MIMUN 2017

Московская международная модель ООН

СПЧ

Совет по правам человека

Доклад эксперта

Право на неприкосновенность частной жизни в цифровой век

Содержание

Введение

«Все жертвы нарушений прав человека должны иметь возможность полагаться на Совет по правам человека как форум и плацдарм для действий».

- Пан Ги Мун, Генеральный секретарь ООН, 12 марта 2007 г., Открытие 4-й сессии Совета по правам человека

В Уставе ООН термин «права человека» упоминается семь раз, что делает поощрение и защиту прав человека основной целью и руководящим принципом работы Организации Объединенных Наций.[1] В 1948 году Всеобщая декларация прав человека – юридический документ, защищающий универсальные права человека – поместила вопросы прав человека в сферу международного права. Вместе с Международным пактом о гражданских и политических правах и Международным пактом об экономических, социальных и культурных правах эти три инструмента образуют так называемый Международный билль о правах человека.[2] Целый ряд международных договоров в области прав человека и другие документы, принятые начиная с 1945 года, расширили нормы международного права в области прав человека.

Совет по правам человека является межправительственным органом в системе Организации Объединенных Наций, отвечающим за содействие всеобщему уважению и защите всех прав человека по всему миру и за рассмотрение ситуаций, связанных с нарушением прав человека, а также подготовку соответствующих рекомендаций.[3]

В наше время цифровые технологии, такие как Интернет, смартфоны и другие устройства с поддержкой Wi-Fi сети безусловно стали частью повседневной жизни. Интернет стал мощным прорывом в научно-техническом прогрессе в области глобальной связи. Цифровые технологии как средства связи несомненно увеличивают возможности современного человека для выражения его мнения, помогают расширить круг широкомасштабного обсуждения любого вопроса, повысить качество доступа к информации. Хотя данные технологии упрощают жизни многих людей, они также дают возможность правительствам, компаниям и частным лицам перехватывать и собирать личные данные.

Эти инструменты в руках правозащитников являются несомненно важным орудием выявления нарушений прав человека. Они же в руках нарушителей закона становятся опасным оружием. Огромными темпами во всем мире растет такое явление, как киберпреступность. Кибершпионаж – методы получения секретной конфиденциальной информации без предварительного разрешения

---

1 Официальный сайт ООН URL: http://www.un.org/ru/sections/what-we-do/protect-human-rights/index.html

2 Международный билль о правах человека URL: http://www.un.org/ru/documents/decl_conv/hr_bill.shtml

3 Официальный сайт СПЧ URL: http://www.ohchr.org/ru/HRBodies/HRC/Pages/AboutCouncil.aspx

владельцев данной информации (личной, служебной или засекреченной): частных лиц, конкурентов, правительства[4] – ставит под угрозу личные и государственные интересы. Особую опасность представляет деятельность террористических групп в глобальной сети - кибертерроризм. Через сайты террористической направленности и посредством распространения экстремистской информации в интернет-пространстве, в ряды террористических групп вербуются новые члены. Кибермошенничество – один из видов киберпреступлений, целью которого является причинение материального или иного ущерба путем хищения личной информации пользователя[5] – кибершпионаж и кибертерроризм как угрозы национальной, конституционной, военной, экономической безопасности спровоцировали рост государственного контроля в информационном пространстве. Поэтому появляется много научных работ, реализуются проекты, направленные на противодействие компьютерной преступности и обеспечению информационной безопасности от современных киберугроз.

Сегодня государство обладает обширными возможностями слежения в глобальной сети, а упрощение системы хранения информации лишь облегчает поиск и перехват данных. На фоне стремительного развития коммуникационных технологий увеличиваются возможности и уменьшаются затраты на хранение полученного материала, что исключает материальные и фактические ограничения возможностей государства. Как показывают многочисленные примеры открытого или тайного наблюдения с использованием цифровых технологий во всем мире, сплошное слежение со стороны государства из исключительной меры перерастает в опасную привычку.[6] Многочисленные примеры показывают, что такое вмешательство со стороны государства не только является чрезвычайно опасным, но и может вовсе выйти из-под правительственного контроля, позволяя негосударственным субъектам следить и перехватывать информацию, имеющую непосредственную связь с частной жизнью человека. Такие примеры вызывают особое беспокойство за соблюдение прав человека.

В Организации Объединенных Наций важное место занимает вопрос защиты права на неприкосновенность частной жизни человека в глобальной сети. Несмотря на актуальность вопроса безопасности в киберпространстве, на остроту киберугроз, реальные и планомерные действия стали применяться всего несколько лет назад. Совет по правам человека ставит для себя особой задачей предлагать меры по сохранению безопасности личной жизни человека как в реальном, так и в виртуальном пространстве.[7]

---

4 https://ru.neospy.net/functions/work/Kibershpionazh/

5 http://evlevavg.3dn.ru/publ/informacionnaja_bezopasnost/roditeljam/kibermoshennichestvo/3-1-0-17

6 Доклад Управления Верховного комиссара ООН по правам человека A/HRC/27/37/ от 30 июня 2013 года URL: http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A_HRC_27_37_RUS.doc

7 Резолюция Совета ООН по правам человека A/HRC/RES/20/8 от 16 июня 2012 URL: http://www.un.org/ru/documents/ods.asp?m=A/HRC/RES/20/8

Базовая терминология

Частная жизнь – та область жизнедеятельности человека, которая относится к отдельному лицу, касается только его и не подлежит контролю со стороны общества и государства, если она не носит противоправный характер.[8]

Неприкосновенность частной жизни (юридич.) – гарантированные государством возможность и право человека самостоятельно контролировать информацию о самом себе, препятствовать разглашению сведений личного, интимного характера.[9]

Право на неприкосновенность частной жизни – право, по которому жизнедеятельность человека не может быть подвержена никакому вмешательству извне, подразумевающее под собой в том числе запрет на сбор, хранение, обработку и разглашение конфиденциальной информации без согласия данного человека. Право на неприкосновенность частной жизни нормативно закреплено рядом международных документов, прежде всего: Всеобщей декларацией прав человека, Международным пактом о гражданских и политических правах, Европейской конвенцией о защите прав человека и основных свобод.

Цифровые технологии - инструменты, которые используют дискретный метод, чтобы передать информацию, такую как письма или числа.[10]

Цифровой век (эпоха цифровых технологий) – эпоха, в которую основные средства производства приобретают цифровой характер. Термин возник в процессе глобального распространения цифровых технологий, поскольку этот процесс оказывает существенное воздействие на многие социально-культурные аспекты современной жизни.[11]

---

8 Комментарий КС РФ к Статье 23, части 1, Конституции Российской Федерации

9 Энциклопедия права. -2015.

10 URL: http://www.soyouwanna.com/define-digital-technology-22582.html

11 Толковый словарь по информационному обществу и новой экономике. 2007.

