ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«БЕЛГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ»
(Н И У « Б е л Г У »)

ЮРИДИЧЕСКИЙ ИНСТИТУТ

КАФЕДРА КОНСТИТУЦИОННОГО И МЕЖДУНАРОДНОГО ПРАВА

Международное сотрудничество государств в сфере информационной безопасности

Выпускная квалификационная работа
обучающегося по специальности
40.05.01 Правовое обеспечение национальной безопасности
очной формы обучения, группы 01001312
Бондаревой Алины Владимировны

Научный руководитель:
к.ю.н., доцент
Никонова Л.И.

Рецензент:
к.ю.н., доцент кафедры теории и истории государства и права Белгородского университета кооперации, экономики и права
Шабалина Е.И.

БЕЛГОРОД 2018

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Актуальность вопросов международного сотрудничества государств в сфере информационной безопасности обусловлена зависимостью всех сфер жизни современного общества от информационных технологий. Распространение новейших информационных технологий и глобальных средств коммуникации, с одной стороны, открывает колоссальные возможности для развития общества, а с другой, порождает многочисленные проблемы политического, социально-экономического, научно-технического, военного и правового характера. Причем решение этих проблем возможно только совместными усилиями международного сообщества на основе взаимовыгодного сотрудничества между государствами.

Акцентирует внимание на необходимости сотрудничества государств в данной сфере Президент России В.В. Путин: «уровень угроз в информационном пространстве повышается, число рисков увеличивается, а негативные последствия разного рода кибератак носят уже не локальный, а действительно глобальный характер и масштаб. Формирование международной системы информационной безопасности соответствует сегодня не только национальным интересам России, но и интересам всего мирового сообщества»[1].

Вопросы информационной безопасности исследуется как в теоретическом аспекте, так и в контексте социально-психологической, правовой, экономической и технической проблематики. В связи с чем, **теоретическая основа работы** сформирована с учетом научных трудов как ученых в области международного публичного права, так и политологов, криминалистов, специалистов в области информационных технологий: П.В. Агапова, С.В. Баринова, Д.Г. Грибкова, А.В. Даниленкова, Е.С. Зиновьевой, Т.В Закупень, Е.И. Ильичева, О.В. Казарина, Е.А. Меркурьевой, М.С. Соколова и др.

Нормативно-правовую базу исследования составляют как международные и региональные договоры, конвенции и резолюции, так и националь-

[1] Выступление Президента РФ В.В. Путина на заседании Совета Безопасности 26 октября 2017 г., Москва, Кремль [Электронный ресурс] // Официальный сайт Президента России; URL: http://www.kremlin.ru/events/president/news/55924 (дата обращения 28.02.2018)

ные нормативно-правовые акты, регулирующие вопросы обеспечения информационной безопасности.

Объектом исследования являются урегулированные нормами права общественные отношения, складывающиеся в сфере международного сотрудничества государств по обеспечению информационной безопасности.

Предмет исследования составляют международные, региональные и национальные правовые нормы, определяющие основы, принципы и порядок взаимодействия государств по созданию системы международной информационной безопасности.

Целью выпускной квалификационной работы является комплексный анализ вопросов международного сотрудничества государств в сфере информационной безопасности. Достижение указанной цели связано с решением следующих **задач:**

- выявить терминологические и содержательные различия понятий, используемых при определении информационной безопасности в России и зарубежных странах;
- определить характер угроз информационной безопасности;
- рассмотреть международные акты, регулирующие вопросы в сфере обеспечения информационной безопасности;
- проанализировать региональное и двустороннее сотрудничество России по вопросам обеспечения информационной безопасности;
- рассмотреть проблемы, возникающие при взаимодействии государств по созданию международной системы информационной безопасности.

Методологическая основа работы. В процессе исследования использовались общенаучные методы познания, такие как анализ изучаемых явлений и синтез полученных результатов, индукция и дедукция, а также применялись частноправовые методы: историко-юридический, сравнительно-правовой, формально-логический и др.

Структура работы включает в себя введение, две главы, заключение и список использованных нормативно-правовых актов и литературы.

ГЛАВА 1. Теоретико-правовые аспекты информационной безопасности

1.1. Информационная безопасность: терминологические и содержательные различия

Вопросы информационной безопасности различных сфер жизнедеятельности человека стали возникать в 70-е годы XX в. и были вызваны появлением микропроцессорной техники и, в частности, персональных компьютеров, а также созданием новых информационно-коммуникационных технологий (ИКТ). Активизировался этот процесс вначале XXI в., когда наметился значительный прогресс в развитии технологий, формирующих современное информационное пространство. Причем в последние годы акцент сместился с корпоративной и персональной информационной безопасности на национальный и международный уровень.

Актуальность и значимость информационной безопасности для национальных интересов России подчеркивает тот факт, что о ней упоминается в ряде важнейших нормативных актов, формирующих направления внутренней и внешней политики страны, среди которых можно выделить: Указ Президента РФ от 31 декабря 2015 г. № 683 «О Стратегии национальной безопасности Российской Федерации»[1], Указ Президента РФ от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы»[2], «Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года»[3], Указ Президента РФ от 30 ноября 2016 г. № 640 «Об утвер-

---

[1] Указ Президента РФ от 31 декабря 2015 г. № 683 «О Стратегии национальной безопасности Российской Федерации» // Собрание законодательства Российской Федерации. 2016. № 1 (часть II). Ст. 212; Официальный интернет-портал правовой информации (www.pravo.gov.ru) 31 декабря 2015 г. (дата обращения 18.02.2018).

[2] Указ Президента РФ от 09 мая 2017г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы» // Официальный интернет-портал правовой информации (www.pravo.gov.ru) 10 мая 2017 г. (дата обращения 18.02.2018).

[3] Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года (утв. Президентом РФ 24 июля 2013 № Пр-1753 // Официальный сайт Совета Безопасности РФ; URL: http://www.scrf.gov.ru. (дата обращения 18.02.2018).

ждении Концепции внешней политики Российской Федерации»[1], Указ Президента РФ от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации»[2] и др.

Первоначально законодательное определение термина «информационная безопасность» было закреплено в Федеральном законе от 4 июля 1996 г. № 85-ФЗ «Об участии в международном информационном обмене». Информационная безопасность представляла собой «состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государства»[3]. Однако в действующем сегодня Федеральном законе от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»[4] дефиниция этого термина отсутствует.

Как следствие, в научной литературе можно встретить неоднозначные взгляды на содержательную составляющую анализируемого понятия. Так, Представители Центра стратегических оценок и прогнозов предлагают под информационной безопасностью понимать «состояние защищенности национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства»[5].

По мнению А.Д. Урсул, информационная безопасность представляет собой «состояние защищенности основных сфер жизнедеятельности по от-

---

[1] Указ Президента РФ от 30 ноября 2016 г. № 640 «Об утверждении Концепции внешней политики Российской Федерации» // Официальный интернет-портал правовой информации (www.pravo.gov.ru) 01 декабря 2016 г. (дата обращения 18.02.2018).

[2] Указ Президента РФ от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // Собрание законодательства Российской Федерации. 2016. № 50. Ст. 7074.

