Guiding Questions
Наводящие вопросы

I. Криминализация

i. Первая группа вопросов[1]:

1. Какие элементы [психического/неправомерного] (например, [злонамеренный/нечестный] умысел) следует фиксировать при рассмотрении правонарушений, связанных с[незаконным/неправомерным/несанкционированным] доступом и перехватом? Должна ли конвенция предусматривать введение правовой защиты для исследователей в области кибербезопасности и других специалистов, работающих в области кибербезопасности (включая, среди прочего, тестировщиков на проникновение)?

Деяния, включенные в главу о криминализации проекта конвенции, соавторами которого стали Китай и ряд других государств, характеризуются прямым умыслом, что связано с характеристикой и способом совершения преступлений в сфере ИКТ. В частности, неправомерное воздействие на цифровую информацию (статья 8), создание, использование и распространение вредоносных программ (статья 10) и др. подразумевает умысел на совершение конкретного преступления и достижение определенной цели, корыстной или иной личной заинтересованности. В ряде случаев, однако, осведомленность в наличии такого посягательства может и вовсе отсутствовать, когда зараженное вредоносным программным обеспечением IT устройство лица применяется для сокрытия противоправной деятельности злоумышленника. С другой стороны, существуют киберзависимые деяния, при совершении которых прямого умысла в действиях преступника может и не содержаться.

---

1 **Первая группа: вопросы, касающиеся следующих предлагаемых положений:**

[Незаконный] [неправомерный] [несанкционированный] доступ; [данные] вмешательство [в цифровкю информацию]; вмешательство в компьютерную [систему] [сеть], [телекоммуникационную сеть] или [электронное устройство]; Препятствование работе компьютера, программы или данных; Нарушение работы сетей информационных и коммуникационных технологий; Атака на структуру сайта; Несанкционированный доступ или вмешательство в критически важную информационную инфраструктуру; [Незаконный] [неправомерный] [несанкционированный] перехват; Незаконное использование устройств или создание, использование и распространение вредоносного программного обеспечения; получение нечестным путем украденного компьютерного ресурса или устройства связи; Незаконное использование или содействие незаконному использованию информационных и коммуникационных технологий.

Что касается правовой защиты лиц, осуществляющих так называемый «правомерный» взлом компьютерных систем и средств их защиты (например, различных экспертов, тестировщиков, специалистов), необходимо ограничить пределы такого «добросовестного» вмешательства территорией и инфраструктурой своего государства, без возможности осуществлять такие действия на территории других государств и в их информационных сетях и пространстве. Возможность проведения «правомерного» взлома на территории иного государства допустима только по запросу и с согласия компетентных органов этого государства, иначе эти действия могут привести к нарушению права государств на суверенитет.

2. Считаете ли вы, что любое из предлагаемых действий должно приводить или иметь намерение причинить конкретный или серьезный вред или материальный ущерб, чтобы считаться правонарушением? Как определить «вред»?

Данный вопрос относится в основном к киберзависимым деяниям. Размер ущерба определяется национальным законодательством. По этому критерию возможно отграничение преступлений от правонарушений. Вместе с тем, если вопрос касается не материального ущерба, а конкретно вреда, то к таковому можно отнести вред здоровью, государственным интересам, окружающей среде и т.д.

3. Следует ли рассматривать нарушение мер безопасности как условие признания некоторых действий правонарушением, и если да, то при каких обстоятельствах?

См. комментарий к вопросу 1.

4. Можем ли мы рассматривать предлагаемые положения «Воспрепятствование работе компьютера, программы или данных», «Покушение на дизайн сайта» и «Нарушение работы сетей информационно-коммуникационных технологий» как формы [незаконного] [неправомерного] [несанкционированного] вмешательства?

Такие положения частично охватывается статьями 8 (Неправомерное воздействие на цифровую информацию) и 9 (Нарушение функционирования информационно-коммуникационных сетей) российского проекта конвенции, соавторами которого стали Китай и ряд других государств.

5. Как, по вашему мнению, конвенция должна решать вопрос о «несанкционированном доступе или вмешательстве в критически важную информационную инфраструктуру»?