§1. Историческая ретроспектива

Мировому сообществу известно много открытий и изобретений, изменивших существование человека и повлиявших на различные мировые процессы. Интернет занимает почетное место в ряду величайших изобретений прошлого столетия. «Интернет первоначально был предназначен для военных целей, и исторически одной из основных причин его возникновения стало военное противостояние 60-х годов XX в. и угроза нанесения ракетно-ядерного удара. Интернет создавался и развивался как технологическая система информационного обмена между лицами, передающими и получающими информацию, по произвольным маршрутам через узловые соединения. При этом базовая технологическая архитектура интернета изначально зиждилась на саморегулировании, децентрализованной «сетевой» организационной модели, не предполагающей иерархии управления и идентификации лиц, получающих и передающих информацию, включая определение статуса таких лиц».[12]

Прогресс информационно-коммуникационных технологий (ИКТ) существенно улучшил общение и обмен информацией онлайн. Благодаря этому упростились процессы обмена, хранения, получения информации, возможность проведения различных переговоров и многое другое.

Но вместе с этим открылась и тёмная сторона прогресса: выяснилось, что новые устройства и технологии могут быть подвержены электронному слежению и перехвату информации. Последние открытия подтвердили, с какой высокой скоростью тайно разрабатываются новые технологии, причём не только с целью защиты от подобных угроз, но и непосредственного «шпионажа».

Первые примеры несанкционированного получения информации в киберпространстве относятся к концу 1990-х годов, как следствие развития Интернета и увеличения роли компьютеров во всех областях жизни. Так, Отдел защиты Пентагона свидетельствовал,[13] что еженедельно информационные узлы министерства подвергаются более чем 60 нападениям. Большинство из них совершают хулиганствующие хакеры, но во время бомбардировок Югославии в 1999 группы хакеров в России, Сербии и других странах целенаправленно атаковали принадлежащие американским государственным структурам серверы. В августе 1997 зафиксирован случай нападения тамильской кибергруппы «Черные тигры интернет» на электронную почту правительства Шри-Ланки.[14] В мае и июне 1998 протестующие против индийских ядерных испытаний хакеры уничтожили домашнюю страницу и электронную почту Индийского атомного исследова-

---

12 Кибербезопасность и управление интернетом: Документы и материалы для российских регуляторов и экспертов; М.Б. Касенова; Раздел 1, 8 стр.; – М.: Статут, 2013.

13 Терроризм и террористы. Исторический справочник. — Мн.: Харвест. Жаринов К. В. Под общ. ред. А. Е. Тараса. 1999.

14 Терроризм и террористы. Исторический справочник. — Мн.: Харвест. Жаринов К. В. Под общ. ред. А. Е. Тараса. 1999.

тельского центра в Вадхе.[15] В сентябре 1998 в Швеции одной из левых группировок был уничтожен сервер шведских правых радикалов.[16]

За последние годы было замечено немало примеров слежения и нарушения неприкосновенности личной жизни человека. Можно привести в пример компьютерный вирус «I Love You», который был разослан на почтовые ящики с Филиппин в ночь с 4 на 5 мая 2000 года. В общей сложности вирус поразил более 3 миллионов компьютеров по всему миру. Предполагаемый ущерб, нанесенный мировой экономике, оценивается в размере 10-15 млрд долларов. Как результат, данный вирус считается одним из самых вредоносных за все время существования интернет-сети.[17]

В 2013 году французская газета «Le Monde» сообщила, что сотрудниками Агентства Национальной Безопасности США (АНБ) велось прослушивание телефонных разговоров граждан Франции. Эти данные были предъявлены бывшим сотрудником американских спецслужб Эдвардом Сноуденом. Так, в период с 10 декабря 2012 года по 8 января 2013 года АНБ был осуществлен перехват 70,3 млн телефонных разговоров и посланных смс. Более того, на портале WikiLeaks были выложены документы, свидетельствующие о прослушивании спецслужбами США переговоров французских президентов - Жака Ширака, Николя Саркози и Франсуа Олланда. Согласно представленным документам с пометкой «совершенно секретно», американские спецслужбы как минимум в период с 2006 по 2012 годы проводили прослушивание мобильных телефонов президентов, ряда министров, высокопоставленных чиновников и дипломатов, включая посла Франции в США.[18]

Не менее известным политическим скандалом является также история прослушивания мобильного телефона канцлера ФРГ Ангелы Меркель. 23 октября 2013 года официальный представитель правительства ФРГ Штеффен Зайберт заявил, что немецкое правительство получило информацию о том, что спецслужбы США могли отслеживать мобильный телефон канцлера ФРГ Ангелы Меркель. Данные сведения вновь предоставил Эдвард Сноуден. Но уже 12 июня 2015 года был опубликован пресс-релиз федеральной прокуратуры ФРГ, в котором сообщалось, что дело о прослушивании телефона главы правительства ФРГ закрыто в связи с тем, что «обвинение не может быть доказано в судебном порядке.[19]

Можно также упомянуть несколько мощнейших хакерских атак, проведённых в последние годы. В январе 2012 года был закрыт сайт MegaUpload, в знак протеста группа Anonymous провела крупнейшую в истории DDoS-атаку, выполняемую одновременно с большого числа устройств, с применением LOIC, программы с открытым исходным кодом, предназначенной

---

15 *Там же.*

16 *Там же.*

17 *http://www.securitylab.ru/informer/240711.php*

18 *https://ria.ru/world/20131026/972834493.html*

19 *https://ria.ru/world/20131026/972834493.html*

для осуществления DDoS-атак. На несколько часов были выведены из строя сайты ФБР, Белого дома, Министерства юстиции, холдинга звукозаписи Universal Music Group, Американской ассоциации звукозаписывающих компаний, Американской ассоциации кинокомпаний, Американского управления авторского права. В апреле 2013 года Anonymous атаковали более 100 тысяч израильских сайтов. Общий ущерб от атаки сами хакеры оценили в 3 млрд долларов. Акция стала ответом на операцию «Облачный столп», прошедшую в ноябре 2012 года. Также во время украинского кризиса в марте 2015 года хакеры подвергли мощной атаке правительственные сайты РФ и сайты российских СМИ.[20]

Формат настоящего Доклада не позволяет перечислить больше примеров несанкционированного вмешательства. Но, как видно из приведенных исторических справок, на фоне активно развивающихся научно-технического и информационного прогрессов, в которых за календарный год возможности цифровых технологий могут меняться кардинально, кибератаки и кибершпионаж имеют далекие исторические корни, и носят не только политический, государственный характер, создают экономический ущерб частным компаниям, но и нарушают права на неприкосновенность личной жизни граждан разных государств.

