
15. Конвенция Совета Европы о защите детей от сексуальной эксплуатации и сексуального насилия (Лансарот, 25 окт. 2007 г.) [Электронный ресурс] // Электронный фонд нормативно-технической и нормативно-правовой информации Консорциума «Кодекс». — Режим доступа: <https://docs.cntd.ru/document/499039123>. — Дата доступа: 08.02.2023.
16. Макаров, О. С. Правовое обеспечение информационной безопасности на примере защиты государственных секретов государств — участников Содружества Независимых Государств: автореф. дис. ... д-ра юрид. наук: 12.00.13 / О. С. Макаров. — М., 2013. — 52 с.
17. Мозолина, О. В. Публично-правовые аспекты международного регулирования отношений в Интернете: автореф. дис. ... канд. юрид. наук: 12.00.10 / О. В. Мозолина. — М., 2008. — 26 с.
18. Мороз, Н. О. Международно-правовое сотрудничество в борьбе с преступностью в сфере высоких технологий / Н. О. Мороз. — Минск: Междунар. ун-т «МИТСО», 2017. — 266 с.
19. Об утверждении Концепции национальной безопасности Республики Беларусь: Указ Президента Респ. Беларусь от 9 нояб. 2010 г. № 575 [Электронный ресурс] // КонсультантПлюс. Беларусь / ООО «ЮрСпектр», Нац. центр правовой информ. Респ. Беларусь. — Минск, 2023.