В данном случае необходимо наличие умысла и отсутствие специального разрешения в соответствии с внутренним законодательством. При криминализации указанного состава преступления перечень КИИ может оставаться открытым и формироваться каждой страной в зависимости от национальных приоритетов.

6 Почему некоторые государства-члены выбирают использование термина «незаконный» «illegal», а другие «unlawful», третьи «unauthorized»? В чем разница по вашему мнению?

Считаем, что термин незаконный «illegal» («unlawful») является наиболее определенным, четким и понятным для всех государств-участников, не влечет неоднозначного толкования. При этом термин «illegal» используется в большинстве международных договоров по преступности. Полагаем, что термин «unauthorized» не всегда указывает на незаконность действий.

7 Почему некоторые государства-участники выбирают использование термина «без права» (without right), другие – без надлежащего санкционирования (without due authorization), третьи – незаконный (unlawfull)? В чем разница?

Полагаем, что ответ на данный вопрос приведен в ответе на вопрос 6. Наиболее приемлемым с точки зрения определённости является термин незаконный «illegal» («unlawful»).

8 Есть ли какая-либо разница между терминами данные и цифровая информация? И какой бы был предпочтительнее термин для Вас?

Понятия “информация (information)” и “данные (data)” для нас синонимичны. Представляется, что для целей разрабатываемой конвенции стоит вести речь исключительно об информации/данных, подлежащих автоматизированной обработке. Вместе с тем термин “данные”, по нашему мнению, в силу своей широты охватывает также и информацию в форме, неприемлемой для автоматизированной обработки. В этой связи предпочтительным для целей конвенции полагаем использование термина “цифровые данные” или “цифровая информация”.

9 Была ли какая-либо причина в некоторых предложениях не включать понятие ухудшение информации, а в других предложениях предпочтительнее использовать термин блокирование или подавление?

Для разрешения этого вопроса требуются дополнительные комментарии государств-участников, использующих указанные термины.

10 Считается ли копирование частью вмешательства в данные?

Полагаем, что если копирование цифровых данных осуществляется умышленно с целью последующего противоправного их использования, либо

в результате неправомерного доступа к ним, то, несомненно, такие действия являются вмешательством в цифровые данные. Умышленное неправомерное воздействие на цифровую информацию/данные возможно путем ее повреждения, удаления, изменения, блокирования, модификации либо копирования информации в цифровой форме.

11. Что касается уголовно-наказуемых деяний, имеющих отношение к вмешательству в систему/сеть, какие, по вашему мнению, устройства (и их номенклатура), к которым эта статья применяется: компьютерная система, компьютерная сеть, телекоммуникационная сеть, электронное устройство или устройство ИКТ?

Данная статья может применяться для уголовно наказуемых деяний в отношении информационных систем, информационно-телекоммуникационных сетей, устройств ИКТ.

12. Есть ли необходимость рассматривать перехват, как деяние, совершенное мошенническим путем?

Если мы правильно понимаем вопрос, то его суть сводится к следующему: всегда ли перехват осуществляется мошенническим путем?
Перехват не всегда совершается путем мошенничества. Вместе с тем перехват может рассматривается как деяние, совершенное мошенническим путем, например, если умысел направлен на хищение имущества путем уничтожения, блокирования, модификации либо копирования цифровой информации или иного вмешательства в функционирование ИКТ.

i. Вторая группа[2] вопросов

1. Считаете ли вы, что мошенничество, совершенное полностью или частично в Интернете, достаточно для охвата других действий, таких как кража,

2 ***Вторая группа: вопросы, касающиеся следующих предлагаемых положений:***

Подлог с использованием [Компьютера] [ИКТ] ; Создание и использование цифровой информации для введения пользователя в заблуждение; кража, связанная с информационными и коммуникационными технологиями; Мошенничество, связанное с компьютерами [ИКТ-]; Незаконное использование электронных платежных инструментов; преступления, связанные с использованием личных данных; Нарушение авторских и смежных прав с помощью информационно-коммуникационных технологий

мошенничество, финансовые преступления и преступления с использованием электронных платежных инструментов?