Для защиты права на неприкосновенность личной жизни перед глобальной угрозой вмешательства извне различные государства объединяют свои силы в борьбе с ней. Этим занимаются многие международные организации: Организация Объединенных Наций, Совет Европы, Организация экономического сотрудничества и развития, Интерпол. Все эти организации вместе с различными многосторонними неформальными партнерствами играют важную роль в координации международных усилий, построении международного сотрудничества в борьбе с преступлениями в сфере высоких технологий.

---

20 https://www.bfm.ru/special/kaspersky

§2. Основные механизмы ООН, направленные на борьбу с угрозами неприкосновенности частной жизни в цифровой век

Существует несколько механизмов ООН, регулирующих частную жизнь человека и следящих за ее неприкосновенностью.

Начать стоит с Всеобщей декларации прав человека, принятой Резолюцией 217 A (III) Генеральной Ассамблеи ООН от 10 декабря 1948 года.[21] Статья 12 Всеобщей декларации раскрывает право на неприкосновенность частной жизни: «Никто не может подвергаться произвольному вмешательству в его личную и семейную жизнь, произвольным посягательствам на неприкосновенность его жилища, тайну его корреспонденции или на его честь и репутацию. Каждый человек имеет право на защиту закона от такого вмешательства или таких посягательств».

Кроме того, рассматривая право на неприкосновенность в цифровой век стоит упомянуть Международный пакт о гражданских и политических правах, принятый Резолюцией 2200 A (XXI) Генеральной Ассамблеи от 16 декабря 1966 года[22], а именно статью 17, которая описывает данный вопрос в пункте первом: «Никто не может подвергаться произвольному или незаконному вмешательству в его личную и семейную жизнь, произвольным или незаконным посягательствам на неприкосновенность его жилища или тайну его корреспонденции или незаконным посягательствам на его честь и репутацию», и его защиту в пункте втором: «Каждый человек имеет право на защиту закона от такого вмешательства или таких посягательств». Здесь же стоит отметить, что нормы международно-правовых актов о правах человека адресованы именно государству, которое может нарушить права человека в лице своих органов и должностных лиц. Однако нельзя утверждать, что негосударственные субъекты не совершают преступления, не нарушая самих прав личности. Государства берут на себя обязательство установления уголовной или административной ответственности за совершение соответствующих преступлений частными лицами.[23]

Особое внимание стоит обратить на Венскую декларацию и Программу действий, принятую на Всемирной конференции по правам человека в Вене 25 июня 1993 года.[24] В статье 11 декларации говорится о том, что прогресс в сфере цифровых технологий может повлечь негативные последствия неприкосновенности частной жизни человека, поэтому большую роль Всемирная конференция уделяет

---

21 Всеобщая декларация прав человека от 10 декабря 1948 года. URL: http://www.un.org/ru/documents/decl_conv/declarations/declhr

22 Международный пакт о гражданских и политических правах от 16 декабря 1966 года. URL: http://www.un.org/ru/documents/decl_conv/conventions/pactpol

23 Там же.

24 Венская декларация и Программа действий от 25 июня 1993 года. URL: http://www.un.org/ru/documents/decl_conv/declarations/viendec93.shtml

международному сотрудничеству в целях защиты и обеспечения уважения данного права личности в данной сфере.

В 2003 и 2005 годах под эгидой ООН состоялась Всемирная встреча на высшем уровне по вопросам информационного общества (ВВУИО).[25] На первом этапе саммита (Женева, 2003) была принята декларация принципов «Построение информационного общества – глобальная задача в новом тысячелетии», и Женевский план действий.[26] На втором этапе (Тунис, 2005) – «Тунисское обязательство» (WSIS-05/TUNIS/DOC/7-R)[27] и «Тунисская Программа для информационного общества» WSIS-05/TUNIS/DOC/6(Rev.1).[28] Эти документы призывали к новым формам солидарности, партнерства для создания открытого всем информационного общества; интернет стал для общества ресурсом глобального масштаба, и одним из основных пунктов повестки дня информационного общества должно стать регулирование его использования; контроль за использованием интернета касается как технических вопросов, так и вопросов государственной политики, в него должны быть вовлечены государственные и международные организации, а также все заинтересованные стороны.

Ключевой документ – Резолюция Совета ООН по правам человека A/HRC/RES/20/8[29] «Поощрение, защита и осуществление прав человека в Интернете» от 16 июня 2012 – подтвердил, 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, в соответствии со статьями 19 Всеобщей декларации прав человека и Международного пакта о гражданских и политических правах». В Резолюции «глобальный и открытый характер интернета» признается «одной из движущих сил ускорения прогресса по пути развития в его различных формах».

Резолюция «Защита правозащитников» Совета по правам человека ООН A/HRC/RES/22/6 от 12 апреля 2013 года[30] гласит: «новые формы коммуникации, включая распространение информации в режиме онлайн и офлайн, могут послужить правозащитникам полезным подспорьем в деле поощрения и обеспечения защиты прав человека».

В Докладе Специального докладчика ООН «По вопросу о праве на свободу мнений и их свободное выражение»

---

25 Всемирная встреча на высшем уровне по вопросам информационного общества URL: http://www.itu.int/net/wsis/index-ru.html

26 Всемирная встреча на высшем уровне по вопросам информационного общества URL: http://www.itu.int/net/wsis/index-ru.html

27 Тунисское обязательство WSIS-05/TUNIS/DOC/7-R от 15 ноября 2005 года URL: http://www.itu.int/net/wsis/docs2/tunis/off/7-ru.doc

28 Тунисская Программа для информационного общества» WSIS-05/TUNIS/DOC/6(Rev.1) от 18 ноября 2005 года URL: http://www.itu.int/net/wsis/docs2/tunis/off/6rev1-ru.pdf

29 Резолюция Совета ООН по правам человека A/HRC/RES/20/8 от 16 июня 2012 URL: http://www.un.org/ru/documents/ods.asp?m=A/HRC/RES/20/8

30 Резолюция по правам человека ООН A/HRC/RES/22/6 от 12 апреля 2013 года URL: http://www.ishr.ch/sites/default/files/article/files/hrc_resolution_22-6.pdf

Франка Ла Рю A/HRC/23/40[31] от 17 апреля 2013 года был приведен подробный отчет о том, как использование ИКТ может повлечь за собой нарушение права человека на неприкосновенность частной жизни. «Государства могут отслеживать передвижения отдельных мобильных устройств, распознавать личность любого человека через его мобильный телефон вместе с его местонахождением, перехватывать звонки и сообщения, используя разнообразные методы. Некоторые государства используют вневоздушные мобильные мониторы – Международный Идентификатор Мобильного Абонента (IMSI). Они могут быть установлены временно на определенной территории или постоянно (например, в аэропорту или в других пунктах пересечения границы). Эти ловушки имитируют вышку сотовой связи путем отправки сигналов на мобильные устройства и получения сигналов в ответ с целью распознавания уникального идентификационного модуля (SIM) карты всех абонентов мобильной связи в пределах задействованной территории». Также в Докладе сделан акцент на многоразовые обращения правительственных спецслужб в IT корпорации (Microsoft, Facebook, Google, Yahoo и др.) с целью получения конфиденциальных данных. Кроме этого, докладчик напомнил, что к настоящему времени государства постепенно исключили любые варианты анонимного общения, хотя ранее пользователи Интернета имели возможность анонимной передачи и доступа к информации, что было одним из преимуществ сети. Внимание также уделяется деятельности АНБ США. Докладчиком особо выделяется, что Агентство злоупотребляет запросами на предоставление им личных данных пользователей.