20. Об утверждении перечня иностранных государств и территорий, совершающих недружественные действия в отношении Российской Федерации, российских юридических и физических лиц: распоряжение Правительства Рос. Федерации от 5 марта 2022 г. № 430-р [Электронный ресурс] // КонсультантПлюс. Россия / ЗАО «Консультант Плюс». — М., 2023.
21. Овчинский, В. Организованная киберпреступность / В. Овчинский, Ю. Жданов [Электронный ресурс] // Завтра. ру. — 25.11.2021. — Режим доступа: <https://zavtra.ru/blogs/organizovannaya_kiberprestupnost_>. — Дата доступа: 02.01.2023.
22. О Концепции информационной безопасности Республики Беларусь: постановление Совета Безопасности Респ. Беларусь от 18 марта 2019 г. № 1 [Электронный ресурс] // КонсультантПлюс. Беларусь / ООО «ЮрСпектр», Нац. центр правовой информ. Респ. Беларусь. — Минск, 2023.
23. О присоединении Республики Беларусь к Конвенции Совета Европы о противодействии торговле людьми: Закон Респ. Беларусь от 12 июля 2013 г. № 40-З [Электронный ресурс] // Там же.
24. О присоединении Республики Беларусь к Протоколу против незаконного изготовления и оборота огнестрельного оружия, его составных частей и компонентов, а также боеприпасов к нему, дополняющему Конвенцию Организации Объединенных Наций против транснациональной организованной преступности: Закон Респ. Беларусь от 4 авг. 2004 г. № 312-З [Электронный ресурс] // Там же.
25. О ратификации Протокола о взаимодействии государств — членов Организации Договора о коллективной безопасности по противодействию преступной деятельности в информационной сфере: Закон Респ. Беларусь от 15 июля 2015 г. № 292-З [Электронный ресурс] // Там же.
26. О ратификации Протокола о предупреждении и пресечении торговли людьми, особенно женщинами и детьми, и наказании за нее, дополняющего Конвенцию Организации Объединенных Наций против транснациональной организованной преступности: Закон Респ. Беларусь от 3 мая 2003 г. № 197-З [Электронный ресурс] // Там же.
27. О ратификации Протокола против незаконного ввоза мигрантов по суше, морю и воздуху, дополняющего Конвенцию Организации Объединенных Наций против транснациональной организованной преступности: Закон Респ. Беларусь от 3 мая 2003 г. № 196-З [Электронный ресурс] // Там же.
28. Осуществление Конвенции Организации Объединенных Наций против транснациональной организованной преступности: инструментарий оценки потребностей. — Нью-Йорк: ООН, 2016. — vi, 103 с. [Электронный ресурс] // Управление Организации Объединенных Наций по наркотикам и преступности. — Режим доступа: <https://www.unodc.org/documents/organized-crime/tools_and_publications/16-02940_R_ebook.pdf>. — Дата доступа: 02.01.2023.
29. О Шанхайской организации сотрудничества [Электронный ресурс] // Шанхайская организация сотрудничества. — 08.12.2015. — Режим доступа: <https://rus.sectsco.org/20151208/16789.html>. — Дата доступа: 02.01.2023.
30. Полякова, Т. А. Развитие системы международной информационной безопасности и стратегические задачи правового обеспечения информационной безопасности на национальном и региональном уровнях / Т. А. Полякова [Электронный ресурс] // Сборник докладов участников пятнадцатого международного форума «Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности», Москва, 27—29 сент. 2021 г. — С. 47—50. — Режим доступа: <https://namib.online/wp-content/uploads/2021/12/%D0%A1%D0%91%D0%9E%D0%A0%D0%9D%D0%98%D0%9A-%D0%94%D0%9E%D0%9A%D0%9B%D0%90%D0%94%D0%9E%D0%92-%D0%A3%D0%A7%D0%90%D0%A1%D0%A2%D0%9D%D0%98%D0%9A%D0%9E%D0%92-XV-%D0%9C%D0%95%D0%96%D0%94%D0%A3%D0%9D%D0%90%D0%A0%D0%9E%D0%94%D0%9D%D0%9E%D0%93%D0%9E-%D0%A4%D0%9E%D0%A0%D0%A3%D0%9C%D0%90.pdf>. — Дата доступа: 02.01.2023.
31. Российский дипломат назвал Будапештскую конвенцию по киберпреступлениям устаревшей [Электронный ресурс] // ТАСС. — 04.12.2017. — Режим доступа: <https://tass.ru/politika/4782506>. — Дата доступа: 10.04.2023.
32. Россия и Беларусь предлагают разработать конвенцию о борьбе с использованием информационных технологий в преступных целях [Электронный ресурс] // Новости ООН. — 20.10.2019. — Режим доступа: <https://news.un.org/ru/story/2019/10/1365291>. — Дата доступа: 26.09.2023.
33. Сеитов, Т. Б. Международно-правовое сотрудничество государств в борьбе с компьютерной преступностью: автореф. дис. ... канд. юрид. наук: 12.00.10 / Т. Б. Сеитов. — Алматы, 2002. — 23 с.
34. Соглашение о сотрудничестве государств — участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации от 01.06.2001 г. [Электронный ресурс] // Исполнительный комитет Содружества Независимых Государств. — Режим доступа: <https://cis.minsk.by/page/866>. — Дата доступа: 02.01.2023.
35. Содействие оказанию технической помощи и наращиванию потенциала для усиления национальных мер и укрепления международного сотрудничества в целях борьбы с киберпреступностью, включая обмен информацией: док. ООН A/RES/74/173 [Электронный ресурс] // Цифровая библиотека Организации Объединенных Наций. — Режим доступа: <https://digitallibrary.un.org/record/3847137>. — Дата доступа: 02.01.2023.
36. Сотрудничество в сфере безопасности [Электронный ресурс] // Интернет-портал СНГ. — Режим доступа: <https://e-cis.info/cooperation/2828/>. — Дата доступа: 02.01.2023.
37. Calderoni, F. The European legal framework on cybercrime: striving for an effective implementation / F. Calderoni // Crime, Law a. Social Change. — 2010. — Vol. 54, N 5. — P. 339—357. (http://dx.doi.org/10.1007/s10611-010-9261-6)
38. Consolidated negotiating document on the general provisions and the provisions on criminalization and on procedural measures and law enforcement of a comprehensive international convention on countering the use of information and communications technologies for criminal purposes: [status as of 21 Jan. 2023] [Electronic resource] // United Nations Office on Drugs and Crime. — Mode of access: <https://www.unodc.org/documents/Cybercrime/AdHocCommittee/4th_Session/Documents/CND_21.01.2023_-_Copy.pdf>. — Date of access: 19.10.2023.
39. Cooperation between the United Nations and the International Criminal Police Organization (INTERPOL): UN Doc. A/RES/75/10 [Electronic resource] // United Nations Digital Library. — Mode of access: <https://digitallibrary.un.org/record/3893795>. — Date of access: 02.02.2023.
40. Cooperation between the United Nations and the International Criminal Police Organization (INTERPOL): UN Doc. A/RES/71/19 [Electronic resource] // United Nations Digital Library. — Mode of access: <https://digitallibrary.un.org/record/851099>. — Date of access: 02.02.2023.
41. Cooperation between the United Nations and the International Criminal Police Organization (INTERPOL): UN Doc. A/RES/77/20 [Electronic resource] // United Nations Digital Library. — Mode of access: <https://digitallibrary.un.org/record/3996188>. — Date of access: 02.02.2023.
42. Cooperation between the United Nations and the International Criminal Police Organization (INTERPOL): UN Doc. A/RES/73/11 [Electronic resource] // United Nations Digital Library. — Mode of access: <https://digitallibrary.un.org/record/1654579>. — Date of access: 02.02.2023.
43. Council of Europe Convention on Action against Trafficking in Human Beings (CETS № 197) (Warsaw, 16.05.2005) [Electronic resource] // Conventions. — Mode of access: <https://www.conventions.ru/int/11578/>. — Date of access: 08.02.2023.