Мошенничество является одной из форм хищения, также как и кража. Под хищением следует понимать совершенные с корыстной целью противоправные безвозмездное изъятие и (или) обращение чужого имущества в пользу виновного или других лиц, причинившие ущерб собственнику или иному владельцу этого имущества.
В российском проекте, соавторами которого стали Китай и ряд других государств, отражена общая категория таких посягательств – «хищение с использованием ИКТ – т.е. хищение имущества, либо незаконное приобретение права на него, в том числе посредством мошенничества, путем уничтожения, блокирования, модификации либо копирования цифровой информации или иного вмешательства в функционирование ИКТ». В российском уголовном законодательстве для таких преступлений применяется универсальная формулировка «с использованием информационно-телекоммуникационных сетей, включая сеть «Интернет», при этом отдельно также выделяется состав преступления, связанный с хищением при использовании электронных платежных инструментов.

Универсальный характер носит формулировка «с использованием информационно-телекоммуникационных сетей, включая сеть «Интернет» Отдельно можно выделить хищение с использованием электронных платежных инструментов.

2. Что касается подлога, связанного с компьютером/ИКТ, какие элементы [психического/ошибочного] (например, [злонамеренного/нечестного] намерения) следует включить в криминализацию такого деяния? Должна ли конвенция предусматривать введение правовой защиты для исследователей в области кибербезопасности и других специалистов, работающих в области кибербезопасности (включая, среди прочего, тестировщиков на проникновение)?

См. комментарий к вопросу 1 первой группы вопросов.

3. Можем ли мы рассматривать предлагаемые положения о «Создании и использовании цифровой информации для введения пользователя в заблуждение» как форму подлога, связанного с [Компьютером] [ИКТ]?

На данный вопрос мы можем ответить положительно с учетом предусмотренных в российском проекте положений, которыми охватывается подлог. Однако такая квалификация будет зависеть от обстоятельств совершения преступления, связанного с введением пользователя в заблуждение.

4. Как, по вашему мнению, конвенция должна регулировать правонарушения, связанные с использованием личных данных?

Криминализация соответствующих действий важна с учетом массового характера противоправных действий в отношении таких данных. Они могут являться как непосредственно объектом посягательства, так и использоваться при совершении иных преступлений, в рамках рассылки вредоносного программного обеспечения на корпоративную или личную почту, социальной инженерии для получения банковских реквизитов или введения жертвы в заблуждение. Персональные данные могут также впоследствии использоваться для совершения ряда преступных действий, в числе которых, например, «Identity-related offences». Помимо криминализации действий по незаконной обработке данных считаем также необходимым криминализацию действий по созданию, использованию и распространению информационных ресурсов, заведомо предназначенных для такой незаконной обработки данных.

5. Чем обосновано включение правонарушений, связанных с нарушением авторских прав, в сферу действия конвенции, поскольку этот вопрос также рассматривается в других международных договорах?

Включение тех или иных противоправных деяний в содержание конвенции должно быть обусловлено их общественной опасностью. Применение ИКТ при их совершении обуславливает их массовый характер, частоту совершения и скорость, а также анонимность злоумышленников и доступ к широкому кругу объектов посягательства и информации. Тем самым, соответствующий общепринятый международный документ будет являться по сути ответом на те вызовы и угрозы, которые противопоставляются правам и законным интересам граждан преступниками при совершении криминализованных конвенцией деяний.

i. **Третья группа[3] вопросов:**

3 ***Третья группа: вопросы, касающиеся следующих предлагаемых положений:***
Сексуальное насилие над детьми в Интернете; сексуальное вымогательство; Распространение интимных изображений без согласия («порно-месть»); Правонарушения, связанные с порнографией; Побуждение или принуждение к самоубийству; Вовлечение несовершеннолетних в совершение противоправных действий; Отправка оскорбительных сообщений через службу связи; угрозы и шантаж; нарушение неприкосновенности частной жизни.

1. Как можно определить преступления, связанные с сексуальным насилием над детьми в Интернете, чтобы обеспечить детям наибольшую защиту от вреда? Что следует учитывать при выборе терминологии?