Резолюция Совета по правам человека ООН A/HRC/RES/24/5 от 8 октября 2013 года «Права на свободу мирных собраний и право на свободу ассоциации»[32] «напоминает государствам об их обязательстве уважать и в полной мере защищать права всех лиц на свободу мирных собраний и свободу ассоциации как в режиме онлайн, так и в режиме офлайн, в том числе в контексте выборов, и включая лиц, которые придерживаются не разделяемых большинством или отличных от общепринятых взглядов или убеждений, правозащитников, членов профсоюзов и других лиц, в том числе мигрантов, стремящихся осуществлять или поощрять эти права, и принимать все необходимые меры в целях обеспечения того, чтобы любые ограничения свободного осуществления прав на свободу мирных собраний и ассоциации соответствовали их обязательствам по международному праву прав человека».

Особо внимательно эта проблема стала рассматриваться в мировом сообществе после действий Эдварда Сноудена,

---

31 Доклад Специального докладчика ООН A/HRC/23/40 от 17 апреля 2014 года URL: http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf

32 Резолюция Совета по правам человека ООН A/HRC/RES/24/5 от 8 октября2013 URL: http://daccess-dds-ny.un.org/doc/UNDOC/GEN/G13/178/35/PDF/G1317835.pdf?OpenEleme

бывшего работника ЦРУ. «Агентство национальной безопасности США за последние пять лет многократно превышало свои полномочия в сфере сбора информации», - данное сообщение опубликовала газета The Washington Post 15 августа 2013 года[33] со ссылкой на результаты внутренней проверки АНБ, которые изданию предоставил Эдвард Сноуден. Как Совет по правам человека ООН, в который входит всего 47 государств, так и Генеральная Ассамблея ООН признают права человека онлайн. Это, в первую очередь, подтверждается в Резолюции Генеральной Ассамблеи ООН A/RES/68/167 «Право на неприкосновенность личной жизни в цифровой век» от 18 декабря 2013 года.[34] Этот документ не только подтверждает само право человека на неприкосновенность частной жизни в цифровой век, а также открытый характер Интернета и чрезвычайно быстрое развитие информационно-коммуникационных технологий, но и призывает все государства-члены ООН уважать данное право, принимать определенные меры для устранения нарушений права на неприкосновенность личной жизни, провести обзор уже существующих собственных процедур, практик и законодательств, касающихся данной сферы, с целью защиты этого права, и, кроме этого, учреждать новые и продолжать использовать старые внутренние надзорные механизмы.

Представленный на 69-й сессии Генеральной Ассамблеи Доклад Верховного Комиссара по правам человека Нави Пиллэй A/HRC/27/37 от 30 июня 2014 года[35] безусловно также требует внимания. Именно в этом документе были пояснены вопросы, касающиеся права на неприкосновенность частной жизни в цифровой век. В Докладе было раскрыто понятие права на защиту от произвольного или незаконного вмешательства в личную и семейную жизнь: «все программы по наблюдению за коммуникацией должны проводиться на основании доступных для всеобщего ознакомления законодательных норм, которые, в свою очередь, должны соответствовать конституционному режиму государства и международному праву прав человека», посягательства на неприкосновенность жилища или тайну корреспонденции, а также были даны ответы на вопрос, как происходит защита закона: «Защита закона» должна быть обеспечена посредством надежных процессуальных гарантий, включая эффективные институциональные механизмы с необходимыми ресурсами», и на вопрос, кто и где находится под данной защитой: «требуется уважать и обеспечивать признаваемые в [Международном] Пакте [о Гражданских и Политических правах] права всем

---

33 https://www.washingtonpost.com/world/national-security/nsa-broke-privacy-rules-thousands-of-times-per-year-audit-finds/2013/08/15/3310e554-05ca-11e3-a07f-49ddc7417125_story.html

34 Резолюцию Генеральной Ассамблеи A/RES/68/167 от 18 декабря 2013 года URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N13/449/49/PDF/N1344949.pdf?OpenElement

35 Доклад Верховного Комиссара по правам человека A/HRC/27/37 от 30 июня 2014 года. URL: http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A_HRC_27_37_RUS.doc

лицам, находящимся в пределах их [государств-участников] территории, и всем лицам, находящимся под их [государств-участников] юрисдикцией. Это означает, что государство-участник обязано уважать и обеспечивать любому лицу, находящемуся в пределах компетенции или эффективного контроля этого государства-участника, права, признаваемые в [Международном] Пакте [о Гражданских и Политических правах], даже если лицо не находится на территории государства-участника». Здесь же упомянуты процессуальные гарантии, которые должны обеспечивать защиту закона, и эффективный надзор в данной сфере. Верховный Комиссар также раскрывает понятие права на эффективное средство правовой защиты: «Эффективные средства правовой защиты, как правило, имеют некоторые общие характерные особенности. Во-первых, такие средства правовой защиты должны быть известны и доступны всем, кто утверждает, что их права были нарушены [...] Во-вторых, эффективные средства правовой защиты будут включать в себя тщательное оперативное и беспристрастное расследование предполагаемых нарушений», а также судебные, законодательные и административные формы, которые эти эффективные средства могут принимать. Хотя факт того, что прослеживание с учетом законных и международных норм признается эффективным и нужным средством законного обеспечения порядка или сбора информации, обеспокоенность по поводу массовой слежки все же присутствует в связи с угрозой произвольного нарушения права на неприкосновенность частной жизни. В своем Докладе Управление Верховного Комиссара по правам человека рассмотрело нормы международного права, предусмотренные для защиты прав человека, со стороны неприкосновенности личной жизни. Было раскрыто определение «вмешательства в личную жизнь» в контексте онлайновых сообщений: «таким образом, вмешательством в личную жизнь становится само существование программы массового слежения», определение «произвольного и незаконного» вмешательства в этом же контексте и вопрос о том, в каких ситуациях и чьи права подлежат защите.

