СЕРИЯ УНИВЕРСИТЕТСКИХ МОДУЛЕЙ

Киберпреступность 3

ПРАВОВАЯ БАЗА И ПРАВА ЧЕЛОВЕКА

UNODC

Дохинская декларация:
ПООЩРЕНИЕ КУЛЬТУРЫ
СОБЛЮДЕНИЯ ЗАКОННОСТИ

образование для правосудия

Управление Организации Объединенных Наций по наркотикам и преступности

ОБРАЗОВАНИЕ ВО ИМЯ ПРАВОСУДИЯ
СЕРИЯ УНИВЕРСИТЕТСКИХ МОДУЛЕЙ

КИБЕРПРЕСТУПНОСТЬ

Модуль 3

ПРАВОВАЯ БАЗА И ПРАВА ЧЕЛОВЕКА

Организация Объединенных Наций
Вéна, 2019

Этот модуль является ресурсом для преподавателей.

Этот модуль, разработанный в рамках инициативы «Образование для Правосудия»(E4J), являющейся компонентом Глобальной программы по осуществлению Дохинской декларации, Управления Организации Объединенных Наций по наркотикам и преступности (УНП ООН) и является частью серии учебных модулей «Образование для правосудия» (E4J) по Киберпреступности и сопровождается учебным пособием. Полный спектр материалов «Образование для правосудия» E4J включает в себя университетские модули по вопросам честности и этики, предупреждения преступности и уголовного правосудия, борьбы с коррупцией, организованной преступности, торговли людьми / незаконного ввоза мигрантов, огнестрельного оружия, охраны дикой природы, лесных и рыболовных преступлений, борьбы с терроризмом, а также киберпреступность.

Все модули в серии модулей университета «Образование для правосудия» E4J содержат предложения для выполнения в классе упражнений, оценки учащихся, слайды и другие учебные пособия, которые преподаватели могут адаптировать к своему контексту и интегрировать в существующую учебную программу. Модуль предоставляет план для трехчасового занятия, но может использоваться для более коротких или более длительных занятий.

Все университетские модули «Образование для правосудия» E4J участвуют в действующих научных исследованиях и дебатах и могут содержать информацию, мнения и заявления из различных источников, включая сообщения прессы и независимых экспертов. Ссылки на внешние ресурсы были проверены на момент публикации. Однако, поскольку сторонние веб-сайты могут измениться, пожалуйста *contact us*, если вы столкнулись с неработающей ссылкой или перенаправлены на неприемлемый контент. Также сообщите нам, если вы заметили, что публикация связана с неофициальной версией или веб-сайтом.

Несмотря на то, что были приложены все усилия для обеспечения точного перевода модуля, обратите внимание, что модуль на английском языке является утвержденной версией. Поэтому в случае сомнений, пожалуйста, обратитесь к первоисточнику в английской версии.

Ознакомиться с условиями использования Модуля можно на *веб-сайте E4J*.

Оглавле́ние

Введение

Национальные, региональные и международные законы могут регламентировать поведение в киберпространстве и регулировать вопросы уголовного правосудия, относящиеся к киберпреступлениям. В этих законах изложены не только правила и ожидания в отношении поведения, но и процедуры, которым необходимо следовать в случае нарушения таких правил и несоответствия ожиданиям. Однако различия положений национального законодательства разных стран, касающихся основных видов киберпреступлений, затрудняют международное сотрудничество в сфере уголовного судопроизводства (эта проблема подробно рассматривается в модуле 7 серии модулей по киберпреступности: «Международное сотрудничество в борьбе с киберпреступностью», а также в серии университетских модулей по организованной преступности, в частности в модуле 11: «Международное сотрудничество в области борьбы с транснациональной организованной преступностью»).

В данном модуле основное внимание уделяется описанию правовой картины киберпреступности, подчеркивается необходимость унификации законодательства и рассматривается взаимосвязь между законами в области киберпреступности и правами человека. Как показано в данном модуле, законы по борьбе с киберпреступностью должны соответствовать нормам права в области прав человека, и любое ограничение прав человека должно соответствовать стандартам и принципам защиты прав человека.

Результаты обучения

- Определить, обсудить и изучить потребность в законах в области киберпреступности и их роль
- Дать определение материальному, процессуальному и превентивному законодательству в области борьбы с киберпреступностью и описать различие между ними
- Определить и критически оценить национальные, региональные и международные законы в области киберпреступности
- Критически оценить защиту прав человека в сети Интернет

Основные вопросы

Борьба с киберпреступностью может осуществляться (и осуществляется) путем применения действующих законов, которые охватывают правонарушения, совершаемые вне сети Интернет; внесения поправок в законы для включения положений, касающихся киберпреступлений; и принятия законов, конкретно нацеленных на борьбу с киберпреступностью. Однако действующие законы могут оказаться неприменимыми к киберпреступлениям, поскольку они могли быть приняты до появления Интернета и цифровых технологий и/или могли разрабатываться без учета Интернета и цифровых технологий. Поэтому законы, которые созданы для борьбы с преступлениями, не относящимися к киберпреступности, могут иметь ограниченные последствия для киберпреступников и прочих правонарушителей, действия которых сопряжены с информационно-коммуникационными технологиями (ИКТ) в качестве предмета, либо средства совершения преступления. В связи с этим может возникнуть необходимость в принятии специальных законов, касающихся киберпреступности. Вопрос необходимости принятия законов в области киберпреступности «зависит от характера отдельных деяний, а также от охвата и интерпретации национального законодательства» (УНП ООН, 2013, стр.52).

Рассмотрим случай 2013 года, связанный с сексуальным надругательством с использованием изображений (именуемое в разговорной речи как «порноместь»), которое является одной из форм домогательства в киберпространстве, предполагающего «создание, распространение и угрозу распространения изображений интимного или сексуального характера без соответствующего на то обоюдного согласия» (Henry, Flynn and Powell, 2018, p. 566), чтобы «расстроить, унизить жертву и/или причинить ей вред иного характера» (Maras, 2016, p. 255), когда лицо, совершившее такое надругательство, не могло быть привлечено к уголовной ответственности на основании действующих законов Нью-Йорка (для получения дополнительной информации о сексуальном надругательстве с использованием изображений см. модуль 12 серии модулей по киберпреступности: «Киберпреступления против личности»). В частности, преступник выложил фотографии своей подруги (бывшей таковой на момент инцидента) в обнаженном виде в «Twitter» и отправил эти фотографии по электронной почте сестре и работодателю своей подруги (*People v. Barber*, 2014). Ему были предъявлены обвинения, среди которых было обвинение в домогательстве при отягчающих обстоятельствах во второй степени. Согласно статье 240.30(1)(a) Уголовного закона штата Нью-Йорк, «лицо признается виновным в домогательстве при отягчающих обстоятельствах во второй степени, когда, с целью домогательства, причинения беспокойства, угрозы или запугивания другого лица, оно…связывается с лицом, анонимно или иным способом, по телефону, телеграфу или по электронной почте, либо путем передачи или доставки

письменного сообщения любой иной формы таким способом, который может причинить беспокойство или испуг». Поскольку этот закон распространяется на прямые коммуникации между потерпевшим и правонарушителем (*People v Smith*, 1977, 791), суд, рассматривавший дело *People v. Barber* (2014), постановил, что деяние подсудимого (т.е. отправление фотографий подруги в обнаженном виде по электронной почте сестре и работодателю потерпевшей и размещение этих фотографий в «Twitter») не являются домогательством при отягчающих обстоятельствах. Такой пример ограниченного распространения закона на Интернет-пространство является далеко не единственным. Как отмечалось в проекте доклада УНП ООН «Всестороннее исследование проблемы киберпреступности» в 2013 году, «многие традиционные законы общего права не учитывают особенности информации и информационных технологий, которые применяются для совершения киберпреступлений и преступлений, при совершении которых образуются электронные доказательства» (стр. 57).

Роль законодательства о киберпреступности

Законодательство о киберпреступности определяет стандарты приемлемого поведения для пользователей информационно-коммуникационных технологий (ИКТ); устанавливает социально-правовые санкции за кибепреступления; защищает пользователей ИКТ в целом и смягчает и/или предотвращает вред, причиняемый людям, данным, системам, сервисам и инфраструктуре в частности; защищает права человека; обеспечивает возможность для проведения расследований и осуществления уголовного преследования в отношении преступлений, совершаемых в сети Интернет (вне пределов реального мира); и содействует сотрудничеству между странами по делам, связанным с киберпреступлениями (УНП ООН, 2013, стр. 57). Законодательство в области киберпреступности предусматривает правила и стандарты поведения при использовании Интернета, компьютеров и связанных с ними цифровых технологий и действия публичных, государственных и частных организаций; нормы доказательственного права, правила осуществления уголовного судопроизводства и прочие вопросы уголовного права, связанные с киберпространством; положения о снижении риска и/или смягчении вреда, причиненного физическим лицам, организациям и инфраструктуре в случае совершения кибепреступления. Таким образом, законодательство в области киберпреступности включает в себя материальное, процессуальное и превентивное право.

Материальное право

Незаконное деяние должно быть четко прописано в законе и запрещено законом. В соответствии с моральным принципом *«nullum crimen sine lege»* (лат. «нет преступления без предусматривающего его закона»), лицо не может быть подвергнуто наказанию за деяние, которое не было прописано в законе на момент совершения лицом этого деяния (УНП ООН, 2013, стр. 59). *Материальное право* определяет права и обязанности субъектов права, к которым относятся физические лица, организации и государства. Источниками материального права являются нормативно-правовые акты и распоряжения, принимаемые местными и центральными законодательными органами (*статутное право*), федеральные конституции и конституции федеральных единиц, а также судебные решения (в системах общего права).

> *Знаете ли вы?*
>
> Некоторые страны, вместо разработки новых специальных законов по борьбе с киберпреступностью, внесли поправки в свои национальные законодательства или кодексы, дополнив их отдельными положениями, касающимися киберпреступлений. Эта практика имела любопытные, заслуживающие внимания последствия, которые заключались в том, что некоторые страны решили отдельно криминализировать деяние, связанное с незаконным использованием информационно-коммуникационных технологий для совершения какого-либо преступления. Таким образом, если бы преступник использовал незаконный доступ для совершения подлога или мошенничества, такое деяние образовало бы одновременно два преступления.

Материальное законодательство в области киберпреступности включает в себя законы, которые запрещают конкретные виды киберпреступлений (они описаны в модуле 2 серии модулей по киберпреступности: «Основные виды киберпреступности»), и предусматривает наказание за несоблюдение этих законов. К киберпреступлениям относятся традиционные преступления в реальном мире (вне сети Интернет) (например, мошенничество, подлог, организованная преступность, отмывание денег и кража), совершаемые в киберпространстве, которые являются «гибридными» преступлениями или «преступлениями с использованием киберсетей», а также «новыми» или «киберзависимыми» преступлениями, которые стали возможными с изобретением Интернета и цифровых технологий, функционирующих через Интернет (Wall, 2007; Maras 2014; Maras, 2016). Поэтому многие страны разработали законы, которые конкретно предназначены для противодействия киберпреступности. Например, Германия, Япония

и Китай внесли поправки в соответствующие положения своих уголовных кодексов с целью борьбы с киберпреступлениями. Некоторые страны также использовали действующие законы, которые были разработаны для борьбы с преступностью в реальном мире (вне сети Интернет), чтобы охватить определенные виды киберпреступности и киберпреступников. В качестве еще одного примера можно привести Ирак, где действующие гражданский кодекс (Гражданский кодекс Ирака №.40 от 1951 года) и уголовный кодекс (Уголовный кодекс Ирака №.111 от 1969 года) используются для судебного преследования за преступления, совершаемые в реальном мире (например, мошенничество, шантаж, хищение персональных данных) с использованием Интернет и цифровых технологий.