44. Cybercrime [Electronic resource] // INTERPOL. — Mode of access: <https://www.interpol.int/Crimes/Cybercrime>. — Date of access: 18.12.2022.
45. Cybersecurity: public sector threats and response / ed. by K. J. Andreasson. — Boca Raton: CRC Press, 2011. — 392 p. (https://doi.org/10.1201/b11363)
46. Global Strategy on Organized and Emerging Crime [Electronic resource] // INTERPOL. — Mode of access: <https://www.interpol.int/content/download/5582/file/Global%20Strategy%20on%20Organized%20and%20Emerging%20Crime.pdf>. — Date of access: 09.12.2021.
47. Kramer, A. E. Expert Issues a Cyberwar Warning / A. E. Kramer, N. Perlroth [Electronic resource] // The New York Times. — 03.06.2012. — Mode of access: <https://www.nytimes.com/2012/06/04/technology/cyberweapon-warning-from-kaspersky-a-computer-security-expert.html>. — Date of access: 12.01.2023.
48. Kruessmann, T. Human rights in combating organised crime and the problem of «illegal» migration in Europe / T. Kruessmann // Журн. Белорус. гос. ун-та. Право. — 2020. — № 3. — С. 24—29.
49. McCusker, R. Transnational organized cyber crime: distinguishing threat from reality / R. McCusker // Crime, Law and Social Change. — 2006. — Vol. 46, N 4-5. — P. 257—273.
50. Merkushin, V. V. Non-state actors as quasi-subjects of transnational organised crime: implications for the security of states / V. V. Merkushin // Journal of the Belarusian State University. International Relations. — 2022. — N 1. — P. 66—73.
51. Organized crime [Electronic resource] // INTERPOL. — Mode of access: <https://www.interpol.int/Crimes/Organized-crime>. — Date of access: 18.12.2022.
52. Schjolberg, S. A Global Treaty on Cybersecurity and Cybercrime / S. Schjolberg, S. Ghernaouti-Helie [Electronic resource] // CyberCrime Law. — Mode of access: <https://cybercrimelaw.net/documents/A_Global_Treaty_on_Cybersecurity_and_Cybercrime,_Second_edition_2011.pdf>. — Date of access: 01.01.2023.
53. The Russian Federation submitted to the United Nations the world's first draft convention against cybercrime [Electronic resource] // CySecurity. — 29.07.2021. — Mode of access: <https://www.cysecurity.news/2021/07/the-russian-federation-submitted-to.html>. — Date of access: 08.11.2022.
54. 2022: the year in review [Electronic resource] // INTERPOL. — 23.12.2022. — Mode of access: <https://www.interpol.int/News-and-Events/News/2022/2022-the-year-in-review>. — Date of access: 02.01.2023.
55. UNGA and UNSC resolutions highlighting INTERPOL's role [Electronic resource] // INTERPOL. — Mode of access: <https://www.interpol.int/Our-partners/International-organization-partners/INTERPOL-and-the-United-Nations/UNGA-and-UNSC-resolutions-highlighting-INTERPOL-s-role>. — Date of access: 02.01.2023.
56. United Nations designates 7 September as International Day of Police Cooperation [Electronic resource] // INTERPOL. — Mode of access: <https://www.interpol.int/News-and-Events/News/2022/United-Nations-designates-7-September-as-International-Day-of-Police-Cooperation>. — Date of access: 18.12.2022.

Статья поступила в редакцию 16 апреля 2023 г., доработана в октябре 2023 г.



**ПРИЛОЖЕНИЕ**
*Проект*

## Протокол о предотвращении и пресечении преступлений в сфере высоких технологий, особенно киберпреступлений, и наказаниях за них, дополняющий Конвенцию ООН против транснациональной организованной преступности 2000 г.