[3] Федеральный закон от 04 июля 1996 г. № 85-ФЗ (ред. 29.06.2004 № 58-ФЗ) «Об участии в международном информационном обмене» // Собрание законодательства Российской Федерации. 1996. № 28. Ст. 3347.

[4] Федеральный закон от 27 июля 2006 г. № 149-ФЗ (ред. 25.11.2017 г. № 327-ФЗ) «Об информации, информационных технологиях и о защите информации» // Собрание законодательства Российской Федерации. 2006. № 31 (часть I) Ст. 3448; 2017. № 48. Ст. 7051.

[5] Информационная война и защита информации. Словарь основных терминов и определений // Центр стратегических оценок и прогнозов. М., 2011. С. 22.

ношению к опасным информационным воздействиям»[1]. А.В. Еркин также предлагает определение, включающее только информационно-техническую сферу. Информационная безопасность – это «состояние рассматриваемой системы управления, при котором ее информационная инфраструктура не дестабилизируется под воздействием внешних и внутренних угроз; восприятие результата ее деятельности во внешнем окружении является объективным»[2].

Считаем, что такие определения несколько некорректны, т.к. они учитывает только техническую составляющую безопасности, не включая вопросы защиты прав и интересов личности в информационном пространстве. Солидаризируемся с точкой зрения Т.В. Закупень, что «при исследовании правовой сущности информационной безопасности важно понимать, что она представляет собой еще и социальное, а не только чисто техническое явление»[3].

В.Н. Лопатин считает, что под информационной безопасностью следует понимать состояние защищенности национальных интересов страны (жизненно важных интересов личности, общества и государства на сбалансированной основе) в информационной сфере от внутренних и внешних угроз[4].

Схожую формулировку предлагают В.А. Мазуров и В.В. Невинский, подразумевающие под данным термином «состояние защищенности жизненно важных интересов личности, общества, государства в информационной сфере от внешних и внутренних угроз, обеспечивающее ее формирование, использование и развитие»[5].

И.Э. Кванталиани придерживается более объемного определения, включающего в себя защищенность информационных ресурсов, информаци-

---

[1] Урсул А.Д. Информационная стратегия и безопасность в концепции устойчивого развития // Научно-техническая информация. Серия 1: Организация и методика информационной работы. 1996. № 1. С. 7.

[2] Еркин А.В. Понятия «информация» и «информационная безопасность»: от индустриального общества к информационному // Информационное общество. 2012. № 1. С. 73.

[3] Закупень Т.В. Понятие и сущность информационной безопасности, и ее место в системе обеспечения национальной безопасности РФ // Информационные ресурсы России. 2009. № 4. С. 32.

[4] См.: Лопатин В.Н. Информационная безопасность России: Человек. Общество. Государство. СПб.: Фонд «Университет», 2000. 433 с.

[5] Мазуров В.А., Невинский В.В. Понятие и принципы информационной безопасности // Известия Алтайского государственного университета. 2003. № 2. С. 59.

онных каналов, открытого доступа к любому источнику информации гражданина, общественной организации и государства в целом. У этого автора национальная информационная безопасность России представлена компонентом военной безопасности, относящимся к защите информационных ресурсов, каналов, баз данных и знаний, средств их переработки и хранения, который используется чисто в военных целях, и защищающим жизненно важные интересы граждан, общества, государства[1].

Сегодня нормативное закрепление рассматриваемого термина содержится в «Доктрине информационной безопасности Российской Федерации», утвержденной 5 декабря 2016 г. Указом Президента России. Центральное понятие документа конкретизировано в отношении России и представляет собой «состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства»[2].

М.С. Соколов, анализируя данное определение, пишет, что устранена неясность и неопределённость в понятии «состояние защищенности». Говорить о национальной информационной безопасности можно только при такой защищённости, когда обеспечены права и свободы, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое развитие России, оборона и безопасность государства[3].

---

[1] Кванталиани И.Э., Жданов Н.Б. Информационная безопасность – важнейший аспект интегральной безопасности//Журнал научных публикаций аспирантов и докторантов.2011. № 10. С. 43.

[2] Указ Президента РФ от 05 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // Собрание законодательства Российской Федерации. 2016. № 50. Ст. 7074.

[3] См.: Соколов М.С. Информационная безопасность. К вопросу о содержании понятия «информационная безопасность» // Закон и право. 2011. № 5. С. 9-14.

Схожая формулировка только без термина «информационная» использована в Стратегии национальной безопасности Российской Федерации[1]. Проводя сравнительный анализ понятий «национальная безопасность Российской Федерации» и «информационная безопасность Российской Федерации», Н.А. Молчанов и Е.К. Матевосова отмечают, что правовое регулирование не должно содержать неопределенности основных терминов и дефиниций, оно предназначено устранять пространность и неоднозначность центральных понятий[2].

В обоснование существующего нормативного подхода следует пояснить, что информационная безопасность представляет собой один из элементов сложной многоуровневой системы безопасности нашей страны. Сегодня информационно-коммуникационные технологии действуют во всех сферах жизнедеятельности общества (финансовой, политической, международной и т.д.), поэтому национальная безопасность во многом зависит от информационной. Соглашаясь с И.Э. Кванталиани, что информационная безопасность является одним из важнейших аспектов интегральной безопасности независимо от уровня: международного, национального, отраслевого, корпоративного или персонального[3], считаем, что особое внимание следует уделить международному аспекту данной проблемы.

Законодательное определение «международной информационной безопасности» содержится в п. 6 Основ государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года. Под ней понимается «такое состояние глобального информационного пространства, при котором исключены возможности нарушения прав личности, общества и прав государства в информационной сфе-

---

[1] Указ Президента РФ от 31 декабря 2015 г. № 683 «О Стратегии национальной безопасности Российской Федерации» // Собрание законодательства Российской Федерации. 2016. № 1 (часть II). Ст. 212.

[2] Молчанов Н.А., Матевосова Е.К. Доктрина информационной безопасности Российской Федерации (новелла законодательства) // Актуальные проблемы российского права. 2017. № 2. (75). С. 162.

[3] См.: Кванталиани И.Э., Жданов Н.Б. Указ. соч. С. 43.

ре, а также деструктивного и противоправного воздействия на элементы национальной критической информационной инфраструктуры»[1].

Исходя из данной дефиниции, можно сделать вывод, что содержательная часть включает в себя как технические аспекты (критическую информационную инфраструктуру), так и обширный круг политико-идеологических моментов (манипулирование информацией, пропаганду посредством глобальных информационных сетей, информационное воздействие и др.).

Согласно ст. 2 Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»[2] критическая информационная инфраструктура включает как объекты (информационные системы, автоматизированные системы управления субъектов критической информационной инфраструктуры, информационно-телекоммуникационные сети), так и сети электросвязи, используемые для организации их взаимодействия. Например, информационные системы сети госорганов, автоматизированные системы управления технологическими процессами в оборонной индустрии, в сфере здравоохранения, связи, на транспорте, в кредитно-финансовой сфере и энергетике, а также в ряде отраслей промышленности, включая топливную, атомную, ракетно-космическую и другие отрасли.