Правовые системы

Каждое государство имеет свою собственную правовую систему, которая влияет на создание материального уголовного права в области киберпреступности. Эти системы включают в себя (Maras, forthcoming, 2020) (готовится к публикации):

1) *Общее право*. Страны с системой общего права создают законы на основе *судебных прецедентов* (т.е. решение, вынесенное по делу, является обязательным для суда и нижестоящих судов) и устоявшейся практики. Эти законы существуют в виде отдельных законов и *прецедентного права* (т.е. права, которое формируется на основе решений судов или судебных прецедентов).

2) *Гражданское право.* Страны с такой системой права имеют кодифицированные, консолидированные и всеобъемлющие правовые нормы и законоположения, которые устанавливают границы основных прав, обязательств, обязанностей и ожиданий в отношении поведения. Эти системы основаны преимущественно на законодательстве и конституциях.

3) *Обычное право*. Эти правовые системы включают в себя укоренившиеся и общепринятые модели поведения в рамках культуры, которые воспринимаются носителями этой культуры в качестве закона (*opinio juris – убежденность в правомерности)*. В международном праве обычное право регулирует взаимоотношения и практику между государствами и считается обязательным для всех государств.

4) *Религиозное право.* В системах религиозного права в качестве источника права используются правила, основанные на религиозных учениях или религиозной литературе.

5) *Правовой плюрализм*. В правовой системе такого типа возможно сосуществование двух или более вышеупомянутых правовых систем (т.е. общего, гражданского, обычного или религиозного права).

Материальное право сосредоточено на *существе* преступления, например, элементах состава преступления, которые включают в себя запрещенное деяние (*actus reus* – «виновное действие») и субъективную сторону (*mens rea* – «преступный умысел»). Разные страны могут отдавать предпочтение криминализации различных деяний на основе разных элементов, образующих состав преступления. В качестве альтернативы страны могут криминализовать те же самые деяния, однако законы могут различаться с точки зрения того, какая «субъективная сторона» делает лиц виновными за такое деяние (т.е. с точки зрения степени уголовно-правовой вины). В этой связи законы, которые криминализируют, например, несанкционированный доступ к компьютерным системам и данным, отличаются в разных странах в зависимости от степени намерения предполагаемого преступника (см. «Уровни уголовно-правовой вины» во вставке ниже).

Уровни (формы) уголовно-правовой вины

Существуют разные уровни уголовно-правовой вины (или уголовной ответственности) в зависимости от степени, в которой незаконное действие было преднамеренным (совершенным сознательно или умышленно) или непреднамеренным (совершенным по опрометчивости или по неосторожности), которая в разных правовых системах толкуется по-разному (Simons, 2003; Dubber, 2011; Maras, 2020):

- *Сознательно*. Лицо *сознательно* совершает преступление, когда оно действует с целью причинения вреда (т.е. лицо имеет *намерение* причинить вред). В качестве примера можно привести Закон Соединенного Королевства о неправомерном использовании компьютерных технологий 1990 года, который криминализирует, в числе прочего, несанкционированный доступ к системам и данным с намерением вызвать изменения и/или повреждения, нарушения нормальной работы систем и сервисов и модификации системных данных и программ.

- *Умышленно*. Лицо *умышленно* совершает преступление, когда ему известно о том, что его действие причинит вред, но оно, тем не менее, совершает такое действие и причиняет вред. В соответствии с Законом о компьютерном мошенничестве и злоупотреблении 1986 года, в частности, параграфом 1030(a)(1) раздела 18 Свода законов США, лицу могут быть предъявлены обвинения, если оно:

  сознательно проникнув в компьютер без необходимых на то санкций или преступив границы санкционированного доступа и посредством данного действия получив информацию, которая была определена Правительством Соединенных Штатов согласно указу или акту исполнительной власти как требующая защиты от несанкционированного раскрытия из соображений национальной обороны или международных отношений, либо получив какую-либо закрытую информацию, как это определено в параграфе «y» статьи 11 Закона об атомной энергии от 1954 года, при наличии основания полагать, что полученная таким образом информация может использоваться с целью причинения вреда Соединённым Штатам или в пользу какого-либо иностранного государства, умышленно сообщает, направляет, передает либо принимает меры для сообщения, направления или передачи, либо пытается сообщить, направить, передать или принять меры для сообщения, направления или передачи такой информации любому лицу, которое не имеет права получать ее, либо умышленно сохраняет эту информацию и не передает ее должностному лицу или служащему Соединенных Штатов, которое имеет право на ее получение.

- *По опрометчивости (или легкомыслию)*. Лицо совершает преступление *по опрометчивости,* когда оно совершает акт, даже несмотря на то, что оно осознает существенный и неоправданный риск причинения вреда другим лицам, однако демонстрирует пренебрежение или безразличие к такому риску причинения вреда. В Австралии лицу могут быть предъявлены обвинения на основании положений раздела 477.2(1)(c) Закона о киберпреступности 2001 г. (№.161, 2001), если «лицо опрометчиво не осознает того, что [несанкционированное] изменение [данных] нарушает или нарушит: (i) доступ к этим или любым другим данным, хранящимся в любом компьютере; либо (ii) достоверность, безопасность или применимость любых таких данных».

- *По неосторожности*. *Неосторожность* представляет собой самую низкую степень виновности. Лица, совершающие какие-либо действия по неосторожности, не осознают негативных последствий своего поведения. В Сенегале «любое лицо, которое, даже по неосторожности, обрабатывает или организует обработку персональных данных без соблюдения формальных требований, изложенных в Законе о персональных данных, до использования таких данных, подлежит наказанию» (статья 431-17, Закон №.2008-11 о киберпреступности).

Примечание: уровни (формы) уголовно-правовой вины не являются универсальными (Fletcher, 2000, p. 445-446, cited in Ohlin, 2013 p. 82).

Здесь важно отметить два момента. Во-первых, местное применение закона (уголовное преследование) возможно лишь в том случае, когда уголовное преследование отвечает интересам общества, при этом большое количество массовых киберпреступлений, таких как мошенничество через Интернет, относятся к малозначительным в соответствии с принципом *de minimis non-curat lex* (лат. закон не заботится о мелочах), в том смысле, что по отдельности они считаются слишком незначительными по своим последствиям, чтобы оправдать расследование полицией или уголовное преследование. Тем не менее, они могут повлечь за собой значительные совокупные последствия в международном масштабе, поэтому они должны подпадать под действие международного права. Во-вторых, «при отсутствии надежного обоснования криминализации определенных деяний возникает риск чрезмерной криминализации. В этом плане международное право в области прав человека является одним из важных инструментов, необходимых для оценки уголовного права в соответствии с внешними, международными стандартами» (УНП ООН, 2013, стр. 60) (см. раздел «Международное право в области прав человека и законодательство о киберпреступности» в настоящем модуле).

Процессуальное право

Процессуальное право определяет границы процессов и процедур, которые необходимо соблюдать при применении норм материального права, а также правила, обеспечивающие возможность для применения материального права. Важной частью процессуального законодательства является *уголовно-процессуальное право*, которое включает в себя исчерпывающие правила и руководящие принципы в отношении того, как должны обращаться с подозреваемыми, обвиняемыми и осужденными лицами система уголовного правосудия и ее сотрудники (Maras, forthcoming, 2020 (готовится к публикации); для получения общей информации об уголовно-процессуальном праве см. LaFave et al., 2015; для получения информации о международном уголовно-

процессуальном праве см. Boas, et al., 2011). Наконец, процессуальное законодательство в области киберпреступности включает в себя положения о юрисдикции и следственных полномочиях, нормы доказательственного права и правила осуществления уголовного судопроизводства, которые относятся к процедурам сбора данных, перехвата сообщений, обыска и выемки, сохранения и хранения данных (которые более подробно рассматриваются в модуле 4: «Введение в цифровую криминалистику», модуле 5: «Расследование киберпреступлений», модуле 6: «Практические аспекты расследования киберпреступлений и цифровой криминалистики» и модуле 10: «Конфиденциальность и защита данных»; см. также УНП ООН, 2013, стр. xxii-xxiii). Киберпреступность создает некоторые уникальные сложности, касающиеся процедур, особенно тех, которые связаны с юрисдикцией, расследованиями и цифровыми доказательствами.

Юрисдикция. Правоохранительные органы вправе осуществлять расследование киберпреступлений, а национальные суды вправе выносить решения по делам о киберпреступлениях только в тех случаях, если заинтересованное государство обладает соответствующей юрисдикцией. Под юрисдикцией понимается право и полномочия государства применять законы и назначать наказание за несоблюдение законов (эта тема подробно рассматривается в модуле 7 серии модулей по киберпреступности: «Международное сотрудничество в борьбе с киберпреступностью»). Вопрос юрисдикции тесно связан с государственным суверенитетом, т.е. с правом государства осуществлять полномочия на своей собственной территории (УНП ООН, 2013, стр. 61). Юрисдикция обычно связана с географической территорией или *locus commissi deliciti* (место совершения преступления), когда государство заявляет о своей юрисдикции в отношении преступлений, совершенных на его территории и осуществляет преследование виновных в их совершении (*принцип территориальности*). Учитывая отсутствие географических границ и территорий в киберпространстве, местоположение не может использоваться для определения юрисдикции. Поэтому государства используют целый ряд иных факторов, чтобы определить юрисдикцию (Brenner and Koops, 2004; Rahman 2012; Maras, forthcoming, 2020) (готовится к публикации). Одним из таких факторов является гражданство правонарушителя (*принцип государственной принадлежности; принцип активной правосубъектности*). Этот принцип признает право государств осуществлять преследование своих граждан, даже если эти граждане находятся за пределами их территории. В меньшей степени (с точки зрения применимости) для установления юрисдикции в отношении преступления может использоваться гражданство потерпевшего (*принцип государственной принадлежности; принцип пассивной правосубъектности*). Государство может также устанавливать юрисдикцию в том случае, когда преступление, совершенное в другом государстве (например, государственная измена или шпионаж), нанесло ущерб интересам и безопасности государства, добивающегося осуществления юрисдикции в отношении этого преступления (*принцип защиты*). Наконец, любое государство может установить юрисдикцию в отношении определенных транснациональных преступлений,

таких как массовые злодеяния (например, геноцид), которые рассматриваются как преступления, затрагивающие всех людей, независимо от географического местоположения, когда государство, на территории которого было совершено преступление, не желает или не в состоянии осуществлять преследование виновных лиц (*принцип универсальности*).

Следственные действия и полномочия. Цифровые доказательства киберпреступлений сопряжены с особыми трудностями – как в плане обращения с ними, так и с точки зрения их использования в судебном производстве (см. модуль 5 серии модулей по киберпреступности: «Расследование киберпреступлений» и модуль 6 серии модулей по киберпреступности: «Практические аспекты расследования киберпреступлений и цифровой криминалистики»). Как отмечалось в проекте доклада УНП ООН «Всестороннее исследование проблемы киберпреступности» в 2013 году, «[в] то время как некоторые такие следственные действия могут быть осуществлены на основании традиционных полномочий, многие процессуальные положения, в основе которых лежит пространственный, объектно-ориентированный подход, трудно применять в ситуациях, связанных с хранением [цифровых] данных и потоками данных в режиме реального времени» (стр. 137), поэтому для проведения расследования необходимы специальные полномочия (УНП ООН, 2013, стр. 60). Такие специальные полномочия предусматриваются законом и не только распространяются на доступ к необходимой информации, но и включают в себя гарантии для обеспечения того, чтобы данные были получены в соответствии с надлежащими законными распоряжениями и были доступны только в той степени, в которой это необходимо и разрешено законом (эта тема дополнительно рассматривается в модуле 5 серии модулей по киберпреступности: «Расследование киберпреступлений»). Закон США о сохраненных сообщениях (титул 18 Свода законов США, § 2701-2712), представляющий собой титул II Закона о конфиденциальности электронных сообщений 1986 года, предусматривает такие гарантии. Например, согласно параграфу 2703(a) титула 18 Свода законов США:

> государственное учреждение вправе требовать от провайдера услуг электронных коммуникаций раскрытия содержания проводных или электронных сообщений, хранящихся в электронном хранилище системы электронных коммуникаций в течение не более ста восьмидесяти дней, только на основании ордера, выданного в соответствии с процедурами, описанными в Федеральных правилах уголовного производства (или, в случае суда штата, выданного в соответствии с порядком выдачи судебных ордеров, действующим в этом штате), судом компетентной юрисдикции.