Данный вопрос заслуживает особого внимания. Интересны мнения и предложения других государств по этой теме.

Общая формулировка криминализации преступлений, связанных с изготовлением и оборотом материалов или предметов с порнографическими изображениями несовершеннолетних, совершенных с использованием ИКТ, возможно, позволит в наиболее широком виде предусмотреть на национальном уровне соответствующий формат ответственности за деяния данной категории.

2. Следует ли ввести уголовную ответственность за доступ или просмотр материалов о сексуальном насилии над детьми; если да, следует ли поставить условие для обязательности криминализации этих деяний, например, «в соответствии с его правовыми принципами» или «без ущерба для его внутреннего законодательства»?

Вопрос о введения уголовной ответственности за такой вид преступления должен быть проработан на внутригосударственном уровне.

В случае введения положений о криминализации таких действий следует рассмотреть вопрос о возможности для государств сделать оговорку к таким положениям.

3. Каким может быть обосновано (отсутствие гармонизации, новые формы сексуального насилия в сети, возникающие благодаря новым технологическим средствам, недостаточность существующих международных инструментов…) включение предлагаемых положений о: «сексуальном вымогательстве, несогласованном распространении интимных изображения и другие правонарушения, связанные с порнографией»?

Данный вопрос заслуживает внимание и требует проработки на внутригосударственном уровне

4. Будет ли в целом достигнуто соглашение о возрастном пределе для определения ребенка в возрасте до 18 лет для целей статей (это будет соответствовать конвенции о правах ребенка)?

Возражений нет. Полагаем, что применение положений конвенции о правах ребенка при формулировании проектируемых норм приемлемо.

5. Чем обосновано включение предложенных положений о: склонении или принуждении к самоубийству и вовлечении несовершеннолетних в совершение противоправных действий?

В сети Интернет распространяются различные игры, финал которых приводит или может привести к совершению суицидальных действий, а злоумышленники зарабатывают на их продаже. Распространяются также другие приложения и различные материалы суицидальной направленности, содержащие информацию о способах самоубийства, причинении себе вреда. Кроме того, стоит учесть, что использование ИКТ в таких случаях не только облегчает возможность совершения преступления (в части анонимности, скорости, массовости и т.д.), но и создает необходимые условия для массового воздействия на сознание целых групп детей в различных частях света.

6. Чем обосновано включение предлагаемых положений о: «отправке оскорбительных сообщений через средства связи; угрозы и шантаж; нарушение неприкосновенности частной жизни»?

Хотелось бы выслушать мнение других государств, предлагающих включение в проект конвенции таких положений, в российском проекте, соавторами которого стали Китай и ряд других государств, подобных положений нет.

i. Четвертая группа[4] вопросов:

1. Какое обоснование для включения следующих предлагаемых положений:

- Правонарушения, связанные с дискриминацией, расизмом или ксенофобией;

---

4 ***Четвертая группа: вопросы, касающиеся следующих предлагаемых положений:***

Подстрекательство к подрывной или вооруженной деятельности; преступления, связанные с терроризмом; преступления экстремистской направленности; Правонарушения, связанные с дискриминацией, расизмом или ксенофобией; Правонарушения, связанные с распространением наркотических средств и психотропных веществ; преступления, связанные с незаконным оборотом оружия; Реабилитация нацизма, оправдание геноцида или преступлений против мира и человечности; Незаконное распространение поддельных лекарственных средств и изделий медицинского назначения; Использование информационных и коммуникационных технологий для совершения деяний, признанных преступлениями по международному праву.

- Правонарушения, связанные с распространением наркотических средств и психотропных веществ, незаконным оборотом оружия, Незаконным распространением контрафактных лекарственных средств и изделий медицинского назначения; производство оружия, торговля людьми, преступное сообщество?

Использование ИКТ облегчает возможность совершения преступления (в части анонимности, создания теневых площадок для торговли, транснациональных каналов связи, легализации преступных доходов в т.ч. с применением криптовалют и т.д.), а также создает необходимые условия для трансграничного и массового характера посягательств, позволяя создавать широкие сети преступных организаций при полной «отстраненности» конкретных организаторов таких преступлений. При этом в настоящее время по сути почти все деяния в рассматриваемых сферах совершаются с применением средств ИКТ.