Одним из важнейших документов, требующих рассмотрения, является Резолюция Генеральной Ассамблеи ООН «Право на неприкосновенность личной жизни в эпоху цифровых технологий» A/RES/69/166 от 18 декабря 2014 года.[36] В ней отмечен тот факт, что слежение за частной жизнью человека онлайн посредством цифровых технологий должно осуществляться только в рамках международно-правовых норм и на такой правовой базе, которая была бы ясной, четкой, прозрачной и всесторонней. Более того, любое вмешательство в личную жизнь должно быть законным, а государства-участники Международного пакта о гражданских и политических правах должны следовать конкретным путям с целью принятия законов или других методов, которые могут быть необходимыми для осуществления прав, указанных в Международном

---

36 Резолюция Генеральной Ассамблеи ООН A/RES/69/166 от 18 декабря 2014 года URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N14/707/06/PDF/N1470706.pdf

Пакте. Одним из важнейших пунктов данной резолюции является признание государствами-членами ООН глобального и открытого характера Интернета и чрезвычайно быстрого развития ИКТ, как одной из основных сил ускорения информационно-технического прогресса. Генеральная Ассамблея, помимо всего прочего, призывает мировое сообщество принимать необходимые меры для искоренения нарушений, связанных с правом на неприкосновенность личной жизни, создавать условия для предотвращения таких нарушений, а также провести пересмотр уже существующих методов и способов слежения, которые могут касаться слежения за личными сообщениями (включая массовое слежение), их перехват и сбор в целях защиты права на неприкосновенность частной жизни путем обеспечения всестороннего выполнения всех обязательств, касающихся международного права прав человека. Генассамблея также призывает учреждать новые и продолжать использовать старые действенные методы и механизмы регулирования и судебного, административного и/или парламентского контроля за соблюдением права на неприкосновенность. В соответствии с данным документом государства-члены ООН должны предоставлять доступ к средствам защиты тем лицам, чье право на неприкосновенность было нарушено вследствие незаконного слежения средствами правовой защиты в соответствии с международно-правовыми обязательствами в области прав человека. Кроме этого, Генеральная Ассамблея призывает Совет по правам человека продолжать активно обсуждать данный вопрос для выявления и уточнения принципов, стандартов и передовой практики в области поощрения и защиты права на неприкосновенность личной жизни и рассмотреть возможность установления с этой целью специальной процедуры.

Кроме того, вопросы слежки также затрагивались и в подготовленном Докладе A/69/397 от 23 сентября 2014 года[37] Специального докладчика по вопросам защиты прав человека в условиях борьбы с терроризмом Бена Эммерсона. Основанием для Доклада являются мероприятия, осуществленные Специальным докладчиком в период с 17 декабря 2013 года по 31 июля 2014 года, а именно участие в различных дискуссиях, семинаре экспертов и пресс-конференции. В нем он заключает, что обязательства государств в соответствии со статьей 17 Международного пакта о Гражданских и Политических правах включают в себя обязательство уважать частную жизнь и безопасность цифровой связи. Подразумевается, что люди имеют право делиться информацией и идеями друг с другом без вмешательства государства, совершенно точно зная, что их сообщение будет прочитано только непосредственными получателями. Меры, которые вмешиваются в это право должны быть санкционированы внутригосударственным правом, которое в свою очередь должно быть четким и прозрачным и соответствовать требованиям Пакта. Они также должны преследовать лишь законную цель. Специальный Докладчик соглашается с Верховным комиссаром по правам человека, что су-

37 *https://ilsa.org/jessup/jessup16/Batch%202/A69397.pdf*

ществует реальная необходимость для государств, использующих в этих целях цифровые технологии пересмотреть и обновить национальное законодательство, чтобы гарантировать соответствие нормам международного права. В том случае, когда право на неприкосновенность частной жизни всего цифрового сообщества находится под угрозой, необходимо ни что иное как подробное и ясное законодательство.

В Докладе Управления Верховного комиссара ООН по правам человека «Резюме обсуждения на дискуссионном форуме вопроса о праве на неприкосновенность частной жизни в цифровой век» A/HRC/28/39 от 19 декабря 2014 года[38] утверждается следующее: на дискуссионном форуме по вопросу о праве на неприкосновенность частной жизни, прошедшем 12 сентября 2014 года, участники дискуссии пришли к заключению, что технический прогресс может создать новые проблемы для действующего законодательства. «Вместе с тем необходимо более действенное осуществление международных норм, касающихся права на неприкосновенность частной жизни, на уровне государств с помощью необходимого законодательства и более действенных гарантий и контроля». Полномочия правительств в получении доступа к связанным с общением данным должны быть основаны на ясном и прозрачном законодательстве, учитывающем технологический прогресс и соответствующим международным нормам и стандартам в сфере прав человека.

В марте 2015 г. Совет ООН по правам человека резолюцией A/HRC/28/L.27 Совета по Правам Человека ООН «Право на неприкосновенность личной жизни в цифровой век»[39] учредил должность Специального Докладчика по вопросу права на неприкосновенность личной жизни. Круг его функций определяет в том числе: проводить исследования и отчитываться по ситуации в какой-либо стране или определенной теме касательно прав человека. В июле 2015 года Совет по Правам человека назначил профессора Джозефа Кэннэйтаки (Мальта) первым в истории Специальным Докладчиком по праву на неприкосновенность частной жизни. Согласно Резолюции Совета по правам человека «Право на неприкосновенность частной жизни в цифровой век» A/HRC/RES/28/16 от 01 апреля 2015 года[40] в обязанности Специального Докладчика входят функции, некоторыми из которых являются следующие: сбор актуальной информации о событиях, происходящих как на международном, так и на государственном уровнях; изучение тенденций, событий и проблем, возникающих относительно права на неприкосновенность частной жизни и представление рекомендаций, с целью продвижения и защиты данного права, включая проблемы, являющиеся результатом использования новых

38 Доклад Управления Верховного комиссара ООН по правам человека A/HRC/28/39 от 19 декабря 2014 года URL: http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session28/Documents/A_HRC_28_39_ENG.doc

39 Революция СПЧ ООН A/HRC/28/L.27от 5 марта 2015 года URL: https://documents-dds-ny.un.org/doc/UNDOC/LTD/G15/061/66/PDF/G1506166.pdf

40 Резолюции Совета по правам человека A/HRC/RES/28/16 от 01 апреля 2015 года URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/G15/068/80/PDF/G1506880.pdf

технологий; представление Совету по правам человека предложений и рекомендаций в отношении основных препятствий, стоящих на пути исполнения данного права, включая возникающие препятствия в цифровой век; повышение осведомленности относительно важности продвижения и защиты права на неприкосновенность частной жизни, включая проблемы, возникающие в цифровой век; предоставление годового отчета Совету по Правам человека и Генеральной Ассамблее ООН на тридцать первой сессии и семьдесят первой сессии соответственно.