Однако эти гарантии (т.е. требование о наличии законного распоряжения) требуются не во всех странах. В 2014 году Турция внесла поправки в Закон об Интернете №.5651, чтобы требовать от интернет-провайдеров сохранения данных пользователей и предоставлять

их властям по первому требованию без необходимости получения законного распоряжения (например, решения суда или ордера на обыск) для получения этих данных. Такие следственные полномочия выходят за рамки обычного сбора доказательств и предполагают получение содействия и взаимодействие с другими представителями системы уголовного правосудия по делам, связанным с киберпреступностью. Такая же ситуация сложилась в Танзании, где Закон о киберпреступности 2015 года наделил полицию чрезмерными, неограниченными следственными полномочиями в отношении киберпреступлений. В частности, санкция полиции является единственным требованием для производства обыска и выемки доказательств и принуждения к раскрытию данных. Соответственно, обыск и выемка, а также прочие следственные действия могут производиться без наличия надлежащих законных распоряжений. Кроме того, существует опасность «размывания (отклонения от основного) мандата» или «размывания функций» (эти термины используются для описания случаев распространения законов и/или иных мер на области, находящиеся за пределами их первоначальной сферы действия), когда законы и следственные полномочия, изначально направленные на один вид киберпреступности, впоследствии распространяются на другие, менее тяжкие виды киберпреступлений. В конечном счете полномочия и процедуры, используемые с целью расследования киберпреступлений и судебных разбирательств, должны соответствовать принципам верховенства закона и стандартам в области прав человека (см., например, статью 15 Конвенции Совета Европы о киберпреступности 2001 года).

Идентификация, сбор, обмен, использование и допустимость цифровых доказательств. Процессуальное законодательство в области киберпреступности охватывает аспекты идентификации, сбора, хранения, анализа и обмена цифровых доказательств. К цифровым доказательствам (или электронным доказательствам) относится «информация любого типа, которую можно извлечь из компьютерных систем или иных цифровых устройств, и которая может использоваться для доказательства или опровержения факта правонарушения» (Maras, 2014). Цифровые доказательства (более подробно рассматриваются в модуле 4 серии модулей по киберпреступности: «Введение в цифровую криминалистику») могут подтвердить или опровергнуть показания потерпевшего, свидетеля и подозреваемого, подтвердить или опровергнуть правдивость утверждения о факте, определить мотив, намерение и местоположение правонарушителя, определить поведение правонарушителя (действия и поведение в прошлом) и установить степень уголовно-правовой вины (Maras 2014; Maras, 2016).

Нормы доказательственного права и правила уголовного судопроизводства включают в себя критерии, используемые для определения допустимости цифровых доказательств в суде (Maras, 2014). В них описываются процедуры документирования, сбора, сохранения, передачи, анализа, хранения и защиты цифровых доказательств с целью обеспечения их допустимости в национальных судах. Для того чтобы цифровые доказательства были

допустимыми в суде, проводится их аутентификация и устанавливается их целостность. Процедуры аутентификации включают в себя определение источника/автора цифровых доказательств (например, идентификационной информации об источнике) и проверку целостности доказательств (например, на предмет того, что они не были каким-либо образом изменены, подтасованы или повреждены). Важнейшее значение для обеспечения допустимости цифровых доказательств в большинстве судов является *система охраны доказательств*, которая включает в себя подробный учет доказательств, их состояния, процессов сбора, хранения, получения доступа и передачи, а также причин получения доступа и передачи (УНП ООН, 2013, стр. 60; Maras, 2014). В разных странах действуют разные стандарты норм доказательственного права и правил уголовного судопроизводства. Для борьбы с киберпреступностью необходимы схожие нормы доказательственного права и уголовного судопроизводства, поскольку преступления такого типа не знают границ и воздействуют на цифровые доказательства и системы в любой точке мира посредством подключения к сети Интернет.

Превентивное право

Превентивное право основано на регулировании и снижении рисков правонарушений. В контексте киберпреступности цель превентивного законодательства заключается либо в предотвращении киберпреступлений, либо, как минимум, в смягчении ущерба, причиняемого в результате совершения киберпреступлений (УНП ООН, 2013, стр. 61). Законы о защите данных (например, Общие положения о защите данных ЕС 2016 года и Конвенция Африканского союза о кибербезопасности и защите персональных данных 2014 года, рассматриваемые в модуле 10 серии модулей по киберпреступности: «Конфиденциальность и защита данных») и законы о кибербезопасности (например, Закон Украины «Об основных принципах обеспечения кибербезопасности Украины» 2017 года) приняты с целью снижения материального ущерба в результате киберпреступлений, связанных с утечкой личных данных, и/или минимизации уязвимости граждан к киберпреступлениям. Другие законы позволяют сотрудникам системы уголовного правосудия выявлять и расследовать киберпреступления и осуществлять уголовное преследование виновных путем обеспечения возможности для использования необходимых средств, мер и процедур, облегчающих осуществление таких действий (например, инфраструктуры поставщиков телекоммуникационных услуг и услуг электронной связи, которая дает им возможность перехвата сообщений и сохранения данных). В Соединенных Штатах Америки Закон о содействии правоохранительным органам в области коммуникаций (CALEA) 1994 года (кодифицирован в титуле 47 Свода законов США, параграф 1001-1010) обязывает провайдеров телефонной связи и производителей оборудования принимать меры для того, чтобы их сервисы и продукты обеспечивали органам власти, имеющим законное

разрешение (например, надлежащий судебный ордер), возможность для получения доступа к линиям связи.

> *Знаете ли вы?*
>
> База данных по киберпреступности Управления Организации Объединенных Наций по наркотикам и преступности (УНП ООН), которая является частью Портала управления знаниями SHERLOC, содержит данные о национальных законах о киберпреступности и сведения о судебной практике.

Унификация законодательства

Очевидное большинство стран мира имеют национальные законы, которые охватывают киберпреступность или некоторые аспекты киберпреступности (УНП ООН, 2015). В странах, которые не приняли законы о киберпреступности, создаются безопасные убежища для киберпреступников, поскольку лицо нельзя привлечь к ответственности за киберпреступление, если только оно не рассматривается в качестве незаконной деятельности, преследуемой по закону. Примером служит случай с создателем и распространителем компьютерного вируса «LOVE BUG», гражданином Филиппин, которого невозможно было привлечь к уголовной ответственности (даже несмотря на то, что этот вирус повлек за собой неблагоприятные экономические последствия для многих стран по всему миру), поскольку на Филиппинах отсутствовал закон о киберпреступности на момент совершения деяния (Maras, 2014). Такие безопасные убежища для киберпреступников могут также создаваться в том случае, если законы о киберпреступности не соблюдаются должным образом, и/или если существуют расхождения в законодательстве разных стран в области киберпреступности (УНП ООН, 2013, стр. 61-65).

Унификация основных положений законодательства в области киберпреступности не только позволит предотвратить создание безопасных убежищ для киберпреступников, но и исключит возможность избежания серьезного наказания за совершение киберпреступлений (УНП ООН, 2013, стр. 66-69). Эти безопасные убежища создаются потому, что лишь те действия, которые превышают «порог тяжких преступлений, – который, как правило, выражается в форме возможного наказания, которое может повлечь за собой соответствующее деяние, – оправдывают вложения, необходимые для осуществления международного сотрудничества между государствами (УНП ООН, 2013,

стр. 67). Таким образом, унификация основных положений законов о киберпреступности будет способствовать развитию международного сотрудничества.

Унификация процессуальных норм законодательства в области киберпреступности будет способствовать созданию условий для сбора доказательств в любых странах мира и обмену доказательствами в рамках международного сотрудничества (УНП ООН, 2013, стр. 66-69). Всеобъемлющие и точные процессуальные нормы и протоколы, касающиеся цифровых доказательств и судебной экспертизы (рассматриваются в серии модулей по киберпреступности – модуле 4: «Введение в цифровую криминалистику, модуле 5: «Расследование киберпреступлений» и модуле 6: «Практические аспекты расследования киберпреступлений и цифровой криминалистики»), и унификация этих норм и протоколов могли бы обеспечить, чтобы цифровые доказательства, обрабатываемые в одной стране, были допустимыми в другой стране (или других странах).

Национальные законы содержат положения, которые облегчают международное сотрудничество (рассматривается в модуле 7 серии модулей по киберпреступности: «Международное сотрудничество в борьбе с киберпреступностью»). Например, на Ямайке в 2015 году был принят Закон о борьбе с киберпреступлениями с целью унификации законодательства и выполнения многих существенных и процессуальных положений Конвенции о киберпреступности. В Нигерии Закон о (запрете, предотвращении и т.д.) киберпреступлений 2015 года призывает к созданию Консультативного совета по киберпреступности для содействия осуществлению международного сотрудничества по делам, связанным с киберпреступностью. В Катаре Закон №.14 от 2014 года о введении в действие Закона о профилактике киберпреступности предусматривает следственные полномочия, нормы доказательственного права и правила судопроизводства, международное сотрудничество, взаимную правовую помощь, экстрадицию и обязательства поставщиков услуг, связанные с киберпреступностью. Существование национальных, региональных и международных законов в области киберпреступности и унификация законодательства государств способствуют международному сотрудничеству (УНП ООН, 2013, стр. 61). Унификация и применение национальных, региональных и международных законов также способствуют ликвидации безопасных убежищ для киберпреступников (Maras, 2016).

Международные и региональные правовые документы

Существуют международные и региональные договоры в области борьбы с киберпреступностью. Одним из примеров является Конвенция Совета Европы о киберпреступности 2001 года. Цель этой конвенции заключается в унификации национальных законодательств, совершенствовании методов расследования киберпреступлений и расширении международного сотрудничества. Она также содержит рекомендации для государств-участников конвенции в отношении мер, которые необходимо принять на национальном уровне для борьбы с киберпреступностью, включая внесение поправок и дополнений в нормы материального права (например, введение ответственности за правонарушения, связанные с киберпреступностью, в уголовное законодательство) и уголовно-процессуальное право (например, определение порядка осуществления уголовного расследования и судебного преследования). Конвенция также содержит рекомендации для государств-участников в отношении взаимной помощи и служит в качестве *договора об оказании взаимной правовой помощи* (т.е. соглашения между странами о сотрудничестве в расследовании и уголовном преследовании по некоторым и/или всем правонарушениям, признанным таковыми в национальных законодательствах обеих сторон; Maras, 2016) для стран, которые не имеют подобного договора со страной, запрашивающей помощь.

> *Знаете ли вы?*
>
> В то время как ряд стран активно выступают за принятие глобальной конвенции под эгидой Организации Объединенных Наций, а Российская Федерация, в частности, в 2017 году предложила «Проект Конвенции Организации Объединенных Наций о сотрудничестве в сфере противодействия информационной преступности» (A/C.3/72/12), на сегодняшний день в международном сообществе пока еще не достигнут достаточный консенсус в отношении принятия такой глобальной конвенции в рамках Организации Объединенных Наций.