### ПРЕАМБУЛА

*Государства — участники настоящего Протокола,*

*заявляя*, что для принятия эффективных мер по предотвращению преступлений в сфере высоких технологий, особенно киберпреступлений, и борьбе с ними необходим всеобъемлющий международный подход в странах их подготовки, организации и совершения, включающий меры, направленные на предупреждение таких преступлений, наказание занимающихся ими лиц, включая сотрудничество, обмен информацией и другие надлежащие меры на национальном, региональном и международном уровнях,

*сознавая* безотлагательную необходимость предотвращения и пресечения преступлений в сфере высоких технологий, особенно киберпреступлений, поскольку такие действия наносят ущерб безопасности каждого государства, отдельного региона и мира в целом, создавая угрозу благополучию народов, их социально-экономическому развитию и праву на защиту личной информации,

*учитывая* то обстоятельство, что, несмотря на существование целого ряда региональных международных документов, содержащих нормы и предусматривающих практические меры по борьбе с киберпреступностью, отсутствует универсальный документ, в котором затрагивались бы все аспекты преступлений в сфере высоких технологий, особенно киберпреступлений,

*будучи обеспокоены* тем, что в отсутствие такого документа лица, которые являются уязвимыми с точки зрения преступлений в сфере высоких технологий, не будут в достаточной мере защищены в силу значительного расширения деятельности организованных преступных групп применительно к связанной с этим преступной деятельности, которая причиняет огромный ущерб многим государствам,

*руководствуясь* принципами равноправия и самоопределения народов, закрепленными в Уставе Организации Объединенных Наций, Декларации о принципах международного права, касающихся дружественных отношений и сотрудничества между государствами, в соответствии с Уставом Организации Объединенных Наций и Конвенции о международном праве опровержения,

*будучи убеждены*, что дополнение Конвенции Организации Объединенных Наций против транснациональной организованной преступности, принятой 15 ноября 2000 г. (далее — Конвенция), международным документом о предотвращении и пресечении преступлений в сфере высоких технологий, особенно киберпреступлений, и наказаниях за них будет способствовать предупреждению таких преступлений и борьбе с ними,

*согласились о нижеследующем:*

## I. ОБЩИЕ ПОЛОЖЕНИЯ

### Статья 1
### Связь с Конвенцией Организации Объединенных Наций против транснациональной организованной преступности

1. Настоящий Протокол дополняет Конвенцию.

2. Положения Конвенции применяются *mutatis mutandis* к настоящему Протоколу, если в нем не предусмотрено иное.

3. Преступления, признанные таковыми в соответствии со статьей 5 настоящего Протокола, рассматриваются как преступления, признанные таковыми в соответствии с Конвенцией.

### Статья 2
### Цели

Цель настоящего Протокола заключается в предупреждении преступлений в сфере высоких технологий, особенно киберпреступлений, и борьбе с ними, а также в содействии развитию, облегчению и укреплению сотрудничества между Государствами-участниками в достижении этих целей.

### Статья 3
### Термины

Для целей настоящего Протокола:

a) «преступление в сфере высоких технологий» означает преступление, осуществляемое в целях получения, прямо или косвенно, какой-либо финансовой или иной материальной выгоды путем незаконного использования телекоммуникационных технологий и (или) компьютерных технологий, а также иных технических средств, применяемых для сбора данных в целях дальнейшего преобразования этих данных при помощи телекоммуникационных и (или) компьютерных технологий;

b) «киберпреступление» означает осуществление незаконных действий в целях получения, прямо или косвенно, финансовой или иной материальной выгоды, непосредственно совершенных с использованием и (или) против компьютерной информации, компьютерной сети или системы (технологий), телекоммуникационных технологий;

c) «незаконное использование информационно-телекоммуникационных технологий» означает применение способов и форм передачи информации по информационно-коммуникационным сетям (телефонным линиям, каналам спутниковой связи, компьютерным сетям, включая сеть Интернет, и др.) без соблюдения необходимых требований для законного их применения;

d) «незаконное использование компьютерных технологий» означает применение программных средств, осуществляющих функции хранения, передачи, обработки, защиты и визуализации (воспроизведения) данных с использованием компьютерной сети или системы без соблюдения необходимых требований для законного их применения;

e) «детская порнография в информационно-коммуникационных сетях либо с использованием компьютерных технологий» означает преступление, осуществляемое путем создания, распространения и хранения какими бы то ни было средствами любых изображений ребенка, совершающего реальные или смоделированные откровенно сексуальные действия, или любое изображение половых органов ребенка главным образом в сексуальных целях.

### Статья 4
### Сфера применения

Настоящий Протокол, если в нем не указано иное, применяется к предупреждению, расследованию и уголовному преследованию в связи с преступлениями, признанными таковыми в соответствии со статьей 5 настоящего Протокола, если эти преступления носят транснациональный характер и совершены при участии организованной преступной группы, а также к защите права лиц, которые стали объектом таких преступлений.