Представители Центра стратегических оценок и прогнозов к критически важному сегменту информационной инфраструктуры России относят «такую информационно-телекоммуникационную систему, выход из строя или нарушение режима функционирования которой может оказать негативное влияние на состояние национальной безопасности Российской Федера-

---

[1] Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года (утв. Президентом РФ 24 июля 2013 № Пр-1753) // Официальный сайт Совета Безопасности РФ; URL: http://www.scrf.gov.ru (дата обращения 18.02.2018).

[2] Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» // Официальный интернет-портал правовой информации (www.pravo.gov.ru) 27.07.2017. (дата обращения 21.02.2018).

ции»[1]. В критически важный сегмент информационной инфраструктуры включены: системы телекоммуникаций военного и специального назначения; системы управлений энергетикой, транспортом, водными системами; ИТС служб реагирования на чрезвычайные ситуации; банковские и финансовые ИТС; другие государственные и частные ИТС, минимально необходимые для функционирования экономики и государства.

Второй составляющей в российской версии определения международной информационной безопасности является информационно-психологическая, под которой понимается «состояние защищенности от негативных информационно-психологических воздействий в связи с использованием специальных средств и методов воздействия на психику отдельных лиц и (или) групп лиц, и связанных с этим иных жизненно важных интересов личности, общества и государства в информационной сфере»[2].

Таким образом, первоначально термин «информационная безопасность» использовался для обозначения проблем, касающихся только технологической сферы, но в последующем приобрел более широкий смысл[3]. Именно такой подход, по мнению Д.А. Молчанова, сочетающий в себе как технические, так и психологические аспекты информационной безопасности и характеризует выбор российской терминологии[4].

Для эффективного сотрудничества между странами в информационной сфере необходима однозначная интерпретация используемых понятий. Зарубежные страны, и прежде всего США, в отличие от России используют термин «cybersecurity». Данная формулировка применяется и Международным

---

[1] Информационная война и защита информации. Словарь основных терминов и определений // Центр стратегических оценок и прогнозов. М., 2011. С. 32.

[2] Баришполец В.А. Информационно-психологическая безопасность: основные положения // Радиоэлектроника. Наносистемы. Информационные технологии. 2012. № 5. С. 65.

[3] Валиахметова Г.Н. Проблемы информационной безопасности в Азии // Известия Уральского федерального университета. 2015. № 1 (137). С. 128.

[4] Молчанов Д.А. Дифференциация содержания понятия «информационная безопасность» в национальном законодательстве Российской Федерации и Соединенных Штатов Америки как сдерживающий фактор прогрессивного развития международно-правового регулирования [Электронный ресурс] // Право: современные тенденции: материалы IV Междунар. науч. конф. (г. Краснодар, февраль 2017 г.). Краснодар: Новация, 2017. С. 122-125; URL: https://moluch.ru/conf/law/archive/225/11706/ (дата обращения 22.02.2018).

союзом электросвязи, членами которого является 191 государство. Кибербезопасность – это совокупность инструментов, политик, понятий безопасности, гарантий безопасности, рекомендаций, подходов управления рисками, действий, обучения, лучших практик, гарантий и технологий, которые используются с тем, чтобы защитить киберсреду («cyberspace») организации-пользователя и активы пользователя. Организация-пользователь и активы пользователя включают связанные вычислительные устройства, персонал, инфраструктуру, прикладные технологии, услуги, телекоммуникационные системы и совокупность переданной и/или сохраненной информации в киберсреде»[1].

В Международной стратегии США для киберпространства «Процветание, безопасность и открытость сетевого мира» 2011 г.[2] определение «cybersecurity» также отражает только один аспект, связанный со средствами обработки информации. Кибербезопасность представляет собой защиту и оборону информации и информационных систем против несанкционированного доступа или модификации информации, находящейся в процессе хранения, обработки или передачи, а также против прекращения функционирования системы для санкционированных пользователей. Информационная безопасность включает меры, необходимые для обнаружения, документирования и ответа на эти угрозы[3].

О выявлении проблем семантического характера при использовании терминов пишет М.Б Касенова. Так, «cybersecurity» напрямую связана с «cyberspace». Термин «cyberspace» применятся в документах Международного союза электросвязи, где означает среду с подключенными компьютерными устройствами, пользователями, инфраструктурой, приложениями, серви-

---

[1] Цит. по: Касенова М.Б. Трансграничное управление Интернетом: основные термины и понятия [Электронный ресурс] // Юридический мир. 2014. № 2. (206). С. 58-63; URL: http://geum.ru/lav/index-42965.php (дата обращения 22.02.2018).

[2] International Strategy For Cyberspace, Washington DC. Prosperity, Security, and Openness in a Networked World // The White House : offic. website. 2011. May.25 p. URL: http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf (дата обращения 28.02.2018).

[3] Касенова М.Б. Указ. соч. С. 60.

сами, телекоммуникационными системами, а также совокупность передаваемой и (или) хранящейся в этой среде информации. В то же время в национальном законодательстве Польши данный термин имеет иное содержательное значение (пространство производства и обмена информацией, создаваемой телеинформационными системами)[1].

В России формулировка «киберпространство» не применяется, а используется «информационное пространство». Оно определено как «сфера деятельности, связанная с формированием, созданием, преобразованием, передачей, использованием, хранением информации, оказывающая воздействие в том числе на индивидуальное и общественное сознание, информационную инфраструктуру и собственно информацию»[2].

Смысловые и содержательные различия употребления тех или иных терминов зависят также и от вариантов их перевода на другие языки. Например, слово «cybersecurity» с английского языка на русский буквально переводится как «кибербезопасность», но Россия использует понятия «информационная безопасность» или «безопасность применения информационно-коммуникационных технологий». Следует отметить, что не только в России применяется данный термин. Например, он сформулирован и закреплён в концепции Конвенции об обеспечении международной информационной безопасности, предложенной к рассмотрению на 66-й сессии Генеральной Ассамблеи ООН в 2011 г. Китаем, Россией, Таджикистаном и Узбекистаном[3].

Модельный закон стран Содружества Независимых Государств 2002 г. «О международном информационном обмене» также использует понятие информационная безопасность и определяет ее как «состояние защищенно-

---

[1] Цит. по: Чеботарева А.А. Правовое обеспечение информационной безопасности личности в глобальном информационном пространстве // Юридический мир. 2016. № 8. С. 63-66.

[2] Конвенция об обеспечении международной информационной безопасности (концепция) // Официальный сайт Министерства иностранных Дел Российской Федерации; URL: http://www.mid.ru/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/191666 (дата обращения 24.02.2018).

[3] Там же.

сти информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государства»[1].

Концепция сотрудничества государств - участников СНГ в сфере обеспечения информационной безопасности, утвержденная Советом глав государств СНГ в 2008 г., трактует информационную безопасность как «состояние защищенности от внешних и внутренних угроз информационной сферы, формируемой, развиваемой и используемой с учетом жизненно важных интересов личности, общества и государства»[2]. Такой узкий технократический подход, включающий только ее защиту, существенно сужает проблему информационной безопасности. Поэтому в Рекомендациях предлагается использовать сущностную трактовку, закрепленную в тексте Соглашения между Правительствами государств - членов Шанхайской организации сотрудничества «О сотрудничестве в области обеспечения международной информационной безопасности» (Екатеринбург, 2009 г.). В этом документе анализируемая категория представлена как «состояние защищенности личности, общества и государства и их интересов от угроз, деструктивных и иных негативных воздействий в информационном пространстве»[3]. Такая дефиниция включает в себя в том числе, и актуальные угрозы социально-гуманитарного плана, например, угрозу распространения информации, наносящей вред общественно-политической и социально-экономической системам государства, духовной, нравственной или культурной среде общества.