Существуют несколько договоров в сфере борьбы с киберпреступностью, имеющих региональный характер:

- Соглашение о сотрудничестве в борьбе с преступлениями в сфере компьютерной информации, подписанное странами-членами Содружества Независимых Государств в 2001 году. Это соглашение призывает государства принять

национальные законы для выполнения положений соглашения и унификации национальных законодательств в сфере борьбы с киберпреступностью.

- Конвенция Лиги арабских государств о борьбе с преступлениями в области информационных технологий, принятая Лигой арабских государств в 2010 году. Основная цель этой конвенции заключается в укреплении сотрудничества между государствами для обеспечения им возможности защиты своего имущества, населения и интересов от киберпреступности.

- Соглашение о сотрудничестве в области обеспечения международной информационной безопасности, принятое Шанхайской организацией сотрудничества в 2010 году. Действие этого соглашения выходит за пределы киберпреступности и кибербезопасности и включает в себя меры обеспечения информационной безопасности государств-участников в качестве одной из главных целей соглашения, а также меры по национальному контролю за информационными системами и их контентом.

- Проект Конвенции Африканского союза о создании юридических основ кибербезопасности в Африке (проект Конвенции Африканского союза) 2012 года. Эта конвенция способствует обеспечению и поддержанию людских, финансовых и технических ресурсов, необходимых для содействия в осуществлении расследований киберпреступлений.

- Конвенция Африканского союза о кибербезопасности и защите персональных данных 2014 года. Эта конвенция содержит, в числе прочих положений, призыв к государствам Африканского союза принимать национальные законы и/или вносить поправки в действующие национальные законы с целью эффективной борьбы с киберпреступностью, унифицировать национальные законодательства, заключать договоры о взаимной правовой помощи (ДВПП), если они еще не заключены, способствовать обмену информацией между государствами, содействовать региональному, межправительственному и международному сотрудничеству и использовать имеющиеся средства для сотрудничества с другими государствами и даже частным сектором.

Региональными организациями и/или региональными межправительственными организациями были также разработаны и имплементированы законы и директивы в сфере борьбы с киберпреступностью. Например:

- Типовой закон о компьютерных преступлениях и киберпреступности Сообщества развития Юга Африки (САДК) 2012 года. Этот закон служит руководством для государств-участников САДК для разработки норм материального и

процессуального права в области борьбы с киберпреступностью. Поскольку этот закон является типовым, он не налагает на государства каких-либо юридических обязательств в отношении осуществления сотрудничества. Государства, которые не имеют и/или не разрабатывают законы о киберпреступности, могут использовать Протокол САДК о взаимной правовой помощи по уголовным делам и Протокол САДК о выдаче для способствования сотрудничеству и координации при осуществлении международных расследований киберпреступлений.

- Директива о борьбе с киберпреступностью Экономического сообщества западноафриканских государств (ЭКОВАС) 2011 года. Эта директива требует от государств-участников криминализации киберпреступности в национальном законодательстве и способствует взаимной правовой помощи, сотрудничеству и выдаче преступников в делах, связанных с киберпреступностью и кибербезопасностью. ЭКОВАС принял Конвенцию о взаимной правовой помощи по уголовным делам и Конвенцию о выдаче с целью способствования сотрудничеству в расследовании киберпреступлений и выдаче киберпреступников.

Международное право в области прав человека и законодательство о киберпреступности

Основные положения некоторых законов о борьбе с киберпреступлениями, особенно теми, которые связаны с контентом в Интернете (см. модуль 2 серии модулей по киберпреступности: «Основные виды киберпреступности» для получения дополнительной информации об этой категории киберпреступности и киберпреступлениях, включенных в эту категорию), такими как неуважение к властям, оскорбление, диффамация главы государства, непристойность или порнографические материалы, могут чрезмерно ограничивать возможность осуществления определенных прав человека (УНП ООН, 2013, стр. xxii и 119-120). Процессуальные нормы законов о киберпреступности, обеспечивающие возможность для использования при расследовании киберпреступлений средств и методов, которые позволяют перехватывать сообщения и осуществлять электронное наблюдение, также могут привести к неоправданному ограничению возможностей осуществления прав человека, таких как право на неприкосновенность частной жизни (УНП ООН, 2013, стр. 136) (см. модуль 10 серии модулей по киберпреступности: «Конфиденциальность и защита

данных»). Необходимо соблюдать баланс между борьбой с киберпреступностью и соблюдением прав человека.

Международное законодательство в области прав человека позволяет вводить ограничения на осуществление определенных прав человека, которые могут ограничиваться на законных основаниях в особых условиях (некоторые права не могут подлежать ограничению). Эти ограничения являются допустимыми, когда они преследуют *законную цель*, *соответствуют действующему законодательству* и являются *необходимыми* и *соразмерными* угрозе, которая оправдывает их применение. Конкретный охват законных целей зависит от применимых прав человека и может включать в себя интересы общественной безопасности, национальной безопасности, экономической безопасности, охраны здоровья, защиты нравственности и защиты прав других лиц. В дополнение к необходимости введения ограничений для достижения одной из вышеупомянутых законных целей, ограничение должно вводиться на основании национального закона. Этот закон должен быть доступен гражданам, чтобы они могли соответствующим образом следить за своим поведением, знать о полномочиях властей при применении этого закона, а также о последствиях его несоблюдения. Закон должен быть четко сформулирован и не должен допускать предоставления государственным органам власти неограниченной свободы действий при применении ограничений (см. Замечание общего порядка №.34 Комитета по правам человека: (2011)). Расплывчатые и чрезмерно широкие оправдания, такие как неконкретные ссылки на «национальную безопасность», «экстремизм» или «терроризм», не подходят под определение четко сформулированных законов. Слово «необходимое» означает, что ограничение должно быть чем-то большим, чем «целесообразное», «разумное» или «желательное» (ЕСПЧ, дело «Санди Таймс» (The Sunday Times) против Соединенного Королевства, постановление суда от 26 апреля 1979 года, пункт 59). Кроме того, должна существовать соответствующая связь между законной целью, которую преследует государство, и действиями государства по достижению этой законной цели. Иными словами, действия должны быть соразмерны защищаемым интересам. Из этого следует, что ограничение является наименее интрузивной мерой по сравнению с другими мерами, с помощью которых можно обеспечить достижение желаемого результата. Государства пользуются некоторой свободой действий при выполнении своих обязательств, принятых в рамках международного законодательства в области прав человека (*свобода усмотрения*).

Свобода усмотрения

Свобода усмотрения является сложной и трудной для понимания доктриной. Для ознакомления с подробным анализом этой доктрины и ее значением см.: https://www.coe.int/t/dghl/cooperation/lisbonnetwork/themis/echr/paper2_en.asp.

Более того, даже некоторые права могут препятствовать осуществлению права на свободу слова или свободу выражения мнений, такие как право на свободу от пыток и других видов жестокого, бесчеловечного или унижающего достоинство обращения, право на неприкосновенность частной жизни (подробно рассматривается в модуле 10 серии модулей по киберпреступности: «Конфиденциальность и защита данных»), право на свободу от дискриминации и право детей на особую защиту.

Свобода выражения мнений (или свобода слова)

Статья 19 Всеобщей декларации прав человека 1948 года
Статья 10 Европейской конвенции по правам человека 1950 года
Статья 19 Международного пакта о гражданских и политических правах 1966 года
Статья 13 Американской конвенции о правах человека 1969 года
Статья 9(2) Африканской хартии прав человека и народов 1981 года

Запрет на применение пыток и других видов жестокого, бесчеловечного и унижающего достоинство обращения и наказания

Статья 5 Всеобщей декларации прав человека 1948 года
Статья 3 Европейской конвенции по правам человека 1950 года
Статья 7 Международного пакта о гражданских и политических правах 1966 года
Статья 5(2) Американской конвенции о правах человека 1969 года
Статья 5 Африканской хартии прав человека и народов 1981 года

Право на неприкосновенность частной жизни

Статья 12 Всеобщей декларации прав человека 1948 года

Статья 8 Европейской конвенции по правам человека 1950 года
Статья 17 Международного пакта о гражданских и политических правах 1966 года
Статья 11 Американской конвенции о правах человека 1969 года

Право на свободу от дискриминации

Статьи 2 и 7 Всеобщей декларации прав человека 1948 года
Статья 14 Европейской конвенции по правам человека 1950 года
Статьи 2(1) и 26 Международного пакта о гражданских и политических правах 1966 года
Статья 2(2) Международного пакта об экономических, социальных и культурных правах 1966 года
Статьи 1 и 24 Американской конвенции о правах человека 1969 года
Статьи 2 и 18(3) Африканской хартии прав человека и народов 1981 года
Статья 5 Конвенции Организации Объединенных Наций о правах инвалидов 2006 года

Такие права на свободу от дискриминации и возможность осуществления этих прав любым лицом в прямой форме предусмотрены в Международной конвенции Организации Объединенных Наций о ликвидации всех форм расовой дискриминации 1966 года и Декларации Организации Объединенных Наций о ликвидации всех форм расовой дискриминации 1963 года.

Право детей на особую защиту

Статья 24 Международного пакта о гражданских и политических правах 1966 года
Статья 10(3) Международного пакта об экономических, социальных и культурных правах 1966 года
Статья 19 Американской конвенции о правах человека 1969 года
Статья 3 Конвенции Организации Объединенных Наций о правах ребенка 1989 года

Европейский суд по правам человека распространил сферу действия этого позитивного обязательства по защите на уязвимых лиц (а именно детей) в сети Интернет, заявив, что страны обязаны принимать меры для защиты детей от вредного воздействия путем принятия соответствующего законодательства (например, см. *Mouvement raelien Suisse v. Switzerland*,

2012; *M.C. v. Bulgaria*, 2003; *Perrin v. United Kingdom*, 2003; *K.U. v. Finland*, 2008).

Совет по правам человека Организации Объединенных Наций неоднократно подтверждал, что «те же права, которые человек имеет в офлайновой среде, должны также защищаться и в онлайновой среде, в частности право на свободу выражения мнений, которое осуществляется независимо от государственных границ и любыми средствами по собственному выбору» (например, A/HRC/RES/20/8; A/HRC/RES/38/7; см. также резолюцию Генеральной ассамблеи A/RES/68/167, в которой содержится такое же подтверждение права на неприкосновенность частной жизни). Свобода выражения мнений рассматривается как право, способствующее осуществлению других основных экономических, социальных, культурных, гражданских и политических прав, включая право на свободу мирных собраний и свободу объединений, право на образование и право на участие в культурной жизни. Генеральная ассамблея Организации Объединенных Наций также признает, что «осуществление права на неприкосновенность личной жизни [также] имеет важное значение для реализации права свободно выражать свои мнения и беспрепятственно придерживаться их и является одной из основ демократического общества» (резолюция Генеральной ассамблеи A/RES/68/167).