### Статья 5
### Криминализация

1. Каждое Государство-участник принимает такие законодательные и другие меры, которые могут потребоваться, с тем, чтобы признать в качестве уголовно наказуемых деяния, указанные в статье 3 настоящего Протокола, когда они совершаются умышленно, в том числе следующие деяния:

a) «кардинг» — использование, продажа, совместное использование или иное распространение украденных данных с кредитной или дебетовой карты;

b) «криптоджекинг» — незаконный майнинг (добывание) криптовалют;

c) «взлом или незаконный доступ к информационно-телекоммуникационным технологиям» — получение несанкционированного или незаконного доступа к информационно-телекоммуникационным технологиям, а также превышение законного (санкционированного) доступа к информационно-телекоммуникационным технологиям в установленных законодательством и иными не противоречащих законодательству случаях;

d) раскрытие личной информации или переход по ссылке, зараженной вредоносным программным обеспечением;

e) «ботнет» — разработка и(или) заражение вредоносными программами информационно-коммуникационных сетей, иных цифровых устройств в целях их отслеживания, удаленного управления и иного использования;

f) «подделка с использованием информационно-коммуникационных технологий (компьютерная подделка)» — незаконное действие в целях ввода, изменения, удаления или подавления компьютерных данных, приводящее к получению недостоверных данных с намерением придания им вида подлинных, независимо от того, доступны данные для прямого чтения или являются понятными;

g) «мошенничество с использованием информационно-коммуникационных технологий (компьютерное мошенничество)» — незаконное действие в целях ввода, изменения, удаления или подавления компьютерных данных или любого вмешательства в функционирование компьютерной системы для получения финансовой, материальной и иной выгоды для себя или другого лица (лиц);

h) «банковское мошенничество с использованием информационно-коммуникационных технологий» — незаконное (несанкционированное) использование платежных данных лиц в целях получения финансовой, материальной и иной выгоды для себя или другого лица (лиц) («скимминг», «фишинг» и пр.);

i) «онлайн мошенничество (мошенничество в сети Интернет)» — незаконное действие посредством нежелательных сообщений в электронной почте, телефонных звонков, текстовых сообщений, платформ социальных сетей, приложений и веб-сайтов в целях вынуждения лица предоставить денежные средства, материальное и иное имущество, а также информацию либо заставить лицо участвовать в каких-либо действиях;

j) «киберэксторсия» — вымогательство с помощью информационно-коммуникационных технологий («сексторсия», мошенничество с выкупом, «доксинг» и др.);

k) незаконные азартные игры в сети Интернет;

l) легализация («отмывание») преступных активов.

2. Каждое Государство-участник при условии соблюдения основных принципов своей правовой системы принимает также такие законодательные и иные меры, которые могут потребоваться с тем, чтобы признать в качестве уголовно наказуемых в соответствии с пунктом 1 настоящей статьи следующие деяния:

a) покушение на совершение соответствующего преступления;

b) участие в качестве сообщника в совершении соответствующего преступления; и

c) организация других лиц в виде пособничества, подстрекательства, содействия, координации и руководства ими в целях совершения соответствующего преступления.

3. Каждое Государство-участник принимает такие законодательные и иные меры, которые могут потребоваться, с тем, чтобы признать в качестве обстоятельств, отягчающих преступления, признанные таковыми в соответствии с пунктом 2 настоящей статьи, и при условии соблюдения основных принципов своей правовой системы обстоятельства:

a) которые ставят или могут поставить под угрозу жизнь или безопасность лиц, использующих информационно-коммуникационные сети (технологии); или

b) которые связаны с унижающим достоинство обращением с лицами, не достигшими 18-летнего возраста, в том числе в целях сексуальной эксплуатации.

4. Ничто в настоящем Протоколе не препятствует Государству-участнику принимать меры в отношении какого-либо лица, деяние которого является уголовно наказуемым согласно внутреннему законодательству данного государства.

### Статья 6
### Конфискация, арест и отчуждение

1. Без ущерба для положений статьи 12 Конвенции Государства-участники принимают в максимально возможной в рамках их внутренних правовых систем степени такие меры, которые могут потребоваться для обеспечения возможности конфискации доходов от преступления согласно статье 2*e)* Конвенции.

2. Государства-участники принимают в рамках своих внутренних правовых систем такие меры, которые могут потребоваться для борьбы с «отмыванием» денежных средств, полученных в результате соответствующих преступлений, без ущерба для положений статей 6 и 7 Конвенции.