Включение таких положений объясняется опасностью таких деяний, а также охватом широких масс людей, как в качестве правонарушителей, так и жертв таких посягательств.

В частности, осуществляется продажа через социальные сети и отдельные сайты поддельных медицинских препаратов. В период пандемии злоумышленники, умело встроившись в новостную повестку, вовсю эксплуатировали тему вакцины от COVID-19.

КТОП и протоколы к ней, общепринятые антинаркотические конвенции и иные международные договоры не предусматривают компонент использования ИКТ для совершения данных преступлений. Принимая во внимание повышенную общественную опасность таких деяний, по нашему мнению, требуется отдельно криминализовать использование ИКТ для их совершения.

Видимое дублирование в данном случае не должно быть основанием для оставления таких видов преступлений без внимания в рассматриваемой конвенции, так как, наоборот, даст дополнительное основание для сотрудничества государств в целях их эффективного расследования.

2. Чем обосновано включение положения о преступлениях, связанных с терроризмом, и преступлениях, связанных с экстремизмом?

Сеть Интернет продолжает оставаться для лидеров радикальных структур инструментом вербовки новых членов, средством коммуникации и организации экстремистских (террористических) акций, разжигания межнациональной вражды, распространения расистских и ксенофобских идей.
Сохраняется тенденция распространения посредством электронных почтовых сервисов и IP-телефонии заведомо ложных сообщений об актах терроризма в административных зданиях органов власти, образовательных учреждениях, торговых центрах, объектах транспортной инфраструктуры. Это делается в целях дестабилизации деятельности органов власти и правоохранительных органов, нагнетания напряженности в обществе.
Посредством сети Интернет осуществляется вовлечение в деятельность экстремистского и террористического толка, путем вербовки в террористические группировки, выкладывание подробных инструкций по подготовке террористических актов. Представители экстремистско-террористической

идеологии, опираясь на недостаточную образованность людей, используют специальные приемы воздействия: искажают первоисточники духовных учений и исторические факты, подменяют личностные смыслы с обещанием с помощью борьбы восстановить социальную справедливость, обещают особое положение для присягнувших, а погибшим – особый почет в потустороннем мире.
В информационном пространстве встречаются как видеообращения лидеров террористического бандподполья, так и постановочные видеоролики, а также псевдо-новостные сюжеты. Контент используется как для демонстрации силы, запугивания и информационно-психологических атак на общество, так и для пропаганды экстремистских идей, приискания новых сторонников (видеоматериалы, отсылающие к боевым действиям, идеологический (обучающий) контент с религиозно-экстремистским уклоном материалы, не связанные с пропагандой терроризма напрямую, однако создающие позитивный образ террористической организации и ее деятельности).
Подобный контент размещается пользователями социальных сетей на персональных страницах вместе с другой «бытовой» информацией.
Использование Интернета террористами – это транснациональная проблема, для решения которой требуются согласованные ответные меры трансграничного характера, невзирая на некоторые различия правовых систем отдельных государств.

3. Чем обосновано включение положения о подстрекательстве к подрывной или вооруженной деятельности?

Осуществление соответствующих действий по агитации к изменению государственного строя и т.д. посредством использования ИКТ способно привлечь к противоправной деятельности большие массы людей, что создает угрозу общественной и национальной безопасности.

4. Чем обосновано включение положения о реабилитации нацизма, оправдании геноцида или преступлений против мира и человечности?

Посредством использования ИКТ распространяется среди широкого круга людей подобная идеология, пропаганда нацизма, навязывается недостоверная информация, связанная с пересмотром истории, что влечет, помимо прочего, возрождение идеологий, основанных на расовой, религиозной и других видах нетерпимости.

5. Должна ли конвенция содержать положение о криминализации использования ИКТ для совершения всех действий, признанных преступлениями в соответствии с международным правом?