Свобода собраний и объединений

Статья 20 Всеобщей декларации прав человека 1948 года
Статья 11 Европейской конвенции по правам человека 1950 года
Статьи 21 и 22 Международного пакта о гражданских и политических правах 1966 года
Статья 15 Американской конвенции о правах человека 1969 года
Статьи 10(1) и 11 Африканской хартии прав человека и народов 1981 года

Право на образование

Статья 26 Всеобщей декларации прав человека 1948 года
Статья 2 Протокола №.1 к Европейской конвенции по правам человека 1950 года
Статья 13 Международного пакта об экономических, социальных и культурных правах 1966 года
Статьи 23 и 28 Конвенции Организации Объединенных Наций о правах ребенка 1989 года
Статья 14 Хартия основных прав Европейского Союза 2000 года

*Право на образование также признается в Конвенции Организации Объединённых Наций по вопросам образования, науки и культуры (ЮНЕСКО) о борьбе с дискриминацией в области образования 1960 года. Это право подтверждено в международных договорах, охватывающих права отдельных групп (женщин, детей, инвалидов, беженцев, мигрантов и коренных народов), таких как Конвенция Генеральной ассамблеи Организации Объединенных Наций о ликвидации всех форм дискриминации в отношении женщин (КЛДОЖ) 1979 года; Конвенция Организации Объединенных Наций о правах ребенка; Конвенция Организации Объединенных Наций о статусе беженцев 1951 года; Конвенция Организации Объединенных Наций о защите прав всех трудящихся-мигрантов и членов их семей 1990 года; Декларация Организации Объединенных Наций о правах коренных народов 1970 года.

Право на участие в культурной жизни

Статья 27 Всеобщей декларации прав человека 1948 года
Статья 15(1) (a) Международного пакта об экономических, социальных и культурных правах 1966 года

Примечание: право на неприкосновенность частной жизни подробно рассматривается в модуле 10 серии модулей по киберпреступности» «Конфиденциальность и защита данных».

Кроме того, в 2016 году Совет по правам человека Организации Объединенных Наций принял резолюцию, осуждающую практику недопущения и/или нарушения доступа к Интернету (A/HRC/RES/32/13). Хотя всеобщий доступ к Интернету не признается в качестве одного из прав человека в международном праве в области прав человека, существуют обязательства государств в отношении поощрения подключения к Интернету, которые могут быть связаны с некоторыми правами человека, такими как право на свободу выражения мнений (A/HRC/17/27). Доступ к Интернету является также необходимым для реализации многих других прав, включая право на свободу объединений, право на свободу собраний, право на образование и охрану здоровья, право на полное участие в социальной, культурной и политической жизни, право на социальное и экономическое развитие (A/HRC/17/27). Эти обязательства включают в себя принятие «эффективных и конкретных стратегий и мер политики, разработанных на основе консультаций с представителями всех слоев общества, включая частный сектор, а также с соответствующими государственными ведомствами, с тем чтобы позволить всем на практике активно и недорого пользоваться Интернетом» (A/HRC/17/27, пункт 66). Кроме того, «[следует применять] правозащитный подход при обеспечении и расширении доступа к Интернету, и … государства [должны прилагать все] усилия для преодоления многочисленных форм цифровых разрывов» (A/HRC/32/L.20, пункт 5). В частности, Комитет по правам человека Организации Объединенных Наций заявляет, что «Государствам-участникам следует учитывать масштабы изменений в информационных и коммуникационных технологиях, таких как электронные системы распространения информации на базе Интернета и мобильной связи, которые существенно изменили методы общения во всем мире. Сегодня создана новая глобальная сеть для обмена идеями и мнениями, которая не обязательно опирается на традиционные средства массовой информации. Государствам-участникам следует принять все необходимые меры для укрепления независимости этих новых СМИ и обеспечить к ним доступ для населения» (Замечание общего порядка №.34, пункт 15). Это обязательство закреплено в национальном законодательстве некоторых страх, таких как Греция, которая внесла следующие поправки в свою конституцию: «каждый имеет право на участие в информационном обществе. Содействие в доступе к информации в электронной форме, а равно к ее производству, обмену и распространению является обязанностью государства».

Важное примечание

проблема неравенства еще более усугубляется вследствие ограничения качества и устойчивости доступа к Интернету.

Кроме того, доступ к онлайновому контенту может быть ограничен (и ограничивается) для зашиты прав других лиц. По мнению «Специального докладчика Организации Объединенных Наций по вопросу о поощрении и защите права на свободу мнений и их свободное выражение», определенные «формы выражения мнений… должны быть запрещены в соответствии с международным правом», включая «выступление в пользу национальной, расовой или религиозной ненависти, представляющее собой подстрекательство к дискриминации, вражде или насилию», и «прямое и публичное подстрекательство к геноциду» (УНП ООН, 2013, стр. 124). Такой запрет также закреплен в статье 20(2) Международного пакта о гражданских и политических правах 1966 года, которая запрещает «[в]сякое выступление в пользу национальной, расовой или религиозной ненависти, представляющее собой подстрекательство к дискриминации, вражде или насилию», и статье III(c) Конвенции о предупреждении преступления геноцида и наказании за него 1948 года, которая запрещает прямое и публичное подстрекательство к совершению геноцида. В «Рабатском плане действий по запрещению пропаганды национальной, расовой или религиозной ненависти, представляющей собой подстрекательство к дискриминации, вражде или насилию» (A/HRC/22/17/Add. 4) проводится четкое различие между различными типами высказываний: «высказывание, которое является уголовным преступлением; высказывание, которое не является уголовно наказуемым, но может подлежать гражданскому иску или административным санкциям; высказывание, не подлежащее уголовным, гражданским или административным санкциям, но, тем не менее, вызывающее озабоченность с точки зрения толерантности, корректности и уважения прав других людей» (пункт 20).

Государства могут ограничивать (и уже ограничили) ксенофобские и расистские высказывания с целью сохранения общественного порядка и защиты прав лиц, к которым обращены такие высказывания. В Танзании Закон о киберпреступлениях 2015 года запрещает производство, предложение, предоставление и распространение расистских и ксенофобских материалов (статья 17) и оскорбления на почве расизма и ксенофобии (статья 18) (для ознакомления с критическим обзором Закона Танзании о киберпреступлениях 2015 года, в том числе его положений, запрещающих расистские и ксенофобские материалы, см. отчет британской правозащитной организации «Article 19»). Европейский суд по правам человека (ЕСПЧ) постановил, что высказывания, в которых заявляется, что все мусульмане являются террористами, и отрицается холокост (*Norwood v. the United Kingdom*, 2003); *Garaudy v. France*, 2003) не подпадают под защиту

статьи 10 Европейской конвенции по правам человека. В Соединенном Королевстве Великобритании Закон о расовой и религиозной ненависти 2006 года предусматривает уголовную ответственность за высказывания, которые разжигают расовую и/или религиозную ненависть.

> *Знаете ли вы?*
>
> Статья 17 Европейской конвенции по правам человека (ЕКПЧ) запрещает злоупотребление правами. Согласно статье 17 ЕКПЧ, «ничто в настоящей Конвенции не может толковаться как означающее, что какое-либо Государство, какая-либо группа лиц или какое-либо лицо имеет право заниматься какой бы то ни было деятельностью или совершать какие бы то ни было действия, направленные на упразднение прав и свобод, признанных в настоящей Конвенции, или на их ограничение в большей мере, чем это предусматривается в Конвенции».

Пропаганда ненависти направлена на то, чтобы очернить целевую группу других людей и разделить членов общества не тех, кто поддерживает пропаганду ненависти и придерживается схожих с ней идеологий (т.е. на группу «мы»), и тех, кто входит в целевую группу *других* людей, толерантных к этой группе, и тех, кто тем или иным образом поддерживает целевую группу. Цель этой пропаганды заключается в обособлении, а порой и в дегуманизации целевой группы путем приравнивая их к насекомым, животным, болезням и демонам. Пропаганда такого типа, наряду с подстрекательством к насилию и геноциду, наблюдалась, например, во время геноцида в Руанде.

Во время геноцида в Руанде тутси были прозваны тараканами (*иньензи*), а радиостанция «Свободное радио и телевидение тысячи холмов» (RTLM) призывала к уничтожению «тараканов тутси» (Gourevitch, 1998; Bhavnani, 2006). Журналисты радио (и печатных средств массовой информации) в Руанде были привлечены к уголовной ответственности и осуждены за распространение ненавистнических высказываний и пропаганду ненависти, а также за подстрекательство к насилию и геноциду. Например, Жан-Боско Бараягвиза и Фердинанд Нахимана, основатели радиостанции «Свободное радио и телевидение тысячи холмов» (RTLM), и Хассан Нгезе, основатель и редактор местной газеты (Kanguara), были признаны виновными, в частности, в прямом и публичном подстрекательстве к геноциду (*The Prosecutor v. Ferdinand Nahimana, Jean-Bosco Barayagwiza, Hassan Ngeze*, 2003; Baisley, 2014, 39). Во время вынесения приговора Фердинанду Нахимане в Международном уголовному трибунале по Руанде судья заявил: «Вы были в полной мере осведомлены о силе слова, и вы использовали радио – средство коммуникации с широчайшим охватом населения – для распространения ненависти и насилия…. Без огнестрельного оружия, мачете или какого-либо иного физического

оружия вы стали причиной гибели тысяч ни в чем не повинных гражданских лиц» (Организация Объединенных Наций, Международный остаточный механизм для уголовных трибуналов 2003; *The Prosecutor v. Ferdinand Nahimana, Jean-Bosco Barayagwiza, Hassan Ngeze*, 2003).

Помимо радио, для ненавистнических высказываний и пропаганды ненависти, а также для подстрекательства к насилию и геноциду могут использоваться (и используются) онлайн-платформы. Рассмотрим роль одной из социальных медиаплатформ в совершении предполагаемых актов геноцида в Мьянме. Как сообщали средства массовой информации, «более 650.000 мусульман-рохинджа… бежали из штата Ракхайн в Мьянме в Бангладеш, после того как нападения повстанцев повлекли за собой жестокие меры по обеспечению безопасности … [в августе 2017 года]. Большинство пострадавших предоставили ужасные доказательства убийств и изнасилований со стороны сил безопасности Мьянмы» (Miles, 2018). По утверждению представителя Независимой международной миссии Организации Объединенных Наций по установлению фактов в Мьянме (Марзуки Дарусман), «Facebook» «сыграл определяющую роль» в Мьянме, «в значительной мере способствовав повышению уровня ярости, раздоров и конфликтов [с мусульманами-рохинджа]» (Baynes, 2018) в «Мьянме путем распространения пропаганды насилия» (Miles, 2018). В частности, в заявлении миссии по установлению фактов говорилось, что

> у членов миссии нет никаких сомнений в том, что широкая распространенность ненавистнических высказываний в Мьянме в значительной степени способствовала росту напряженности и созданию атмосферы, в которой отдельные лица и группы людей могли стать более восприимчивыми к подстрекательству и призывам к насилию. Это также относится к ненавистническим высказываниям в «Facebook». Степень, в которой распространение сообщений и слухов в «Facebook» усилило дискриминацию и насилие в Мьянме, должна быть независимо и тщательно исследована, с тем чтобы можно было извлечь соответствующие уроки и предотвратить аналогичные сценарии. Точно так же необходимо оценить влияние недавних мер, принятых «Facebook» для предотвращения случаев злоупотреблений своей платформой и исправления положения (A/HRC/39/CRP.2, пункт 1354).

Еще один пример связан с использованием другой социальной медиаплатформы, «YouTube», для распространения ненавистнических высказываний и подстрекательства к насилию. Фуад Белкасем, который был лидером и представителем (бывшей) организации «Sharia4Belgium» (Шариат для Бельгии), выложил видеоматериалы на «YouTube», предназначенные для распространения ненависти и, в конечном счете, подстрекательства к насилию; он называл немусульманское население, в частности,

животными и призывал «зрителей вытеснять немусульманское население, ‘преподать ему урок’ и… бороться с ним» (*Belkacem v. Belgium*, 2017; Voorhoof, 2017).