---

[1] Модельный закон «О международном информационном обмене» (Принят постановлением Межпарламентской Ассамблеи государств-участников СНГ от 26 марта 2002 г. № 19-7) // Информационный бюллетень Межпарламентской Ассамблеи государств-участников СНГ. 2002. № 29; URL: http://base.garant.ru/2569410/

[2] Концепция сотрудничества государств-участников Содружества Независимых Государств в сфере обеспечения информационной безопасности и Комплексный план мероприятий по реализации Концепции сотрудничества государств - участников Содружества Независимых Государств в сфере обеспечения информационной безопасности 2008 г. [Электронный ресурс] // Интернет портал стран СНГ. – Режим доступа: http://www.e-cis.info/page.php?id=20229 (дата обращения 24.02.2018).

[3] Распоряжение Правительства РФ от 16 июля 2009 г. № 984-р «Об утверждении Соглашения между правительствами государств - членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности» [Электронный ресурс] // Текст Распоряжения официально опубликован не был; URL: http://www.garant.ru (дата обращения 25.02.2018).

Подписанное в 2012 г. Соглашение о сотрудничестве государств - участников СНГ в области обеспечения информационной безопасности от 28 мая 2012 г. содержало формулировку аналогичную как в Концепции 2008 г.[1] В действующем сегодня Соглашении о сотрудничестве от 2013 г. информационная безопасность понимается как «состояние защищенности личности, общества и государства и их интересов от угроз, деструктивных и иных негативных воздействий в информационном пространстве»[2].

Согласно Конвенции об обеспечении международной информационной безопасности, предложенной в 2011 г. Россией для обсуждения в рамках ООН «международная информационная безопасность» представляет собой состояние международных отношений, исключающее нарушение мировой стабильности и создание угрозы безопасности государств и мирового сообщества в информационном пространстве»[3].

Резюмируя отметим, что на сегодняшний день мировое сообщество не может прийти консенсусу относительно терминологии и содержательной сущности понятия «информационная безопасность». Российская Федерация придерживается широкого подхода к определению содержания информационной безопасности и включает в него как информационно-техническую сферу, так и информационно-психологическую (психофизическую) составляющую. Западные страны и США придерживаются более узкого подхода, ограничиваясь технической сферой, и используют иное определение – «кибербезопасность».

---

[1] Распоряжение Правительства РФ от 28 мая 2012 г. № 856-р «О подписании Соглашения о сотрудничестве государств-участников Содружества Независимых Государств в области обеспечения информационной безопасности» // Собрание законодательства РФ. 2012. № 23. Ст. 3058.

[2] Распоряжение Правительства РФ от 15 ноября 2013 г. № 2120-р «О подписании Соглашения о сотрудничестве государств - участников Содружества Независимых Государств в области обеспечения информационной безопасности // Собрание законодательства РФ. 2013. № 47. Ст. 6135.

[3] Конвенция об обеспечении международной информационной безопасности (концепция) // Официальный сайт Министерства иностранных Дел Российской Федерации; URL: http://www.mid.ru/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/191666 (дата обращения 24.02.2018).

1.2. Характер угроз информационной безопасности

Для эффективного и плодотворного сотрудничества государств по созданию системы международной информационной безопасности необходимо прийти не только к консенсусу при использовании идентичных дефиниций и сущностных характеристик понятий, но необходимо и своевременно проводить анализ угроз, которые могут возникнуть при применении современных информационно-коммуникационных технологий.

Актуальность перманентного анализа для четкого представления тенденций развития глобальной информационной сферы и прогнозирования потенциальных угроз и рисков, подчеркивает Президент России В.В. Путин. В своем выступлении на заседании Совета Безопасности от 26 октября 2017 г. он отметил: «нужно учитывать, что уровень угроз в информационном пространстве постоянно повышается, число рисков увеличивается, а негативные последствия разного рода носят уже не локальный, а действительно глобальный характер и масштаб»[1].

Анализируя резолюции Генеральной Ассамблеи ООН, посвящённые проблематике информационной безопасности, Е.С. Зиновьева выделяет три вида угроз международного характера: 1) кибертерроризм (различные формы); 2) киберпреступность, 3) использование информационного пространства в военно-политических целях (информационные войны и информационное противоборство)[2].

Схожие типы угроз, с которыми столкнулось человечество в результате применения новых информационных технологий, отмечает С.А. Егоров. К ним он относит: 1) «кибервойны» – силовое противостояние государств в информационной сфере; 2), «кибертерроризм» – использование информационных технологий террористическими организациями либо в террористиче-

[1] Выступление Президента РФ В.В. Путина на заседании Совета Безопасности 26 октября 2017 г., Москва, Кремль [Электронный ресурс] // Официальный сайт Президента России; URL: http://www.kremlin.ru/events/president/news/55924 (дата обращения 28.02.2018)

[2] См.: Зиновьева Е.С. Международная информационная безопасность. Монография. – М.: Издательство: МГИМО, 2014. 200 с.

ских целях; 3) «киберпреступность» – использование сети Интернет в противоправных целях, с нарушением установленного правопорядка, преследуемых уголовным законодательством национальных государств[1].

В.А. Жилкин называет информационную безопасность – «символом нашего времени» [2]. Признавая сеть Интернет пространством международной политики, автор указывает на возможные риски: использование глобальной сети различными террористическими и экстремистскими организациями с целью военных угроз и вербовки террористов; воздействие на атомные и военные объекты; кибератаки в сфере коммуникационных сетей и бытовых цифровых технологий; нарушения в кредитно-финансовой сфере и др.

В Основах государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 г. определены следующие виды угрозы:

- использование современных ИКТ в качестве информационного оружия в военно-политических целях для реализации актов агрессии, направленных на дискредитацию суверенитета и нарушение территориальной целостности государств. Несмотря на то, что сегодня данная угроза носит потенциальный характер, ее реализация может привести к негативным последствиям в мировом масштабе;
- использование ИКТ для совершения террористических актов, пропаганды терроризма, с целью вовлечения в террористическую деятельность новых сторонников, деструктивное влияние на элементы критической информационной инфраструктуры;
- использование информационно-коммуникационных технологий с целью вмешательства во внутренние дела суверенных государств, нарушения общественного порядка, разжигания межнациональной, межрасовой и межконфессиональной вражды, пропаганды расистских и ксенофобских идей или

[1] Международное право: учебник./ Отв. ред. д.ю.н. С.А. Егоров. – М.: Статут, 2018. С. 834.
[2] Жилкин В.А. Международная безопасность и роль России в борьбе с международным терроризмом и информационной безопасностью // Международное публичное и частное право. 2017. № 4. С. 25.