В своем Докладе от 8 марта 2016 года A/HRC/31/64[41] Специальный Докладчик отметил задачу формулировки универсального определения частной жизни как приоритетный пункт для него в будущем. Здесь также определен ряд вопросов, которые Специальный Докладчик планирует поставить в приоритет и решить на основе консультаций с заинтересованными сторонами. Специальный Докладчик также выработал план, состоящий из десяти частей, в общих чертах описывающий определенные цели, выполнения которых он намеревается добиться. Некоторыми пунктами в этом списке являются: повышение осведомленности о частной жизни среди граждан; комплексный подход к юридическим, процедурным и дополнительным гарантиям и средствам защиты права; изучение киберпространства (пространства, которое симулируется и опосредуется электронными устройствами[42]), киберконфиденциальности (необходимости предотвращения утечки (разглашения) какой-либо информации в киберпространстве), кибершпионажа, кибервойны и кибермира.

Кроме этого стоит отметить вклад Международного союза электросвязи (МСЭ) в решение данного вопроса. Так, к примеру, в ходе Полномочной конференции МСЭ в Пусане 20 октября – 7 ноября 2014 г. был принят ряд резолюций касательно кибербезопасности и неприкосновенности частной жизни. Резолюция 130 (пересм. Пусан, 2014г.)[43] «Усиление роли МСЭ в укреплении доверия и безопасности при использовании информационно-коммуникационных технологий» предлагает государствам-членам тесно взаимодействовать в рамках усиления регионального и международного сотрудничества и, учитывая Резолюцию 45 (пересм. Дубай, 2014 г.)[44] «Механизмы совершенствования сотрудничества в области кибербезопасности, включая противодействия спаму и борьбу с ним», с тем чтобы укреплять доверие и безопасность при использовании информационно-коммуникационных технологий в целях снижения рисков и угроз, решает вносить вклад в

---

41 Доклад Специального Докладчика Совета по правам человека ООН от 8 марта 2016 года A/HRC/31/64 URL: http://www.ohchr.org/Documents/Issues/Privacy/A-HRC-31-64.doc

42 Социологический словарь. — М.: Экономика. Н. Аберкромби, С. Хилл, Б.С. Тернер. 2004.

43 Заключительные акты Полномочной конференции МСЭ (Пусан, 2014 г.) URL: http://www.itu.int/dms_pub/itu-s/oth/02/01/S02010000544001PDFR.PDF

44 Там же.

дальнейшее укрепление основ доверия и безопасности в соответствии с ролью МСЭ как ведущей содействующей организации по направлению деятельности Всемирной встречи на высшем уровне по вопросам информационного общества. Резолюция 174 (пересм. Пусан, 2014 г.)[45] «Роль МСЭ в связи с вопросами международной государственной политики, касающимися риска незаконного использования информационно-коммуникационных технологий», отмечая большое значение информационно-коммуникационных технологий для социально-экономического развития стран, в частности развивающихся стран, благодаря созданию новых услуг общего пользования, которые содействуют доступу населения к информации и увеличению прозрачности государственных администраций и могут быть полезными для осуществления мониторинга и наблюдения за изменением климата, управления природными ресурсами и сокращения риска стихийных бедствий, предлагает государствам-членам и всем прочим заинтересованным сторонам продолжать диалог на региональном и национальном уровнях в целях поиска взаимоприемлемых решений, а также предлагает Генеральному секретарю осуществлять сбор и распространение информации о передовых мерах, принимаемых государствами-членами для предотвращения незаконного использования ИКТ, и оказывать помощь заинтересованным государствам-членам, в соответствующих случаях.

Среди специализированных организаций ООН особо стоит отметить ЮНЕСКО и ее работу по вопросу права на неприкосновенность личной жизни. ЮНЕСКО получает поддержку Организации Объединенных Наций с 1995 года, принимая во внимание важнейшую роль не только этических аспектов информационного общества в рамках мандата ЮНЕСКО, но и ряд проводимых мероприятий, исследований, публикаций, докладов и других направлений деятельности в данной области. ЮНЕСКО привержена цели обеспечения в полном объеме прав человека и основных свобод, провозглашенных во Всеобщей декларации прав человека, применительно к киберпространству.[46] Резолюция 15, принятая Генеральной конференцией на ее 37-й сессии призывает государства-члены в полной мере участвовать в этом процессе и приложить все усилия, в том числе за счет внебюджетных взносов, для финансирования дополнительных встреч и иных мероприятий. Как подчеркивалось в заключительном исследовании ЮНЕСКО под названием «Основные аспекты укрепления инклюзивных обществ знаний. Доступ к информации и знаниям, свобода выражения мнений, неприкосновенность личной жизни и этические аспекты глобального интернета»[47], «ЮНЕСКО должна работать с другими участниками процесса для «объединения усилий» всех заинте-

45 *Там же.*

46 *Руководство Генеральной конференции ЮНЕСКО URL: http://unesdoc.unesco.org/images/0012/001255/125590r.pdf*

47 *Основные аспекты укрепления инклюзивных обществ знаний URL: http://unesdoc.unesco.org/images/0023/002325/232563r.pdf*

ресованных сторон в сфере интернета». Проведенные для данного исследования анализ и консультации укрепили растущее осознание влияния цифровой революции на все сферы общественной и частной жизни.

§3. Основные препятствия на пути решения данной проблемы. Возможные пути преодоления угроз

Наиболее детально данные препятствия удалось определить Верховному комиссару ООН по правам человека госпоже Нави Пиллэй 20 сентября 2013 года в ходе своих Вступительных замечаний на параллельном мероприятии в рамках 24-й сессии Совета по правам человека «Как защитить право на неприкосновенность частной жизни в эпоху цифровых технологий?».[48] Она описала пять основных проблем, стоящих на пути защиты неприкосновенности частной жизни.

В первую очередь, она отметила препятствие, связанное с тем, каким образом судебные, законодательные и административные органы гарантируют право на неприкосновенность. Она подчеркнула, что действенные национальные правовые нормы чрезвычайно важны для обеспечения полной безопасности от произвольного вмешательства, однако национальное законодательство, освещающее изменения в цифровых технологиях и меры слежения, которые могут быть применены благодаря данным изменениям, еще не было принято.

Второе препятствие, по мнению госпожи Пиллэй, заключается в том, что даже если и существует достаточное

---

48 Вступительные замечания Верховного комиссара ООН по правам человека г-жи Нави Пиллэй URL: http://www.ohchr.org/RU/NewsEvents/Pages/DisplayNews.aspx?NewsID=13758&LangID=R

законодательство и регулирующие механизмы, отсутствие эффективного исполнения влечет за собой и отсутствие должной подотчетности в отношении незаконных вмешательств в личную жизнь.

Третья проблема имеет дело со стремительным прогрессом в области ИКТ, а также со слиянием общественной и частной жизней, вследствие чего стало необходимым призывать мировое сообщество к обращению внимания на масштаб права на неприкосновенность частной жизни.

В-четвертых, Верховный комиссар считает важным определить критерии законности слежения, которое осуществляют спецслужбы, и которое все больше пересекает границу права на неприкосновенность личной жизни. Правительства обладают правом на сбор и защиту некоторой информации (к примеру, касающейся каких-либо операций, методов работы служб разведки) или на ограничение к ней доступа общественности с целью соблюдения законных интересов национальной безопасности, однако право на неприкосновенность частной жизни не должно быть нарушено.