Права интеллектуальной собственности (ИС) могут также служить оправданием для ограничения права на свободу выражения и на доступ к информации. Например, при соблюдении определенных требований блокировка веб-сайтов, незаконно предоставляющих доступ к контенту, который защищен правом интеллектуальной собственности, может быть оправданной. Европейский суд по правам человека постановил и признал, что права авторов интеллектуальной собственности должны защищаться (*Neij and Sunde Kolmisoppi v. Sweden*, 2012). Тем не менее, поскольку меры блокировки являются весьма деликатными мерами, которые могут затрагивать права многих людей (в частности, их право на распространение, поиск и получение информации), следует уделять больше внимания обеспечению баланса между правами человека и требованиями в отношении законных мер блокировки (см., например, дела, рассматривавшиеся в Суде Европейского союза *UPC Telekabel Wien GmbH v Constantin Film Verleih GmbH and Wega Filmproduktionsgesellschaft mbH*, 2014; *Cengiz and Others v. Turkey*, 2015; Комитет по правам человека, Замечание общего порядка №.34 к статье 19 Международного пакта о гражданских и политических правах).

Доступ к Интернету также блокировался в связи с политическими волнениями. В частности, правительства стран закрывали гражданам доступ к Интернету и социальным сетям (полностью или частично) во время акций протестов и прочих событий национального значения (например, в Камеруне, Египте и Уганде) (Odhiambo, 2017). Доступ блокировался для отдельных лиц и/или к отдельному контенту, а в некоторых случаях доступ к Интернету блокировался на определенный период времени для всего населения. В Индии в 2017 году доступ к 22 социальным сетям (например, Twitter, Facebook, Snapchat и YouTube) и приложениям для обмена сообщениями (например, WhatsApp, Skype и WeChat) в Кашмирской долине был заблокирован в связи с массовыми волнениями. Можно привести еще много случаев, когда массовые волнения приводили к блокировке Интернета и работы мобильной и стационарной связи в этом и других регионах Индии (Freedom House, 2017).

Предварительная цензура со стороны государства (т.е. ограничение в отношение контента до того, как он будет доступен для публичного или частного потребления) и практика блокировки онлайн-контента вступают в прямое противоречие с правом отдельных лиц на доступ к информации. В деле *Ahmet Yildirim v. Turkey* (2010) на частном веб-сайте, который был создан через хостинг «Сайты Google», публиковались, в числе прочего, труды его создателя и владельца. Его сайт был сочтен оскорблением памяти и наследию Мустафы Кемаля Ататюрка, что запрещено в соответствии с турецким Законом №.5816 в частности, который предусматривает наказание за преступления против Ататюрка, и в соответствии со статьей 301 Уголовного кодекса Турции в целом, которая

запрещает оскорбления в отношении Турции и ее институтов. В ответ на размещение контента на его вебсайте, вместо блокировки доступа к этому сайту, турецкие власти заблокировали все сайты. Действия Турции были сочтены нарушением требований статьи 10 Европейской конвенции по правам человека. В то время как временные или частичные меры приостановки или блокировки могут быть оправданы в особых обстоятельствах, приостановка работы Интернет-сервисов и блокировка доступа к Интернету для всего населения и его отдельных групп не могут быть оправданы с юридической точки зрения. В докладе Специального докладчика Организации Объединенных Наций по вопросу о поощрении и защите права на свободу мнений и их свободное выражение говорится, что: «блокировка Интернет-платформ и отключение систем телекоммуникационной инфраструктуры представляют собой устойчивую угрозу; даже если основанием для таких мер служат интересы государственной безопасности или поддержания общественного порядка, их применение, как правило, приводит к блокировке сообщений миллионов людей» (A/71/373 пункт 22). В докладе также упоминается, что в 2015 году «Организация Объединенных Наций и региональные эксперты в области свободы выражения мнений в совместном заявлении осудили незаконные блокировки сети Интернет» (A/71/373 пункт 22).

Совет Организации Объединенных Наций по правам человека в своей резолюции 32/13 «безоговорочно осуждает также меры по умышленному недопущению или нарушению доступа к информации или ее распространения в режиме онлайн в нарушение норм международного права прав человека и призывает все государства воздерживаться от таких мер и прекратить их использование» (A/HRC/RES/32/13). Как справедливо отмечает Комитет по правам человека Организации Объединенных Наций (Замечание общего порядка №.34, пункт 43, CCPR/C/GC/34), «любые ограничения на работу вебсайтов, блогов и любых других подобных систем распространения электронной и иной информации, основанных на Интернет-технологиях, в том числе систем, обеспечивающих работу подобных средств коммуникации, таких как системы доступа к сети Интернет или поисковые системы, допустимы в той мере, в какой они совместимы с пунктом 3 [статьи 19 Международного пакта о гражданских и политических правах]. Допустимые ограничения должны основываться главным образом на содержании конкретных материалов; общие запреты на функционирование определенных сайтов и систем несовместимы с пунктом 3 [статьи 19 Международного пакта о гражданских и политических правах 1966 года]. Любые меры блокировки должны быть узконаправленными и индивидуальными, чтобы затрагивать только те веб-страницы, которые содержат незаконный контент. Приостановка работы Интернет-сервисов и блокировка доступа к Интернету для всего населения и его отдельных групп не могут быть оправданы с юридической точки зрения».

Пример ограничения права на свободу слова

Правительство страны К направляет средствам массовой информации уведомление, в котором оно запрещает им популяризировать «западный образ жизни» и высмеивать ценности страны К. Государственный орган страны К закрывает несколько новостных онлайн-каналов за распространение информации, которую правительство считает неверной и/или незаконной, и/или за неспособность удалять на своих сайтах комментарии, поддерживающие высказывания, которые правительство считает недозволительными. Страна К требует, чтобы частные компании в упреждающем порядке отслеживали свои сайты и удаляли этот некорректный и/или незаконный контент.

Заключение

Было заключено несколько международных договоров, связанных с киберпреступностью. В целом существующие многосторонние и региональные правовые документы и национальные законы различаются по своему тематическому содержанию и степени охвата таких аспектов, как криминализация, следственные меры и полномочия, сбор и использование цифровых доказательств, регулирование и риск, юрисдикция и международное сотрудничество. Эти договоры также различаются по своему географическому охвату (т.е. являются региональными или многосторонними) и сфере применения. Такие различия создают препятствия для эффективной идентификации, расследования и уголовного преследования киберпреступников и предупреждения киберпреступности.

Необходимы гарантии для обеспечения того, чтобы законы, ограничивающие контент и доступ к Интернету, применялись в законных целях и соответствовали принципу верховенства закона и стандартам в области прав человека. Кроме того, законы должны содержать предельно четкие положения, не допускающие их использование с целью запрещения доступа к контенту в нарушение законодательства в области прав человека. Существует опасность «размывания (отклонения от основного) мандата» или «размывания функций» (эти термины используются для описания случаев распространения законов и/или иных мер на области, находящиеся за пределами их первоначальной сферы действия), когда законы и следственные полномочия, изначально нацеленные на один вид киберпреступности, впоследствии нацеливаются на другие, менее тяжкие виды киберпреступлений. Более того, сложности, связанные со сферой действия и применения законов о киберпреступности, возникают в тех случаях, «когда

Интернет-контент, генерируемый и приемлемый в одной стране, становится доступен в третьей стране», где такой контент считается незаконным (УНП ООН, 2013, стр. 128).

Список использованной литературы

- Британская правозащитная организация «Article 19». (2015). Танзания: Закон о киберпреступности 2015 года. https://www.article19.org/data/files/medialibrary/38058/Tanzania-Cybercrime-Bill-TO.pdf.
- Baisley, Elizabeth. (2014). Genocide and Constructions of Hutu and Tutsi in Radio Propaganda. *Race & Class*, Vol. 55(3), 38–59.
- Baynes, Chris. (2018). United Nations blames Facebook for spreading hatred of Rohingya Muslims in Myanmar. *The Independent*, March 15, 2018. https://www.independent.co.uk/news/world/asia/myanmar-un-blames-facebook-spreading-hatred-rohingya-muslims-a8256596.html.
- Bhavnani, Ravi. (2006). Ethnic Norms and Interethnic Violence: Accounting for Mass Participation in the Rwandan Genocide. *Journal of Peace Research*, Vol. 43(6), 651-659.
- Boas, Gideon, James L. Bischoff, Natalie L. Reid, and B. Don Taylor III. (2011). *International Criminal Procedure*, Volume 3. Cambridge University Press.
- Brenner, Susan W. and Bert-Jaap Koops. (2004). Approaches to cybercrime jurisdiction. *Journal of High Technology Law*, Vol. 4(1), 1-46.
- Dubber, Markus. (2011). The American Law Institute's Model Penal Code and European Criminal Law. In André Klip (Ed.), *Substantive Criminal Law of the European Union*. Maklu. https://tspace.library.utoronto.ca/bitstream/1807/88953/1/Dubber%20The%20American%20Law.pdf.
- Fletcher, George P. (2000) *Rethinking Criminal Law* (2nd ed.). Oxford University Press.
- Freedom House (2017). Freedom of the Net 2017: India Profile. https://freedomhouse.org/report/freedom-net/2017/india.
- Gourevitch, Philip. (1998). *We Want To Inform You that Tomorrow We Will Be Killed with Our Families: Stories from Rwanda*. Farrar, Straus and Giroux.
- LaFave, Wayne R., Jerold H. Israel, Nancy J. King, and Orin S. Kerr. (2015). *Criminal Procedure*, 4th edition. Thomson Reuters.
- Maras, Marie-Helen. (2014). *Computer Forensics: Cybercriminals, Laws and Evidence*, second edition. Jones and Bartlett.
- Maras, Marie-Helen. (2016). *Cybercriminology*. Oxford University Press.
- Maras, Marie-Helen. *Cyberlaw and Cyberliberties*. Oxford University Press, forthcoming, 2020 (готовится к публикации).

- Miles, Tom. (2018). U.N. investigators cite Facebook role in Myanmar crisis. *Reuters*, March 12, 2018. https://www.reuters.com/article/us-myanmar-rohingya-facebook/u-n-investigators-cite-facebook-role-in-myanmar-crisis-idUSKCN1GO2PN.
- Odhiambo, Sharon Anyango. (2017). Internet shutdowns during elections. Africa Up Close, Wilson Center. https://africaupclose.wilsoncenter.org/internet-shutdowns-during-elections/.
- Ohlin, Jens David. (2013). Targeting and the Concept of Intent. Michigan Journal of International Law, Vol. 35, 79-130. https://scholarship.law.cornell.edu/cgi/viewcontent.cgi?article=2354&context=facpub.
- Rahman, Rizal. (2012). Legal jurisdiction over malware-related crimes: From theories of jurisdiction to solid practical application. *Computer Law & Security Review* 28 (2012) 403-415.
- Sandle, Tim. (2016). UN thinks Internet access is a human right. *Business Insider*, 22 July 2016. http://www.businessinsider.com/un-says-internet-access-is-a-human-right-2016-7.
- Simons, Kenneth, W. (2003). Should the Model Penal Code's Mens Rea Provisions Be Amended? *Ohio State Journal of Criminal Law*, Vol. 1, 179-205. http://www.bu.edu/lawlibrary/facultypublications/PDFs/Simons/MPCMensRea.pdf.
- United Nations International Residual Mechanism for Criminal Tribunals. (2003). Three Media Leaders convicted for Genocide. http://unictr.irmct.org/en/news/three-media-leaders-convicted-genocide.
- УНП ООН (2013). Проект доклада УНП ООН «Всестороннее исследование проблемы киберпреступности» https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf.
- УНП ООН. База данных SHERLOC. https://www.unodc.org/unodc/en/cybercrime/cybercrime-repository.html.
- УНП ООН. (2015). База данных по киберпреступности. https://www.unodc.org/unodc/en/cybercrime/cybercrime-repository.html.
- Voorhoof, Dirk. (2017). European Court of Human Rights: Fouad Belkacem v. Belgium. IRIS 2017-9:1/1. http://merlin.obs.coe.int/article.php?id=15980.
- Wall, David S. (2007). *Cybercrime: The Transformation of Crime in the Information Age*. Polity Press (2nd edition, forthcoming 2020) (готовится к публикации)