теорий, порождающих ненависть и дискриминацию, подстрекающих к насилию;

- использование ИКТ для совершения преступлений, связанных с незаконным доступом к компьютерной информации, кражей финансов с банковских счетов, с созданием, использованием и распространением вредоносных компьютерных программ. По данным Интерпола из всех существующих областей человеческой деятельности за последние годы World Wide Web стала сферой самого активного роста преступности[1].

Е.С. Зиновьева отмечает, что Российская Федерация добавила к триаде угроз опасность вмешательства во внутренние дела суверенного государства посредством ИКТ, нарушение общественной стабильности, разжигание межэтнической, межнациональной розни. Автор связывает данную формулировку в российском нормативном акте с событиями «арабской весны» начала 2011 г., когда социальные сети активно использовались для координации протестного движения[2].

А.Я. Капустин, обращая внимание на угрозу использования ИКТ в качестве информационного оружия в военно-политических целях, доказывает, что информационное нападение может носить косвенный характер. Это связано с тем, что компьютерная атака обладает четырьмя основными характеристиками: опосредованность, неприкосновенность, место проведения (пространственная характеристика или локус) и результат. Часть перечисленных характеристик не создает серьезных проблем для квалификации с точки зрения современного международного права, однако определенный интерес вызывает такая особенность информационного нападения, как опосредованность или косвенный характер ее осуществления. Иногда невозможно доказать ответственность государства за использование на его территории компьютеров, с которых совершалась «кибератака». Такая ситуация не позволяет

[1] Грибков Д.Г. О формировании системы международной информационной безопасности // Международная жизнь. 2015. № 8. С. 86-92.
[2] Зиновьева Е.С. Анализ внешнеполитических инициатив России в области международной информационной безопасности // Интернет-Политика. 2014. № 6 (39). С. 49.

решить вопрос об определении истинного виновника нападения, а также увеличивает риск того, что контрмеры могут быть направлены на невиновные в совершении действий государства или даже на отдельных людей[1].

В качестве примера косвенных атак можно привести манипулирование информационными данными больницы, в результате чего при лечении военным дается неправильная группа крови, или отключение систем управления воздушным движением и др.

Поддерживают данную точку зрения О.В. Казарин и Р.А. Шаряпов, считающие, что сегодня кибервойны могут инициироваться не только государствами и правительствами, но и негосударственными организациями, незаконными вооруженными формированиями, сетевыми комбатантами. Нет ясности в том, кто является противником, война это или не война. Особенностью кибервойны является то, что слабая в военном отношении сторона может успешно противостоять сильному противнику и даже победить его[2].

В Концепции сотрудничества государств - участников СНГ в сфере обеспечения информационной безопасности 2008 г. к упомянутым угрозам добавлены: противодействие доступу к новейшим ИКТ; создание условий технологической зависимости в сфере информатизации в ущерб другим государствам; введение ограничений, ущемляющих интересы государств - участников СНГ в информационной сфере, а также основные права и свободы граждан; информационная экспансия, приобретение контроля над национальными информационными ресурсами другого государства.

Учитывая, что информационная безопасность включает в себя как информационно-техническую, так и информационно-психологическую составляющие, возможно предположить возникновение угроз в этих сферах. Так, Т.В. Закупень обращает внимание на то, что с помощью специально подготовленного контента, распространяемого в глобальной сети, можно создать

---

[1]См.: Капустин А.Я. Угрозы международной информационной безопасности: формирование концептуальных подходов // Журнал российского права. 2015. № 8. С. 89-100.

[2] См.: Казарин О.В., Шаряпов Р.А. Вредоносные программы нового поколения – одна из существенных угроз международной информационной безопасности // Информатика, защита информации, информационная безопасность. 2015. № 12 (155). С 9-23.

атмосферу напряженности и политической нестабильности в обществе, спровоцировать социальные, национальные, религиозные конфликты и массовые беспорядки, которые могут привести к разрушительным последствиям для демократического развития страны[1].

В.А. Жилкин в контексте рассматриваемого вопроса, считает, что распространяемая в сети информация, может оказывать негативное влияние на «сознание гражданина как носителя ценностей гражданских прав и свобод, которые позволяют ему чувствовать национальное достоинство»[2].

И.Е. Ильичев проводит градацию угроз в отношении информационной безопасности личности, общества и государства. Например, источником угроз информационно-психологической безопасности личности автор считает поток негативно-культурной информации. Систематический дисбаланс между позитивной и негативной информацией в сторону последней способен вызвать деформацию психики личности, нарушение и разрушение ценностных ориентаций, десоциализацию и др.

Угрозы для общества связаны с использованием подрывной пропаганды для дестабилизации внутриполитической обстановки в стране. В такой ситуации общество фактически становится объектом необъявленной войны наравне с военной, политической и экономической организацией государства.

В состав угроз информационной безопасности государства ученый включает: угрозы информационному обеспечению государственной политики Российской Федерации; развитию отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи, обеспечению потребностей внутреннего рынка в её продукции и выходу этой продукции на мировой рынок, а также обеспечению накопления, сохранности и эффективного использования отечественных информационных ресур-

[1] Закупень Т.В. Указ. соч. С. 28
[2] Жилкин В.А. Указ. соч. С. 25.

сов; угрозы безопасности информационных и телекоммуникационных средств и систем на территории России[1].

Классификацию угроз технической составляющей информационной безопасности предлагают Д.Г. Есиева и Ю.В. Саханский:

- связанные с нарушением конфиденциальности, нацеленные на разглашение секретной информации;
- связанные с целостностью информации, которые приводят к уничтожению или к нарушению качества информации;
- способствующие нарушению работоспособности автоматизированных систем, т.е. умышленные действия для блокирования доступа к ресурсам системы либо для снижения работоспособности[2].

Следует обратить внимание на то, что угрозы информационной безопасности обладают специфическими особенностями, отличающими их от всех существующих видов международных угроз (применение оружия массового уничтожения, распространения эпидемий, пандемий, экологические проблемы и т.д.). Международным сообществом для предотвращения таких угроз были выработаны механизмы силового и правового противодействия, которые не подходят для информационных. Так, П.А. Шариков среди особенностей выделяет то, что ресурсы, необходимые для создания информационной угрозы, не могут контролироваться государством. Для создания возможностей использования информационных ресурсов в качестве угрозы международной безопасности достаточно применения технологий, имеющихся в свободной продаже. Еще одной характерной чертой является значительная степень анонимности информационного пространства, что суще-

---

[1] См.: Ильичев И.Е. Проблемы обеспечения информационной безопасности личности, общества и государства в современной России // Проблемы правоохранительной деятельности. Наука. Теория. Практика. 2015. № 2. С. 13-21.

[2] Есиева Д.Г., Саханский Ю. В. Анализ угроз информационной безопасности в современном цифровом пространстве [Электронный ресурс]// Научные исследования и перспективные проекты 2017; URL: http://old.fa.ru/fil/chair-matinf-vladik/Pages/nirs.aspx (дата обращения 24.02.2018).

ственно осложняет международное расследование информационных правонарушений[1].