## II. ПРЕДУПРЕЖДЕНИЕ ПРЕСТУПЛЕНИЙ В СФЕРЕ ВЫСОКИХ ТЕХНОЛОГИЙ, ОСОБЕННО КИБЕРПРЕСТУПЛЕНИЙ

### Статья 7
### Информация

1. Каждое Государство-участник обеспечивает хранение в течение не менее десяти лет информации, которая касается преступлений, указанных в статье 3 настоящего Протокола. Такая информация включает, в частности:

a) данные, касающиеся методов, способов и средств совершения преступлений, а также лиц, совершивших преступления, указанные в статье 5 настоящего Протокола;

b) данные об организованных преступных группах, которые, как это известно или которые подозреваются, принимают участие в совершении преступлений в сфере высоких технологий, особенно киберпреступлений, и методах, которые они используют;

c) средства сокрытия, используемые при совершении преступлений в сфере высоких технологий, особенно киберпреступлений, и способы их выявления;

d) законодательный опыт, а также практику и меры, направленные на предупреждение и пресечение преступлений в сфере высоких технологий, особенно киберпреступлений, и борьбу с этими деяниями;

e) научно-техническую информацию, полезную для деятельности правоохранительных органов в целях расширения их возможностей по предупреждению, выявлению и расследованию деяний, указанных в статье 5 настоящего Протокола, и уголовного преследования причастных к ним лиц.

2. Государства-участники предоставляют или в надлежащих случаях обмениваются между собой соответствующей научно-технической информацией в интересах правоохранительных органов с тем, чтобы расширить их возможности в отношении предупреждения, выявления и расследования преступлений в сфере высоких технологий, особенно киберпреступлений, и судебного преследования причастных к такой незаконной деятельности лиц.

3. Государства-участники сотрудничают между собой в предупреждении, выявлении и расследовании преступлений в сфере высоких технологий, особенно киберпреступлений. Такое сотрудничество включает незамедлительный ответ на запросы об оказании помощи в выявлении и отслеживании указанных преступлений в пределах имеющихся возможностей.

4. При условии соблюдения основных принципов своей правовой системы или любых других международных соглашений каждое Государство-участник гарантирует конфиденциальность получаемой им в соответствии с настоящей статьей от другого Государства-участника информации, относящейся к государственным секретам, а также иной защищаемой информации в соответствии с законодательством Государств-участников, включая защищенную правами собственности информацию, связанную с коммерческими сделками, и соблюдает любые ограничения в отношении использования такой информации в случае обращения к нему с соответствующей просьбой Государства-участника, предоставляющего информацию. Если такая конфиденциальность не может быть обеспечена, Государство-участник, предоставившее информацию, уведомляется об этом до ее разглашения.

5. Государство-участник, которое получает информацию, выполняет любую просьбу предоставляющего Государства-участника, сопряженную с установлением ограничений в отношении ее использования.

### Статья 8
### Сотрудничество

1. Государства-участники сотрудничают на двустороннем, региональном и международном уровнях в целях предупреждения и пресечения преступлений в сфере высоких технологий, особенно киберпреступлений, и борьбы с такими деяниями.

2. Без ущерба для положений пункта 13 статьи 18 Конвенции каждое Государство-участник назначает национальный орган или должностное лицо для поддержания связей между ним и другими Государствами-участниками по вопросам, относящимся к настоящему Протоколу.

3. Государства-участники рассматривают возможность заключения двусторонних или региональных соглашений, или оперативных договоренностей, или взаимопониманий, направленных на:

a) принятие наиболее надлежащих и эффективных мер по предупреждению деяний, указанных в статье 5 настоящего Протокола, и борьбу с ними; или

b) развитие применения положений настоящего Протокола в отношениях между Государствами-участниками.

**Статья 9**
**Подготовка кадров и техническая помощь**

Государства-участники сотрудничают друг с другом и в надлежащих случаях с соответствующими международными организациями в предоставлении Государствам-участникам по их просьбе помощи в подготовке кадров и технической помощи, необходимой для укрепления их возможностей в области предупреждения и пресечения преступлений в сфере высоких технологий, особенно киберпреступлений, и борьбы с такими деяниями, в том числе технической, финансовой и материальной помощи по вопросам, указанным в статьях 29 и 30 Конвенции.

**Статья 10**
**Брокеры и брокерские операции**

1. В целях предупреждения и противодействия преступлениям в сфере высоких технологий, особенно киберпреступлениям, Государства-участники, которые еще не предприняли соответствующие меры, рассматривают возможность создания системы регулирования деятельности лиц, осуществляющих брокерские операции. Такая система может предусматривать принятие одной или нескольких мер, например установления требований:

a) регистрации брокеров, действующих на их территории;

b) лицензирования или получения разрешения на брокерские операции; или

c) указания доменных имен или наименований брокеров, участвующих в сделке, и данных о их местонахождении в импортных и экспортных лицензиях, или разрешениях, или сопровождающих документах.