Список дел

- *Ahmet Yildirim v. Turkey* ECHR (App. no. 3111/10), 18 December 2012.
- *Akdeniz v. Turkey*, ECHR (App no. 25165/94), 31 May 2005.
- *Belkacem v. Belgium* ECHR (App. no. 34367/14), 20 July 2017.
- *Cengiz and Others v. Turkey*, ECHR (Apps nos. 48226/10 and 14027/11) 1 December 2015.
- *Garaudy v. France*, ECHR (App no. 23131/03), 24 June 2003.
- *K.U. v. Finland*, ECHR (App no. 2872/02), 2 December 2008
- *M.C. v. Bulgaria* (App no. 39272/98) [2005] 40 EHRR 20.
- *Mouvement raelien Suisse v. Switzerland* (App no. 16354/06) [2011] ECHR 1832.
- Neij and Sunde Kolmisoppi v. Sweden, ECHR (App no. 40397/12), 19 February 2013.
- *Norwood v. the United Kingdom*, ECHR (App no. 23131/03), 16 November 2004.
- Perrin v. United Kingdom, ECHR (App no. 5446/03), 18 October 2005.
- *The Prosecutor v. Ferdinand Nahimana, Jean-Bosco Barayagwiza, Hassan Ngeze* (Judgment and Sentence), ICTR-99-52-T (3 December 2003).
- *UPC Telekabel Wien GmbH v. Constantin Film Verleih GmbH and Wega Filmproduktionsgesellschaft mbH*, CJEU (C-314/12) 27 March 2014.

Законы

- Африканская хартия прав человека и народов 1981 года (http://www.achpr.org/instruments/achpr/).
- Конвенция Африканского союза о кибербезопасности и защите персональных данных 2014 года. (https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection).
- Проект Конвенции Африканского союза о создании юридических основ кибербезопасности в Африке 2012 года (https://ccdcoe.org/sites/default/files/documents/AU-120901-DraftCSConvention.pdf).
- Американская конвенция о правах человека 1969 года (https://www.cidh.oas.org/basicos/english/basic3.american%20convention.htm).
- Конвенция Лиги арабских государств о борьбе с преступлениями в области информационных технологий 2010 года (http://itlaw.wikia.com/wiki/Arab_Convention_on_Combating_Information_Technology_Offences).
- Хартия основных прав Европейского Союза 2000 года (Хартия основных прав Европейского Союза 2000 года). (http://www.europarl.europa.eu/charter/pdf/text_en.pdf)

- Соглашение Содружества Независимых Государств о сотрудничестве в борьбе с преступлениями в сфере компьютерной информации 2001 года. (https://dig.watch/instruments/agreement-cooperation-combating-offences-related-computer-information-commonwealth).
- Закон о содействии правоохранительным органам в области коммуникаций 1994 года (Соединенные Штаты Америки). (https://www.fcc.gov/public-safety-and-homeland-security/policy-and-licensing-division/general/communications-assistance).
- Закон о компьютерном мошенничестве и злоупотреблении 1986 года (Соединенные Штаты Америки) (https://www.law.cornell.edu/uscode/text/18/1030).
- Закон о компьютерном мошенничестве и киберпреступности 2003 года (Маврикий) (https://www.unodc.org/res/cld/document/computer_misuse_and_cybercrime_act_2003_html/Computer_Misuse_and_Cybercrime_Act_2003.pdf).
- Конвенция Совета Европы о киберпреступности 2001 года (https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680081561).
- Закон о неправомерном использовании компьютерных технологий 1990 года (https://www.legislation.gov.uk/ukpga/1990/18/contents).
- Уголовно-процессуальный кодекс Китайской Народной Республики (с поправками 2012 года) (http://en.pkulaw.cn/display.aspx?cgid=169667&lib=law).
- Закон о киберпреступности 2001 года (№.161, 2001) (Австралия) (https://www.legislation.gov.au/Details/C2004A00937).
- Закон о киберпреступности 2015 года (Ямайка) (http://www.japarliament.gov.jm/attachments/339_The%20Cybercrimes%20Acts,%202015.pdf).
- Закон о киберпреступности 2015 года (Танзания) (https://rsf.org/sites/default/files/the_cyber_crime_act_2015.pdf).
- Закон о (запрете, предотвращении и т.д.) киберпреступлений 2015 года (Нигерия) (http://lawnigeria.com/LawsoftheFederation/Cyber-Crime-Act,-2015.html).
- Конвенция ЭКОВАС о выдаче (http://documentation.ecowas.int/download/en/legal_documents/protocols/Convention%20on%20Extradition.pdf).
- Конвенция ЭКОВАС о взаимной правовой помощи по уголовным делам (http://documentation.ecowas.int/download/en/legal_documents/protocols/Convention%20on%20Mutual%20Assistance%20in%20Criminal%20Matters.pdf).
- ЭКОВАС. Директива о борьбе с киберпреступностью (2011) (http://www.tit.comm.ecowas.int/wp-content/uploads/2015/11/SIGNED_Cybercrime_En.pdf).

- Европейская конвенция по правам человека 1950 года (https://www.echr.coe.int/Documents/Convention_ENG.pdf).
- Закон о конфиденциальности электронных сообщений 1986 года (Соединенные Штаты Америки) (https://www.law.cornell.edu/uscode/text/18/part-I/chapter-119).
- Конституция Греции (http://www.hri.org/docs/syntagma/).
- Международный пакт о гражданских и политических правах 1966 года (https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx).
- Международный пакт об экономических, социальных и культурных правах 1966 года (https://www.ohchr.org/EN/ProfessionalInterest/Pages/CESCR.aspx).
- Закон об Интернете №.5651 (Турция) (http://www.wipo.int/wipolex/en/details.jsp?id=11035).
- Гражданский кодекс Ирака №.40 от 1951 года (http://gjpi.org/library/primary/statutes/).
- Уголовный кодекс Ирака №.111 от 1969 года (http://gjpi.org/library/primary/statutes/).
- Закон №.14 от 2014 года о введении в действие Закона о профилактике киберпреступности (Катар) (http://www.ilo.org/dyn/natlex/natlex4.detail?p_lang=en&p_isn=100242).
- Закон №.2008-11 о киберпреступности (Сенегал) (http://www.wipo.int/wipolex/en/text.jsp?file_id=243067).
- Конвенция Лиги арабских государств о борьбе с преступлениями в области информационных технологий 2010 года (http://itlaw.wikia.com/wiki/Arab_Convention_on_Combating_Information_Technology_Offences).
- Типовой закон САДК о компьютерных преступлениях и киберпреступности 2012 года (https://www.itu.int/en/ITU-D/Cybersecurity/Documents/SADC%20Model%20Law%20Cybercrime.pdf).
- Протокол САДК о взаимной правовой помощи по уголовным делам. (https://www.imolin.org/doc/amlid/Namibia_protmutual.pdf).
- Протокол САДК о выдаче (https://www.sadc.int/files/3513/5292/8371/Protocol_on_Extradiction.pdf).
- Шанхайская организация сотрудничества: Соглашение о сотрудничестве в области обеспечения международной информационной безопасности 2010 года (http://cis-legislation.com/document.fwx?rgn=28340).
- Закон США о сохраненных сообщениях 1986 года (Соединенные Штаты Америки) (https://www.law.cornell.edu/uscode/text/18/part-I/chapter-121).
- Закон о расовой и религиозной ненависти 2006 года (Соединенное Королевство) (https://www.legislation.gov.uk/ukpga/2006/1/contents).
- Закон Турции №.5816 (http://www.refworld.org/pdfid/44c611504.pdf).

- Конвенция Организации Объединенных Наций о защите прав всех трудящихся-мигрантов и членов их семей 1990 года (https://treaties.un.org/Pages/ViewDetails.aspx?src=IND&mtdsg_no=IV-13&chapter=4&clang=_en).
- Конвенция Организации Объединенных Наций о правах ребенка 1989 года. (https://www.ohchr.org/EN/ProfessionalInterest/Pages/CRC.aspx).
- Конвенция Организации Объединенных Наций о правах инвалидов (https://www.un.org/development/desa/disabilities/convention-on-the-rights-of-persons-with-disabilities.html).
- Декларация Организации Объединенных Наций о недопустимости вмешательства во внутренние дела государств, об ограждении их независимости и суверенитета (http://www.un-documents.net/a20r2131.htm).
- Декларация Организации Объединенных Наций о ликвидации всех форм расовой дискриминации 1963 года (http://www.un-documents.net/a18r1904.htm).
- Декларация Организации Объединенных Наций о правах коренных народов 1970 года (http://www.un.org/esa/socdev/unpfii/documents/DRIPS_en.pdf).
- Конвенция Генеральной ассамблеи Организации Объединенных Наций о ликвидации всех форм дискриминации в отношении женщин 1979 года (http://www.un.org/womenwatch/daw/cedaw/text/econvention.htm).
- Совет Организации Объединенных Наций по правам человека. Проект Резолюции «Поощрение, защита и осуществление прав человека в Интернете», 29 июня 2012 (A/HRC/20/L.13) (https://documents-dds-ny.un.org/doc/UNDOC/LTD/G12/147/10/PDF/G1214710.pdf?OpenElement).
- Совет Организации Объединенных Наций по правам человека. Проект Резолюции «Поощрение, защита и осуществление прав человека в Интернете», 27 июня 2016 (A/HRC/32/L.20) (http://undocs.org/A/HRC/32/L.20).
- Международная конвенция Организации Объединенных Наций о ликвидации всех форм расовой дискриминации 1966 года (http://www.supremecourt.ge/files/upload-file/pdf/act6.pdf).
- Конвенция Организации Объединенных Наций о статусе беженцев 1951 года (http://www.unhcr.org/en-us/1951-refugee-convention.html).
- Конвенция Организации Объединённых Наций по вопросам образования, науки и культуры (ЮНЕСКО) о борьбе с дискриминацией в области образования 1960 года (http://portal.unesco.org/en/ev.php-URL_ID=12949&URL_DO=DO_TOPIC&URL_SECTION=201.html).
- Всеобщая декларация прав человека 1948 года (http://www.un.org/en/universal-declaration-human-rights/).

Упражнения

Упражнение №.1 – Тематическое исследование: Унижение в сети Интернет и права человека

В 2005 году в сети стало быстро распространяться фото женщины под заголовком «Девушка с собачьей какашкой» в качестве способа унижения за то, что девушка не подобрала экскременты ее собаки в метро (McCreary, 2008; Walker 2013).

Пожалуйста, ознакомьтесь со следующими публикациями:

1) Henig, Samantha. (2005). The tale of Dog Poop Girl is not so funny after all. *Columbia Journalism Review*. https://archives.cjr.org/behind_the_news/the_tale_of_dog_poop_girl_is_n.php.
2) McCreary, Lew. (2008). What was privacy? *Harvard Business Review*, October 2008. https://hbr.org/2008/10/what-was-privacy.
3) Walker, Duncan. (2013). Eight radical solutions to the problem of dog mess. *BBC News*, June 14, 2013. http://www.bbc.com/news/magazine-22853270.

[Примечание: для получения информации о случаях унижения в сети Интернет см.: Chapter 9, Maras, Marie-Helen. (2016). *Cybercriminology*. Oxford University Press].

Вопросы для обсуждения

1) Каким правам противоречит эта практика?
2) Является ли унижение мерой, соразмерной совершенному деянию?