Наличие особенных признаков, присущих информационным угрозам, подчёркивает и Д. Грибков. «Проблема состоит в том, что принцип «сдерживания» (по аналогии с ядерным или обычным оружием) в данном случае не работает. В глобальной сети не существует системы опознавания «свой-чужой». По этой причине, а также в силу трансграничности ИКТ учесть кибернетический потенциал противостоящих сторон невозможно. Таким образом, может возникнуть иллюзия превосходства в средствах ведения информационной войны и появится соблазн нанесения первого удара[2].

О.В. Казарин, В.Ю. Скиба и Р.А. Шаряпов к квалификационным критериям, по которым можно проводить классификацию угроз в информационном пространстве относят:

1) местонахождение источника угрозы (внешняя, внутренняя);

2) степень сформированности угрозы (потенциальная, реальная);

3) степень субъективного восприятия (завышенная, заниженная, адекватная, мнимая, неосознанная);

4) характер (природная, антропогенная, техногенная, комбинированная);

5) среда для осуществления угрозы (технологическая, социальная);

6) сфера жизнедеятельности, для которой опасна угроза (экономическая, социальная, политическая, оборонная, международная)[3].

В.А. Мазуров и В.В. Невинский подразделяют угрозы информационной безопасности России в зависимости от источника их возникновения. Внешние источники угроз: деятельность иностранных разведывательных и информационных структур, международных террористических организаций, а также обострение международной конкуренции за обладание информационны-

---

[1] Шариков П.А. Политика США в области информационной безопасности [Электронный ресурс]: автореф. дисс.… канд. полит. наук. М, 2009. 25 с. URL: http://cheloveknauka.com/politika-ssha-v-oblasti-informatsionnoy-bezopasnosti (дата доступа 28.02.2018)

[2] См.: Грибков Д.Г. Указ. соч. С. 88.

[3] Казарин О.В., Скиба В.Ю., Шаряпов Р.А. Новые разновидности угроз международной информационной безопасности // Вестник РГГУ. Документоведение и архивоведение. Информатика. Защита информации и информационная безопасность. 2016. № 1 (3). С. 56

ми технологиями и ресурсами; увеличение технологического отрыва ведущих государств мира и наращивание их возможностей по противодействию созданию конкурентоспособных российских информационных технологий.

Внутренние источники угроз связаны с критическим состоянием российских отраслей промышленности; неблагоприятной криминогенной обстановкой в стране; недостаточной координацией деятельности федеральных органов власти, органов государственной власти субъектов РФ по формированию и реализации единой государственной политики в области обеспечения информационной безопасности РФ; недостаточной разработанностью нормативной правовой базы, регулирующей отношения в информационной сфере; низким финансированием мероприятий по обеспечению информационной безопасности и др.[1]

Одним из критериев классификации может выступать природа возникновения угроз. Объективные угрозы связывают с воздействием на информационную среду объективных физических процессов или стихийных природных явлений, не зависящих от воли человека. Искусственные (субъективные) угрозы связаны с влиянием на информационную сферу человека. Среди последних выделяют: а) непреднамеренные угрозы – ошибки программного обеспечения, персонала, отказы вычислительной техники; б) преднамеренные (умышленные) угрозы – неправомерный доступ к информации, разработка и распространение вирусных программ и т.д.[2]

В зависимости от сфер жизнедеятельности, в которых могут возникнуть угрозы, Н.В. Сарычев и Д.В. Мельниченко выделяют:

- в политической сфере (информационно-психологическое воздействие с целью формирования отношений в обществе, влияние на реакции общества на происходящие политические процессы);

[1] См.: Мазуров В.А., Невинский В.В. Указ. соч. С. 60.
[2] См.: Охрименко С.А., Черней Г.А. Угрозы безопасности автоматизированным информационным системам (программные злоупотребления) // Научно-техническая информация. Серия 1: Организация и методика информационной работы. 1996. № 5.

- в экономической сфере (влияние на экономические структуры: от недостоверности и запаздывания до незаконного использования экономической информации);
- в военной сфере (влияние на качество добываемой информации и уровень развития информационных технологий, на которых основываются системы разведки, радиоэлектронной борьбы, управления войсками и высокоточным оружием);
- в сфере духовной жизни (опасность развития в обществе с помощью электронных средств массовой информации агрессивной потребительской идеологии, распространения идей насилия и нетерпимости и других негативных воздействий на сознание и психику человека)[1].

В связи со стремительными темпами развития информационных технологий на важность осуществления перманентного контроля появляющихся угроз, указывают О.В. Казарин, В.Ю. Скиба и Р.А. Шаряпов[2]. Эти авторы отмечают, что за последние годы появились новые угрозы, среди которых:

1) кибершпионаж Агентства национальной безопасности США, осуществляемый «через жесткие диски». Предположительно, шпионское программное обеспечение перепрограммирует прошивку жестких дисков, благодаря чему остается невидимыми для антивирусов. Компьютеры с такими дисками были обнаружены в 30 странах мира (Пакистане, Китае, Иране, Афганистане, Сирии, России, Алжире, Мали и др.).

2) Смурф-технологии. В интервью британской телерадиокомпании ВВС Э. Сноуден рассказал о возможности доступа к личным данным пользователей смартфонов[3]. На мобильное устройство отправляется сообщение с зашифрованным текстом, о котором пользователь и не догадывается. В результате чего, спецслужба получает доступ ко всем личным сообщениям, фото-

[1] См.: Сарычев Н.В., Мельниченко Д.В. Внешние и внутренние угрозы информационной безопасности России // Российский психологический журнал. 2010. № 5. С. 108-114.

[2] Казарин О.В., Скиба В.Ю., Шаряпов Р.А. Новые разновидности угроз международной информационной безопасности // Вестник РГГУ. Документоведение и архивоведение. Информатика. Защита информации и информационная безопасность. 2016. № 1 (3). С. 60-65.

[3] Васильев А. Э. Сноуден рассказал о слежке западных спецслужб за смартфонами // Российская газета. 2015, 8 октября.

графиям пользователя и истории его браузера. Кроме того, посредством удаленного доступа можно включать микрофон владельца телефона для его прослушивания и даже сфотографировать этого человека.

3) Террористическое интернет-рекрутирование и пропаганда. Сегодня террористические организации используют всемирную сеть через компьютерные игры, интернет-магазины, трансляцию фильмов, социальные сети для информационного воздействия на население. Сеть Интернет также может использоваться для вербовки и мобилизации сторонников. В дополнение к таким средствам поиска новобранцев, как технологии веб-сайта (звук, видео и т.д.), террористические организации собирают информацию о пользователях, просматривающих их сайты, а затем входят с ними в контакт[1].

4) Киберкражи из банков. В отличие от хищения денежных средств со счетов клиентов банка, здесь предполагается напрямую кража со счетов банка.

5) Угрозы информационной безопасности в международной экономической деятельности, что касается как международных, так и региональных организаций. Например, в схеме обмена электронными документами при трансграничном взаимодействии органов государственной власти государств - членов Евразийского экономического союза между собой и с Евразийской экономической комиссией с участием доверенной третьей стороны возникают коллизии, связанные с возникновением ситуации, при которой субъект взаимодействия (юридическое или физическое лицо) потенциально может подать в государственный орган электронный документ, который он получил от другого субъекта, отличающейся от требуемого вида подачи. В этом случае государственный орган не сможет корректно проверить такой электронный документ. Такая угроза может возникнуть, например, при обеспечении государственных закупок в электронной форме в рамках ЕАЭС[2].