Пятое препятствие имеет дело с обязанностью предпринимателей придерживаться права на неприкосновенность личной жизни в цифровой век. Перед мировым сообществом встает вопрос «Как обеспечить контроль, чтобы корпорации в области коммуникаций и технологий соблюдали право на неприкосновенность частной жизни и другие связанные с ним права человека?»

Основной проблемой на пути решения угроз неприкосновенности частной жизни являются либо политические мотивы, либо корыстные цели, преследуемые злоумышленниками. Так, ежегодно на государственные интернет-ресурсы РФ, США и КНР совершается в среднем по 70 миллионов кибератак.[49] При этом диверсионные технологии становятся, с одной стороны, все более изощренными, а с другой – все более доступными даже для непрофессионалов. Из этого можно сделать вывод, что решать эти проблемы необходимо, прежде всего, на основе совершенствования культуры информационной безопасности на государственном уровне. К сожалению, этот процесс идет сложно и значительно медленнее нарастания самих угроз, для устойчивого же и прогрессивного использования ИКТ необходимы новые механизмы, выработанные совместно мировым сообществом.

В заключительном исследовании ЮНЕСКО[50] был предложен ряд возможных путей преодоления вышеперечисленных угроз. В течение консультаций были предложены следующие меры поощрения секретности информации:

- «Поддержка исследований влияния цифрового перехвата, сбора, хранения и использования данных, а также других новых тенденций на неприкосновенность личной жизни;

---

49 https://digital.report/rol-rossii-v-protsesse-obespecheniya-mezhdunarodnoy-informatsionnoy-bezopasnosti/

50 Основные аспекты укрепления инклюзивных обществ знаний ЮНЕСКО URL: http://unesdoc.unesco.org/images/0023/002325/232563r.pdf

- Подтверждение применения права на неприкосновенность личной жизни и соблюдение этого права как вне сети, так и в интернете в соответствии со статьей 12 Всеобщей декларации прав человека и статьей 17 Международного пакта о гражданских и политических правах и поддержка по мере необходимости усилий, связанных с осуществлением резолюции A/RES/69/166 Генеральной Ассамблеи ООН о праве на неприкосновенность личной жизни в цифровую эпоху;
- Рекомендации государствам взять на себя обязательство установления уголовной или административной ответственности за совершение соответствующих преступлений частными лицами;
- Поддержка распространения передовой практики и усилий государств-членов и других заинтересованных сторон, направленных на решение вопросов безопасности и неприкосновенности личной жизни в Интернете в соответствии с их международными обязательствами в области прав человека и учет в этом отношении ключевой роли частного сектора;
- Признание роли анонимности и шифрования в качестве средств защиты неприкосновенности личной жизни и свободы выражения мнений и содействие диалогу по этим вопросам;
- Обмен передовой практикой в области законного, необходимого и пропорционального сбора личной информации, при котором число идентификаторов личности в данных сводится к минимуму;
- Поощрение инициатив, повышающих осведомленность населения о праве на неприкосновенность личной жизни в сетевом пространстве и изменяющихся способах сбора, использования, хранения информации и обмена данными, используемых правительствами и коммерческими структурами, а также о методах использования цифровых средств обеспечения безопасности для защиты права пользователей на неприкосновенность личной жизни;
- Поощрение инициатив в области защиты личных данных, которые гарантируют пользователям безопасность, уважение их прав и механизмы правовой защиты, а также способствуют повышению доверия к новым цифровым услугам».

Заключение

28 августа 2013 выступая в Лейденском университете в Нидерландах, Генеральный Секретарь ООН выразил обеспокоенность по поводу неоправданного использования практики слежки за людьми, что приводит к серьезным нарушениям основных свобод, в том числе права на неприкосновенность частной жизни. Он подчеркнул, что люди не хотят, чтобы их частные контакты становились предметом незаконной и безосновательной проверки со стороны государства. «Позвольте мне быть предельно ясным. Опасения по поводу национальной безопасности и преступности могут оправдывать исключительное и ограниченное использование программ наблюдения. Но наблюдения без гарантии защиты права на частную жизнь подрывают основные свободы»,

- сказал Пан Ги Мун, говоря со студентами и преподавателями о защите прав человека и основных свобод.[51]

Мировому сообществу стоит обратить особое внимание на то, что незаконное слежение, перехват информации, как и незаконный сбор персональных данных являются действиями, которые вызывают опасения и нарушают права на неприкосновенность частной жизни и права на свободу выражения мнений. Эти действия так же могут представлять угрозу для основ демократического общества. Если в некоторых случаях сбор и защита определенных видов информации и могут быть оправданы соображениями государственных интересов, государства при этом должны обеспечить полное соблюдение своих обязательств, вытекающих из международного права в области прав человека.

Вклад Организации Объединенных Наций в соблюдение права на неприкосновенность частной жизни отражается в Резолюциях и Докладах организации и ее органов, в создании необходимых институтов, мониторинговых центров, проведении мероприятий, направленных на улучшения в данном вопросе. В результате принятых мер, наблюдается позитивная тенденция. Для более эффективного решения проблемы необходимо консолидировать усилия мирового сообщества и более эффективно действовать в рамках созданных институтов.

Задача соблюдения права на неприкосновенность частной жизни в эпоху цифровых технологий является задачей, находящейся *на границе интересов человека, государства и бизнеса.*

Цифровая среда предлагает государствам и частным лицам огромные возможности, приносящие видимые результаты в вопросах национальной безопасности и извлечения выгоды. Однако ценой этому является систематическое нарушение гражданских прав и постоянно нависающая угроза эскалации данной деятельности, особенно в странах, где только происходит становление гражданского общества и правового государства.

Основополагающее значение для пользователей интернета имеет вопрос о том, насколько они могут верить тому, что их права будут соблюдены, в том числе их право на разумные ожидания в

---

51 Центр новостей ООН. URL: http://www.un.org/russian/news/ story.asp?NewsID=20113#.UmP45UARfX-

сфере обеспечения конфиденциальности. Отсутствие доверия может привести к сокращению участия пользователей в развитии интернета, что ограничит его универсальность. Пользователи должны знать о *границе права, которая не может быть нарушена, и методах, с помощью которых они могут защитить свою личную жизнь онлайн. В то же время, сами пользователи также должны соблюдать конфиденциальность других пользователей интернета, и в этом смысле важная задача стоит перед Организацией Объединенных Наций и входящими в ее состав органами.*

Предлагаемые методы защиты права на неприкосновенность частной жизни должны идти в ногу с научно-техническим и информационным прогрессами. Государства-члены должны продолжать работу по реализации уже предложенных *механизмов урегулирования и в то же время договариваться об инновационных методах, соответствующих уровню цифровых технологий.*

В современных условиях информатизации, компьютеризации (т. н. эпохе цифровых технологий) очевидна уязвимость соблюдения этого права. Нерешенным остается вопрос о толковании данной нормы. В связи с этим мировому сообществу необходимо выяснить, каким образом данная проблема должна быть решена.