2. Государства-участники, которые создали систему разрешений в отношении брокерских операций, упомянутую в пункте 1 настоящей статьи, поощряются к обмену сведениями о брокерах и брокерских операциях в рамках обмена информацией и к хранению документации, касающейся брокеров и брокерских операций, согласно статье 7 настоящего Протокола.

**Статья 11**
**Другие меры по предупреждению**

1. Каждое Государство-участник принимает меры по обеспечению создания или совершенствования информационных программ, направленных на углубление понимания обществом того обстоятельства, что деяния, указанные в статье 5 настоящего Протокола, представляют собой преступную деятельность, которую часто осуществляют организованные преступные группы в корыстных целях и которая создает серьезную угрозу для соответствующих пользователей информационно-коммуникационных систем (технологий).

2. В соответствии со статьей 31 Конвенции Государства-участники сотрудничают в области общественной информации в целях предупреждения того, чтобы потенциальные пользователи информационно-коммуникационных систем (технологий) становились жертвами организованных преступных групп.

**Статья 12**
**Меры защиты и помощи**

1. При осуществлении настоящего Протокола каждое Государство-участник принимает в соответствии со своими обязательствами по международному праву все надлежащие меры, в том числе, если это необходимо, в области законодательства, для соблюдения и защиты прав лиц, которые стали объектом деяний, указанных в статье 5 настоящего Протокола, в том объеме, в котором эти права предусмотрены применимыми нормами международного права, в частности правом на свободный и полный доступ к информации при условии соблюдения и уважения прав иных лиц.

2. Каждое Государство-участник принимает надлежащие меры по предоставлению помощи лицам, пострадавшим от преступлений, указанных в статье 5 настоящего Протокола, а также от насилия, которому они могут подвергнуться со стороны отдельных лиц или группы лиц в результате того, что они стали объектом деяний, указанных в статье 5 настоящего Протокола.

3. При применении положений настоящей статьи Государства-участники принимают во внимание особую уязвимость женщин и детей.

4. В случае задержания какого-либо лица, которое стало объектом деяний, указанных в статье 5 настоящего Протокола, каждое Государство-участник выполняет свои обязательства по Венской конвенции о консульских сношениях 1963 г., когда это применимо, в том числе обязательство незамедлительно информировать это лицо о положениях, касающихся уведомлений, направляемых консульским должностным лицам, и сношений с такими должностными лицами.

## III. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

### Статья 13
### Урегулирование споров

1. Государства-участники стремятся урегулировать споры относительно толкования или применения настоящего Протокола путем переговоров.

2. Любой спор между двумя или более Государствами-участниками относительно толкования или применения настоящего Протокола, который не может быть урегулирован путем переговоров в течение разумного периода времени, передается по просьбе одного из этих Государств-участников на арбитражное разбирательство. Если в течение шести месяцев со дня обращения с просьбой об арбитраже эти Государства-участники не смогут договориться о его организации, любое из этих Государств-участников может передать спор в Международный Суд ООН, обратившись с заявлением в соответствии со Статутом Суда.

3. Каждое Государство-участник при подписании, ратификации, принятии, утверждении настоящего Протокола или присоединении к нему может заявить о том, что оно не считает себя связанным положениями пункта 2 настоящей статьи. Другие Государства-участники не связаны положениями пункта 2 настоящей статьи в отношении любого Государства-участника, сделавшего такую оговорку.

4. Любое Государство-участник, сделавшее оговорку в соответствии с пунктом 3 настоящей статьи, может в любое время снять эту оговорку путем направления уведомления Генеральному секретарю Организации Объединенных Наций.

### Статья 14
### Подписание, ратификация, принятие, утверждение и присоединение

1. Настоящий Протокол открыт для подписания всеми государствами в Центральных учреждениях Организации Объединенных Наций в Нью-Йорке начиная с тридцатого дня после его принятия Генеральной Ассамблеей.

2. Настоящий Протокол также открыт для подписания региональными организациями экономической интеграции при условии, что по меньшей мере одно из государств — членов такой организации подписало настоящий Протокол в соответствии с пунктом 1 настоящей статьи.