На постоянно эволюционирующий характер угроз информационной безопасности обращено внимание в «Глобальной программе кибербезопасно-

[1] См.: Брылева Е.А. Право на использование Интернета как одно из «неотъемлемых» прав человека? // Информационное право. 2017. № 2. С. 23-26.

[2] См.: Казарин О.В., Скиба В.Ю., Шаряпов Р.А. Указ. соч. С. 60-65.

сти» Международного союза электросвязи[1]. «В настоящее время существует опасность того, что хакеры изменят свою стратегию и перейдут от модели центрального командного управления бот-сетями к одноранговой модели с распределенной структурой управления, способной охватывать находящиеся в различных странах компьютеры с раскрытой системой безопасности. Такая практика затрудняет определение точного местонахождения отдельного географического объекта как места происхождения кибератак с использованием бот-сетей и, следовательно, значительно осложняет задачу их обнаружения и подавления. Изменение такой стратегии направлено не только на то, чтобы доставлять почту-спам и вредоносные программные средства, но и может также быть использовано для распространения запрещенного контента, например детской порнографии, причем владельцы используемого компьютера могут и не знать, что они принимают и распространяют такой контент»[2].

В целом, спрогнозировать потенциальные угрозы информационной безопасности очень сложно, что связано как с быстрым развитием информационных технологий, так и с разнообразием сфер жизнедеятельности, для которых эти угрозы могут быть опасны.

Для создания действенной системы международной информационной безопасности необходимо согласованное представление разных политических акторов о том, какие виды угроз представляют опасность для мирового сообщества. На сегодняшний момент ключевые игроки международной политики придерживаются совершенно противоположных подходов к обеспечению информационной безопасности. Так, США и страны Европейского Союза к главным угрозам кибербезопасности относят кибертерроризм и киберпреступность, а проблемы межгосударственного противоборства, по их мнению, должны регулироваться международным гуманитарным правом. Россия и Китай придерживаются взглядов о необходимости полной демили-

[1] Глобальная программа кибербезопасности МСЭ. Основа для международного сотрудничества в области кибербезопасности [Электронный ресурс] // URL: http://www.ifap.ru/pr/2008/080908aa.pdf (дата обращения 02.03.2018).
[2] Там же.

таризации информационного пространства, что предполагает заключение международной договоренности об отказе стран от создания средств информационного воздействия и осуществления любых возможных агрессивных действий в информационном пространстве[1].

Расхождение во взглядах наблюдается и в различных восприятиях содержания понятия «угроза». Так, российский вариант, представленный на Лондонской Международной конференции по действиям в киберпространстве (1-2 ноября 2011 г.), в перечень угроз включает «угрозу применения информационных ресурсов для влияния на социально-гуманитарную сферу»[2]. Такой же подход отражен и в Соглашении между правительствами государств - членов ШОС «О сотрудничестве в области обеспечения международной информационной безопасности» 2009 г. В ст. 2 этого документа перечень угроз в области обеспечения информационной безопасности включает «распространение информации, наносящей вред общественно-политической и социально-экономической системам, духовной, нравственной и культурной среде других государств»[3].

Напротив, западные страны признают угрозу, исходящую от враждебных информационных ресурсов, которая влияет только на техническую сферу.

Таким образом, для эффективного сотрудничества государств в сфере информационной безопасности необходима не только унификация понятийно-категориального аппарата, но и требуется достичь консенсуса относительно характера угроз, которые могут представлять опасность при использовании информационного пространства.

---

[1] См.: Зиновьева Е.С. Международная информационная безопасность: монография / Моск. гос. институт междунар. отношений МИД России. М.: МГИМО-Университет, 2014. 194 с.

[2] См.: Меркурьева Е.А Международное сотрудничество России в области обеспечения информационной безопасности [Электронный ресурс] // Центр стратегических оценок и прогнозов; URL: http://csef.ru/ru/nauka-i-obshchestvo/445/mezhdunarodnoe-sotrudnichestvo-rossii-v-oblasti-obespecheniya-informaczionnoj-bezopasnosti (дата обращения 04.03.2018).

[3] Соглашение между правительствами государств - членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности (Екатеринбург, 16 июня 2009 г.) // URL: http://www.conventions.ru/view_base.php?id=1979 (дата обращения 28.02.2018).

ГЛАВА 2. Сотрудничество государств по созданию системы международной информационной безопасности

1.1. Международные акты, регулирующие вопросы обеспечения информационной безопасности

Учитывая, что информационное пространство по своей природе трансгранично и информационные вызовы и угрозы сегодня не ограничиваются пределами одного государства, важно наладить диалог между странами для создания международной системы безопасности. При этом система по предотвращению и ликвидации таких угроз должна включать в себя правовые, организационные, технические, программные, социальные и иные механизмы.

Солидаризируемся с мнением Н.А. Молчанова и Е.К. Матевосовой, которые считают, что «международная информационная безопасность» представляет собой «математическую совокупность» информационной безопасности всех стран, поэтому учесть общее глобальное состояние всей совокупности сегодня не представляется возможным[1]. В контексте выбранной проблематики целесообразно рассмотреть международно-правовое регулирование и меры, которые разрабатываются государствами в целях обеспечения информационной безопасности.

Проанализировав существующие международные документы, отметим, что на сегодняшний момент мировым сообществом не принят единый юридически обязательный универсальный акт, который бы регулировал вопросы обеспечения информационной безопасности. Данная проблема обозначена в Доктрине информационной безопасности РФ: «отсутствие международно-правовых норм, регулирующих межгосударственные отношения в информационном пространстве, а также механизмов и процедур их применения, учитывающих специфику информационных технологий, затрудняет формирование системы международной информационной безопасности, направленной

[1] См.: Молчанов Н.А., Матевосова Е.К. Доктрина информационной безопасности Российской Федерации (новелла законодательства) // Актуальные проблемы российского права. 2017. № 2. (75). С. 159-165.

на достижение стратегической стабильности и равноправного стратегического партнерства стран»[1].

Впервые вопрос о возможности возникновения конфронтации в принципиально новой информационной сфере был озвучен Россией еще в сентябре 1998 г., которая направила в адрес Генерального секретаря Организации Объединенных Наций К. Аннана специальное Послание по проблеме международной информационной безопасности. Эта инициатива получила практическую реализацию в Резолюции ГА ООН (A/RES/53/70)[2] от 4 декабря 1998 г., предлагавшей государствам обсудить вопросы информационной безопасности, дать конкретные определения типов угроз, разработать международные принципы обеспечения безопасности глобальных информационных систем.

Следующим этапом в формировании международной основы по обеспечению информационной безопасности, который указал на возможность возникновения угроз не только в гражданской, но и в военной сфере, стала Резолюция (A/RES/54/49)[3], принятая Генассамблеей в декабре 1999 г. Документ впервые обозначил «триаду» угроз: использование информационных технологий в военных, террористических и преступных целях.