Что является наиболее значимым – свобода или защищенность? Где должна проходить граница между конфиденциальностью и доступностью информации? Какие этические и правовые нормы в киберпространстве стоит установить относительно права человека на неприкосновенность частной жизни? На эти вопросы и должно ответить мировое *сообщество.*

Источники

1. Официальный сайт ООН URL: http://www.un.org/ru/sections/what-we-do/protect-human-rights/index.html
2. Международный билль о правах человека URL: http://www.un.org/ru/documents/decl_conv/hr_bill.shtml
3. Официальный сайт СПЧ URL: http://www.ohchr.org/ru/HRBodies/HRC/Pages/AboutCouncil.aspx
4. Доклад Верховного комиссара ООН по правам человека A/HRC/27/37/ от 30 июня 2013 года URL: http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A_HRC_27_37_RUS.doc
5. URL: http://www.soyouwanna.com/define-digital-technology-22582.html
6. http://www.securitylab.ru/informer/240711.php
7. https://ria.ru/world/20131026/972834493.html
8. https://ria.ru/world/20131026/972834493.html
9. https://www.bfm.ru/special/kaspersky
10. Всеобщая декларация прав человека от 10 декабря 1948 года. URL: http://www.un.org/ru/documents/decl_conv/declarations/declhr
11. Международный пакт о гражданских и политических правах от 16 декабря 1966 года. URL: http://www.un.org/ru/documents/decl_conv/conventions/pactpol
12. Венская декларация и Программа действий от 25 июня 1993 года. URL: http://www.un.org/ru/documents/decl_conv/declarations/viendec93.shtml
13. Всемирная встреча на высшем уровне по вопросам информационного общества URL: http://www.itu.int/net/wsis/index-ru.html
14. Тунисское обязательство WSIS-05/TUNIS/DOC/7-R от 15 ноября 2005 года URL: http://www.itu.int/net/wsis/docs2/tunis/off/7-ru.doc
15. Тунисская Программа для информационного общества» WSIS-05/TUNIS/DOC/6(Rev.1) от 18 ноября 2005 года URL: http://www.itu.int/net/wsis/docs2/tunis/off/6rev1-ru.pdf
16. Резолюция Совета ООН по правам человека A/HRC/RES/20/8 от 16 июня 2012 URL: http://www.un.org/Depts/german/menschenrechte/a-hrc-res-20-8.pdf
17. Резолюция по правам человека ООН A/HRC/RES/22/6 от 12 апреля 2013 года URL: http://www.ishr.ch/sites/default/files/article/files/hrc_resolution_22-6.pdf
18. Доклад Специального докладчика ООН A/HRC/23/40 от 17 апреля 2014 года URL: http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf
19. Резолюция Совета по правам человека ООН A/HRC/RES/24/5 от 8 октября2013 URL: http://daccess-dds-ny.un.org/doc/UNDOC/GEN/G13/178/35/PDF/G1317835.pdf?OpenEleme
20. https://www.washingtonpost.com/world/national-security/nsa-broke-privacy-rules-thousands-

of-times-per-year-audit-finds/2013/08/15/3310e554-05ca-11e3-a07f-49ddc7417125_story.html

21. Резолюцию Генеральной Ассамблеи A/RES/68/167 от 18 декабря 2013 года URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N13/449/49/PDF/N1344949.pdf?OpenElement

22. Резолюция Генеральной Ассамблеи ООН A/RES/69/166 от 18 декабря 2014 года URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N14/707/06/PDF/N1470706.pdf

23. https://ilsa.org/jessup/jessup16/Batch%202/A69397.pdf

24. Доклад Управления Верховного комиссара ООН по правам человека A/HRC/28/39 от 19 декабря 2014 года URL: http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session28/Documents/A_HRC_28_39_ENG.doc

25. Резолюция СПЧ ООН A/HRC/28/L.27 от 5 марта 2015 года URL: https://documents-dds-ny.un.org/doc/UNDOC/LTD/G15/061/66/PDF/G1506166.pdf

26. Резолюции Совета по правам человека A/HRC/RES/28/16 от 01 апреля 2015 года URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/G15/068/80/PDF/G1506880.pdf

27. Доклад Специального Докладчика Совета по правам человека ООН от 8 марта 2016 года A/HRC/31/64 URL: http://www.ohchr.org/Documents/Issues/Privacy/A-HRC-31-64.doc

28. Заключительные акты Полномочной конференции МСЭ (Пусан, 2014г.) URL: http://www.itu.int/dms_pub/itu-s/oth/02/01/S02010000544001PDFR.PDF

29. Руководство Генеральной конференции ЮНЕСКО URL: http://unesdoc.unesco.org/images/0012/001255/125590r.pdf

30. Основные аспекты укрепления инклюзивных обществ знаний ЮНЕСКО URL: http://unesdoc.unesco.org/images/0023/002325/232563r.pdf

31. Вступительные замечания Верховного комиссара ООН по правам человека URL: http://www.ohchr.org/RU/NewsEvents/Pages/DisplayNews.aspx?NewsID=13758&LangID=R

32. https://digital.report/rol-rossii-v-protsesse-obespecheniya-mezhdunarodnoy-informatsionnoy-bezopasnosti/

33. Центр новостей ООН. URL: http://www.un.org/russian/news/ story.asp?NewsID=20113#.UmP45UARfX-

34. https://ru.neospy.net/functions/work/Kibershpionazh/

35. http://evlevavg.3dn.ru/publ/informacionnaja_bezopasnost/roditeljam/kibermoshennichestvo/3-1-0-17

Литература

1. Комментарий КС РФ к Статье 23, части 1, Конституции Российской Федерации

2. Энциклопедия права. -2015.

3. Толковый словарь по информационному обществу и новой экономике. 2007.

4. Кибербезопасность и управление интернетом: Документы и материалы для российских регуляторов и экспертов; М.Б. Касенова; Раздел 1, 8 стр.; – М.: Статут, 2013.

5. Терроризм и террористы. Исторический справочник. — Мн.: Харвест. Жаринов К. В. Под общ. ред. А. Е. Тараса. 1999.

6. Социологический словарь. — М.: Экономика. Н. Аберкромби, С. Хилл, Б.С. Тернер. 2004.

Контакты

Секретариат

Адрес:

119454, Москва, Проспект Вернадского,
76, Спортцентр МГИМО, комната №36

Телефон / факс:

+7 (495) 434-07-10
+7 (495) 434-30-11

vk.com/mimun2017

@mimun2017

fb.com/awesome.mimun

@mimun2017

secretariat@modelun.ru

modelun.ru