3. Настоящий Протокол подлежит ратификации, принятию или утверждению. Ратификационные грамоты или документы о принятии или утверждении сдаются на хранение Генеральному секретарю Организации Объединенных Наций. Региональная организация экономической интеграции может сдать на хранение свою ратификационную грамоту или документ о принятии или утверждении, если по меньшей мере одно из ее государств-членов поступило таким же образом. В ратификационной грамоте или в документе о принятии или утверждении такая организация заявляет о сфере своей компетенции в отношении вопросов, регулируемых настоящим Протоколом. Такая организация также сообщает депозитарию о любом соответствующем изменении.

4. Настоящий Протокол открыт для присоединения любого государства или любой региональной организации экономической интеграции, по меньшей мере одно из государств-членов которой является участником настоящего Протокола. Документы о присоединении сдаются на хранение Генеральному секретарю Организации Объединенных Наций. При присоединении региональная организация экономической интеграции заявляет о сфере своей компетенции в отношении вопросов, регулируемых настоящим Протоколом. Такая организация также сообщает депозитарию о любом соответствующем изменении сферы своей компетенции.

### Статья 15
### Вступление в силу

1. Настоящий Протокол вступает в силу на девяностый день после сдачи на хранение сороковой ратификационной грамоты или документа о принятии, утверждении или присоединении. Для цели настоящего пункта любая такая грамота или документ, сданные на хранение региональной организацией экономической интеграции, не рассматриваются в качестве дополнительных к грамотам или документам, сданным на хранение государствами — членами такой организации.

2. Для каждого государства или региональной организации экономической интеграции, которые ратифицируют, принимают или утверждают настоящий Протокол, или присоединяются к нему после сдачи на хранение сороковой ратификационной грамоты или документа о таком действии, настоящий Протокол вступает в силу на тридцатый день после сдачи на хранение таким государством или организацией соответствующей грамоты или документа или в дату вступления настоящего Протокола в силу в соответствии с пунктом 1 настоящей статьи в зависимости от того, что наступает позднее.

**Статья 16**
**Поправки**

1. По истечении пяти лет после вступления в силу настоящего Протокола Государство — участник настоящего Протокола может предложить поправку и направить ее Генеральному секретарю Организации Объединенных Наций, который затем препровождает предлагаемую поправку Государствам-участникам и Конференции Участников Конвенции в целях рассмотрения этого предложения и принятия решения по нему. Государства — участники настоящего Протокола, принимающие участие в Конференции Участников, прилагают все усилия для достижения консенсуса в отношении каждой поправки. Если все усилия по достижению консенсуса были исчерпаны и согласие не было достигнуто, то в качестве крайней меры для принятия поправки требуется большинство в две трети голосов Государств — участников настоящего Протокола, присутствующих или участвующих в голосовании на заседании Конференции Участников.

2. В вопросах, входящих в сферу их компетенции, региональные организации экономической интеграции осуществляют свое право голоса согласно настоящей статье, располагая числом голосов, равным числу их государств-членов, являющихся участниками настоящего Протокола. Такие организации не осуществляют свое право голоса, если их государства-члены осуществляют свое право голоса, и наоборот.

3. Поправка, принятая в соответствии с пунктом 1 настоящей статьи, подлежит ратификации, принятию или утверждению Государствами-участниками.

4. Поправка, принятая в соответствии с пунктом 1 настоящей статьи, вступает в силу в отношении Государства-участника через девяносто дней после даты сдачи им на хранение Генеральному секретарю Организации Объединенных Наций ратификационной грамоты или документа о принятии или утверждении такой поправки.

5. Поправка вступает в силу, когда она становится обязательной для тех Государств-участников, которые выразили согласие быть связанными ею. Другие Государства-участники продолжают быть связанными положениями настоящего Протокола и любыми поправками, ратифицированными, принятыми или утвержденными ими ранее.

**Статья 17**
**Денонсация**

1. Государство-участник может денонсировать настоящий Протокол путем направления письменного уведомления Генеральному секретарю Организации Объединенных Наций. Такая денонсация вступает в силу по истечении одного года после даты получения уведомления Генеральным секретарем.

2. Региональная организация экономической интеграции перестает быть участником настоящего Протокола, когда все ее государства-члены денонсировали настоящий Протокол.

**Статья 18**
**Депозитарий и языки**

1. Депозитарием настоящего Протокола назначается Генеральный секретарь Организации Объединенных Наций.

2. Подлинник настоящего Протокола, английский, арабский, испанский, китайский, русский и французский тексты которого являются равно аутентичными, сдается на хранение Генеральному секретарю Организации Объединенных Наций.

В УДОСТОВЕРЕНИЕ ЧЕГО нижеподписавшиеся полномочные представители, должным образом уполномоченные на то своими правительствами, подписали настоящий Протокол.