Полагаем, что таким образом может быть достигнут наибольший охват преступлений, совершенных с использованием ИКТ, что будет способствовать эффективности взаимодействия при оказании взаимной правовой помощи между государствами в части сбора доказательств, а также механизмов возврата преступных активов.

Пятая группа[5] вопросов:

1. Поддержат ли государства-члены включение положений об уголовной ответственности за воспрепятствование правосудию и отмывание доходов от преступлений, охватываемых конвенцией?

Включение положений об отмывании доходов от преступлений можно рассматривать в положительном ключе.

Вопрос о необходимости включения в данную конвенцию положений о воспрепятствовании правосудию подлежит дополнительному обсуждению

2. Как, по вашему мнению, конвенция должна регулировать участие, покушение, пособничество и подстрекательство к совершению преступления?

В российском проекте Конвенции, соавторами которого стали Китай и ряд других государств, (статья 28) детально изложены положения о регулировании указанных действий:

- государства-участники принимают меры в соответствии со своим внутренним законодательством, которые признают в качестве преступления приготовление и покушение на деяние, криминализированное в соответствии с конвенцией;

- государства-участники рассматривают возможность принятия мер, чтобы признать в качестве преступления изготовления или приспособления лицом орудий и иных средств совершения преступления, вербовки соучастников преступления, сговора на совершение преступления либо иного умышленного создания условий для совершения преступления, предусмотренного конвенцией, если при этом преступление не было доведено до конца по не зависящим от этого лица обстоятельствам.

- государства-участники принимают меры в соответствии со своим внутренним законодательством для установления ответственности, наряду с непосредственными исполнителями какого-либо преступления, признанного таковым в соответствии с настоящей Конвенцией, в отношении участвующих в его совершении организатора, подстрекателя или пособника, а также

---

*5 **Пятая группа: вопросы, касающиеся следующих предлагаемых положений:***

Отмывание денег; воспрепятствование правосудию; Неспособность защитить данные; Другие противоправные действия; Ответственность юридических лиц; Пособничество, подстрекательство, попытка; санкции и другие меры

усиления ответственности за групповые преступления, включая организованные группы и преступные сообщества.

3. Должна ли уголовная ответственность распространяться не только на физических лиц, но и на юридических лиц?

4. Может ли конвенция следовать формулировке ответственности юридических лиц, содержащейся в статье 10 КТОП? Будет ли необходимость в отдельном правонарушении, наказывающем халатность юридических лиц в поддержании требуемых мер безопасности?

(Ответ на вопросы 3-4) Да. Конвенцию должна быть включена норма, предусматривающая установление ответственности для юридических лиц, которая может быть уголовной, административной или гражданско-правовой в зависимости от правовых принципов государств. Использование статьи 10 КТОП позволит достигнуть консенсуса между государствами.

5. Считаете ли вы, что конвенция должна включать положение об отягчающих обстоятельствах? Если да, то должно ли это быть общее положение об отягчающих обстоятельствах или отдельные статьи должны включать квалифицирующий элемент отягчающих обстоятельств? А смягчающие обстоятельства?

Полагаем, что способ использования ИКТ для совершения преступлений, включенный в другие международные договоры по борьбе с преступностью, мог бы являться отягчающим обстоятельством. В разрабатываемой конвенции в этом нет никакого смысла, поскольку вся конвенция будет посвящена именно этому вопросу.

Интересно услышать аргументацию тех государств, которые предлагают ввести положение об отягчающихся обстоятельствах.

6. Что касается «других незаконных действий» может п. 3 ст. 34 конвенции КПТОП («государства-участники могут принимать более суровые меры, чем те, которые предусмотрены в настоящей конвенции») охватить все эти преступления?

Не совсем понятна суть вопроса.

Мы исходим из того, что будущей конвенцией будут охвачены как киберзависимые так и традиционные преступления, совершенные с использованием ИКТ в отношении которых будет установлено обязательство по принятию соответствующих мер.

В тоже время в отношении тех противоправных деяний, которые не войдут в конвенцию, государства сами должны установить какие меры (возможно более суровые) необходимо принять в отношении этих деяний.