Упражнение №.2 – Тематическое исследование: Отсутствие законов о киберпреступности

В 2000 году скандально известный вирус «LOVE BUG» был распространен по электронной почте; письмо имело заголовок «ILOVEYOU» и приложение (LOVE-LETTER-FOR-YOU.TXT). Как только пользователь открывал приложение, вредоносная программа загружалась в компьютер пользователя, и вирус рассылал копию самого себя всем контактам в адресной книге пользователя. Создатель и распространитель вируса «LOVE BUG», Онель де Гусман (Onel de Guzman), был гражданином Филиппин, где на тот момент времени отсутствовал закон, криминализирующий такое деяние (Maras, 2014).

Вопросы для обсуждения

1) Каковы последствия отсутствия национальных законов о киберпреступности?
2) Существуют ли еще какие-либо страны, где это могло бы произойти сегодня?

Упражнение №.3 – Тематическое исследование: право на свободу выражения мнений и закон о киберпреступности

В августе 2017 года тайский студент-активист был заключен в тюрьму на два с половиной года за размещение в «Facebook» статьи «Би-би-си», которая была сочтена оскорбительной для короля Таиланда. Он выложил в социальную сеть ссылку на статью «Би-би-си» на тайском языке, в которой описывалась биография короля, через два дня после инаугурации нового короля. Статью просмотрели более 2000 человек. Он был также обвинен в нарушении закона о компьютерных преступлениях. В соответствии с тайским законодательством оскорбление величества (lese-majeste) представляет собой тяжкое преступление против королевской семьи.

Пожалуйста, ознакомьтесь со следующими публикациями:

1) Thai activist jailed for two and a half years for posting BBC article. https://www.reuters.com/article/us-thailand-king-insult-idUSKCN1AV0YN
2) Уголовный кодекс Таиланда. Статья 112. http://library.siam-legal.com/thai-law/criminal-code-royal-family-sections-107-112/
3) Press briefing note on Thailand. United Nations High Commissioner's for Human Rights Office https://www.ohchr.org/en/NewsEvents/Pages/DisplayNews.aspx?NewsID=21734&LangID=E

Вопросы для обсуждения

- Каким правам человека противоречит статья 112 Уголовного кодекса Таиланда?
- Преследуют ли существующие ограничения прав человека законную цель, соответствуют ли они действующему законодательству, и являются ли они необходимыми и соразмерными угрозе, которую представляет собой совершенное деяние?

Возможная структура занятия

Ниже описана рекомендуемая структура для занятия. Учащиеся должны закончить прочтение обязательной литературы до начала занятия. Лекции призваны закрепить материал, с которым учащиеся ознакомились при прочтении литературы, а упражнения предназначены для практического применения знаний, полученных из прочтенной литературы и лекций. Для трехчасового занятия предлагается следующая структура. Лекторы могут изменить эту структуру, исходя из своих потребностей и расписания занятий.

Представление занятия и результатов обучения

Лекция (10 минут):

- Вкратце представьте занятие и его содержание
- Определите и обсудите конечные результаты занятия

Роль законодательства о киберпреступности

Лекция (40 минут):

- Опишите материальное и процессуальное право и объясните различие между ними
- Рассмотрите и оцените отдельные национальные законы о киберпреступности

Унификация законов

Лекция (10 минут):

- Обсудите важность унификации законов и международного сотрудничества

Обсуждение тематического исследования (20 минут):
В разделе «Упражнения» данного модуля имеется отдельное упражнение под заголовком «Упражнение №.2 – Тематическое исследование: Отсутствие законов о киберпреступности». Используйте вопросы из этого упражнения для проведения обсуждения этой темы.

[*Напоминание: это упражнение должно быть выполнено до начала занятия. Для того чтобы подготовиться к этому учебному заданию, учащиеся должны выполнить веб-упражнение под названием «SHERLOC» в разделе «Дополнительные средства обучения» данного модуля].

Перерыв

Время: 10 минут

Международные и региональные правовые документы

Лекция (20 минут):

- Определите международные и региональные правовые документы, относящиеся к киберпреступности, обсудите их и проведите различие между ними.

Упражнение (20 минут):
В разделе «Оценка учащихся» данного модуля имеется групповое упражнение под названием «Нормы материального и процессуального права в области борьбы с киберпреступностью». Попросите группы учащихся обсудить свои результаты в классе. Это задание предназначено для практического применения знаний, полученных учащимися после изучения разделов «роль законодательства о киберпреступности», «унификация», «международное сотрудничество», «международные и региональные правовые документы» и ознакомления с основной литературой.
[*Напоминание: это упражнение должно быть выполнено до начала занятия].

Международное право в области прав человека и законодательство о киберпреступности

Лекция (30 минут):

- Изучите региональные и международные договоры в области прав человека и их применимость к защите прав человека в сети Интернет.
- Обсудите связь между правами человека, а также связь между правами человека и законодательством в области киберпреступности.

[*Не забудьте включить материал для оценки учащихся в свою лекцию («Проверка знаний»). В этом материале учащимся задается вопрос о том, подпадает ли то или иное высказывание под действие законодательства о защите свободы слова или не подпадает под его действие].

Обсуждение тематического исследования (20 минут):
В разделе «Упражнения» данного модуля имеется отдельное упражнение под заголовком «Упражнение №.1 – Тематическое исследование: Унижение в сети Интернет и права человека». Используйте вопросы из этого упражнения для проведения обсуждения этой темы.

[Альтернативный вариант: В разделе «Упражнения» данного модуля имеется отдельное упражнение под заголовком «Упражнение №.3 – право на свободу выражения мнений и законодательство о киберпреступности». Используйте вопросы из этого упражнения для проведения обсуждения этой темы].

Список основной литературы

Учащимся следует ознакомиться со следующими публикациями (в основном доступными в открытых источниках), входящими в категорию обязательной для прочтения литературы, до начала занятий по данному модулю:

- Guarda, Nicola Dalla. (2015). Governing the ungovernable: international relations, transnational cybercrime law, and the post-Westphalian regulatory state. *Transnational Legal Theory* Vol. 6(1), 211-249.
- ITU. (2014). Understanding Cybercrime: Phenomena, Challenges and Legal Response. https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Publications.aspx
- Strossen, Nadine. (2000). Cybercrimes v. Cyberliberties. *International Review of Law, Computers & Technology*, Vol. 14(1), 11-24.
- УНП ООН (2013). Проект доклада УНП ООН «Всестороннее исследование проблемы киберпреступности» (pp. 51-116). https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf (Главы 3 и 4).
- Whitmore, Andrew, Namjoo Choi, and Anna Arzrumtsya. (2009). One Size Fits All? On the Feasibility of International Internet Governance. *Journal of Information Technology & Politic*s, Vol. 6(1), 4-11.

Список дополнительной литературы

Следующая литература рекомендуется учащимся, заинтересованным в более детальном изучении тематических вопросов, охваченных данным модулем:

- Brenner, Susan W. (2006). Cybercrime jurisdiction. *Crime, Law and Social Change*, Vol. 46(4), 189–206.
- Farrell, Kristen. (2007). The Big Mamas Are Watching: China's Censorship of the Internet and the Strain on Freedom of Expression. *Michigan State Journal of International Law*, Vol. 15, 577-603.
- Grasmick, Brittany. (2015). Recognizing "Access to Information" as a Basic Human Right: A Necessary Step in Enforcing Human Rights Provisions Within Free Trade Agreements. *Loyola University Chicago International Law Review*, Vol. 12, 215-230.
- Guichard, Audrey. (2009). Hate Crime in Cyberspace: The Challenges of Substantive Criminal Law. *Information & Communications Technology Law*, Vol. 18(2), 201-234.
- Levin, Brian. (2002). Cyberhate: A Legal and Historical Analysis of Extremists' Use of Computer Networks in America. *American Behavioral Scientist*, Vol. 45(6), 958-988.
- Maras, Marie-Helen. *Cyberlaw and Cyberliberties*. Oxford University Press, forthcoming, 2020 (готовится к публикации)
- Schjølberg, Stein. (2016). A Geneva Convention or Declaration for Cyberspace. *VFAC Review*, No. 12, October 2016. Korean Institute of Criminology. http://www.cybercrimelaw.net/documents/Article_on_Geneva_Convention_or_Declaration_for_Cyberspace.pdf.
- Wall, David S. (2017). Crime, security and information communication technologies: The changing cybersecurity threat landscape and implications for regulation and policing (pp. 1075-1096). In R. Brownsword, E. Scotford and K. Yeung. (eds). *The Oxford Handbook of the Law and Regulation of Technology*, Oxford University Press.

Оценка учащихся

В дополнение к упражнениям, другими средствами для оценки учащихся, используемыми в данном модуле, являются обзорные вопросы и домашние задания.

Обзорные вопросы

Эти вопросы могут также использоваться для стимулирования групповых обсуждений во время лекции.

1. В чем заключается различие между нормами материального, процессуального и превентивного права в области борьбы с киберпреступностью?
2. Что представляют собой международные и региональные правовые документы в области борьбы с киберпреступностью?
3. Почему национальные, региональные и международные законы о киберпреступности являются необходимыми?
4. Почему необходимо гармонизировать законы о киберпреступности?
5. Являются ли договоры в области прав человека применимыми к контенту, сообщениям и поведению в сети Интернет? Почему вы так считаете?
6. Могут ли права человека ограничиваться на законных основаниях? При каких обстоятельствах?

Проверка знаний

1. Лицо выкладывает на «YouTube» видеоматериал, в котором оно призывает зрителей вытеснять представителей отдельной религиозной группы, бороться с ними и преподать им «урок».
Относится ли этот материал к высказываниям, защищаемым законодательством о свободе слова? Почему да или почему нет?
[Подсказка: дело *Белкасем против Бельгии* (2004)]

2. Гражданин Франции отрицает, что Холокост имел место.
Относится ли это мнение к высказываниям, защищаемым законодательством о свободе слова? Почему да или почему нет?
[Подсказка: дело *Гароди против Франции*, 2003]

Веб-упражнение: SHERLOC

Учащимся следует осуществить поиск в базе данных УНП ООН «SHERLOC» и определить страны, в которых законы о киберпреступности отстутствуют:
https://www.unodc.org/cld/v3/sherloc/
[Примечание: это упражнение должно быть выполнено до начала занятия].

Групповое упражнение: Нормы материального и процессуального права в области борьбы с киберпреступностью

До начала занятия учащихся следует в произвольном порядке распределить по группам, чтобы они могли выполнить задание до того, как все группы соберутся в классе. Каждой группе в произвольном порядке должна быть определена страна.

Поручите учащимся определить и рассмотреть законы о киберпреступности в странах, определенных их группам. После рассмотрения законов о киберпреступности учащимся следует выявить аспекты материального и процессуального права, охватываемые этими законами, в следующих сферах:

- криминализация киберпреступности
- следственные меры
- идентификация, сбор, распространение, использование и допустимость цифровых доказательств
- регулирование и риск
- юрисдикция и международное сотрудничество

Учащиеся могут обратиться к проекту доклада УНП ООН «Всестороннее исследование проблемы киберпреступности» для ознакомления с аспектами, включенными в эти сферы.

Дополнительные средства обучения

Вебсайты

- The Chairman's Blog. Cybercrime Law. http://www.cybercrimelaw.net/Cybercrimelaw.html.
- Управление Организации Объединенных Наций по наркотикам и преступности (УНП ООН), База данных по киберпреступности. https://sherloc.unodc.org/cld/v3/cybrepo/.

UNODC
United Nations Office on Drugs and Crime

Vienna International Centre, P.O. Box 500, 1400 Vienna, Austria
Tel.: (+43-1) 26060-0, Fax: (+43-1) 26060-3389, www.unodc.org