Дальнейшее обсуждение рассматриваемая проблема получила в Докладе Генерального секретаря ООН (A/55/140)[4]. Российский ответ на вопросы, сформулированные в Резолюции (A/RES/54/49), страна представила в виде «Принципов, касающихся международной информационной безопасности». Фактически РФ предложила рабочий проект кодекса поведения в информа-

---

[1] Указ Президента РФ от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // Собрание законодательства Российской Федерации. 2016. № 50. Ст. 7074.

[2] См.: Текст Резолюции (A/RES/53/70) от 4 декабря 1998 г. «Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности»// Официальный сайт ООН;URL: http://www.un.org/ru/development/ict/res.shtml (дата обращения 28.02.2018).

[3] См.: Текст Резолюции (A/RES/54/49) от 1 декабря 1999 г. // Официальный сайт ООН; URL: http://www.un.org/ru/development/ict/res.shtml (дата обращения 28.02.2018).

[4] Доклад Генерального секретаря ООН A/55/ 140. Генеральная Ассамблея 10 июля 2000 г. Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности. Официальный сайт ООН; URL: http://dag.un.org/bitstream/handle/11176/152212/A_55_140-RU.pdf?sequence=5&isAllowed=y (дата обращения 28.02.2018).

ционной среде, содержаний основные определения и принципы международно-правового регулирования в информационном пространстве.

Резолюция (A/RES/56/19)[1], принятая уже в ноябре 2001 г., переводит общеполитическое обсуждение проблематики международной информационной безопасности в плоскость поиска практических решений и запускает механизм формирования Группы правительственных экспертов ООН (ГПЭ) первое заседание которой состоялось в июле 2004 г.

По инициативе России с 1998 г. каждый год ГА ООН принимаются Резолюции под общим названием «Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности»[2]. Например, Резолюция (A/RES/65/41) от 8 декабря 2010 г. и Резолюция (A/RES/69/28) от 2 декабря 2014 г.[3] призывают государства к участию в обеспечении информационной безопасности и созданию информационного пространства, для которого характерны мир, сотрудничество и гармония.

В сентябре 2015 г. в ходе 70-й Генеральной Ассамблеи ООН Первым комитетом принят российский проект «Достижения в сфере информатизации и коммуникаций в контексте международной безопасности», соавторами которого стали более 80 стран мира (БРИКС, ШОС, СНГ, латиноамериканские и азиатские государства). Впервые соавторами документа выступили Япония и многие члены ЕС, включая Великобританию, Германию, Испанию, Нидерланды и Францию. На сайте МИД РФ отмечено, что «удалось достичь консенсуса по целому ряду принципиальных вопросов, связанных с использованием ИКТ, в частности: технологии должны использоваться исключительно в

---

[1] См.: Текст Резолюции (A/RES/56/19) от 29 ноября 2001 г.// Официальный сайт ООН; URL: http://www.ifap.ru/ofdocs/un/5619.pdf (дата обращения 28.02.2018).

[2] Проблемы информационной безопасности в международных военно-политических отношениях / Под. ред. А.В. Загорского, Н.П. Ромашкиной. М.: ИМЭМО РАН, 2016. С. 17.

[3] См.: Текст Резолюции (A/RES/65/41) от 8 декабря 2010 г. «Достижения в сфере информатизации и коммуникаций в контексте международной безопасности»// URL: http://www.scrf.gov.ru/news/720.html$http://www.securitylab.ruphp http://www.scrf.gov.ru/documents/6/112.html (дата обращения 02.03.2018); Резолюция, принятая Генеральной Ассамблеей ООН 2 декабря 2014 г., A/RES/69/28 «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» [Электронный ресурс] // Официальный сайт ООН; URL: http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N14/662/43/PDF/N1466243.pdf?OpenElement (дата обращения: 02.03.2018).

мирных целях; в цифровой сфере действуют такие общепризнанные международно-правовые принципы, как неприменение силы или угрозы силой, уважение суверенитета, невмешательство во внутренние дела государств; государства обладают суверенитетом над информационно-коммуникационной инфраструктурой на своей территории; любые обвинения в адрес государств в причастности к кибератакам должны быть подкреплены доказательствами и др.»[1]

С целью сотрудничества стран в данной сфере проводятся Всемирные встречи на высшем уровне по вопросам информационного общества (World Summit on Information Society – ВВУИО). Так, под патронажем ООН и Международного союза электросвязи был проведен Саммит, на котором принят ряд документов по вопросам регулирования глобальных сетей. Саммит был разделен на два этапа: первый прошел в Женеве 10-12 декабря 2003 г.; второй этап – в Тунисе 16-18 ноября 2005 г.

В 2014 г. в Женеве проведена встреча государственных министров и руководителей международных организаций (более 1600 участников), на которой обсуждались итоги Тунисского Саммита и принята «Разработанная ВВУИО + 10 концепция ВВУИО на период после 2015 года»[2]. Она содержит комплекс обновленных приоритетных направлений для совместных действий государств, нацеленных на развитие глобальной экосистемы ИКТ и обеспечение ее информационной безопасности.

Несмотря на значительное количество принятых Генеральной Ассамблеей ООН резолюций и работу Группы правительственных экспертов, занимающейся рассмотрением существующих и потенциальных угроз в сфере информационной безопасности, а также возможных совместных мер по их

---

[1] О принятии Первым комитетом Генассамблеи ООН резолюции «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» // Официальный сайт Министерства иностранных дел РФ; URL: http://www.mid.ru/foreign_policy/news/-/asset_publisher/cKNonkJE02Bw/content/id/1922990 (дата обращения 02.03. 2018)

[2] Разработанная ВВУИО+10 концепция ВВУИО на период после 2015 года [Электронный ресурс] // URL: http://www.itu.int/net/pressoffice/press_releases/2014/pdf/34-ru.pdf (дата обращения 02.03.2018).

устранению, на сегодняшний момент единой концепции создания глобальной системы информационной безопасности пока не принято.

Так, 23 июня 2017 г. в Нью-Йорке завершила работу Группа правительственных экспертов ООН по международной информационной безопасности под председательством ФРГ. Предполагалось, что, как и ранее в 2010, 2013 и 2015 гг., в ходе последнего заседания ГПЭ будет принят ее итоговой доклад, однако прийти к согласованному мнению экспертам не удалось.

Позиция России и ее сторонников (Белоруссия, Китай, Бразилия и др.) основана на необходимости учета угрозы использования информационных технологий в военно-политических целях, возможности влияния ИКТ на национальную безопасность и международный военно-политический баланс. «Западный консенсус» (США, Германия, Франция, Великобритания) признают лишь наличие криминальной и террористической составляющей безопасности в данной области.

Вторая проблема связана с тем, что Россия требует рассмотрения ГПЭ содержания информационных потоков, а не только вопросов безопасности инфраструктуры (как этого хотят США)[1]. Поэтому компромисс по данным вопросам до сих пор не достигнут.

В рамках Совета Европы государствам удалось договориться о принятии и выполнении Конвенции о преступности в сфере компьютерной информации[2], подписанной в Будапеште в 2001 г. В английской версии Конвенция называется «Convention on Cybercrime», однако в переводе на русский язык (перевод на русский язык осуществлен Аппаратом Государственной Думы ФС России) этот документ получил название «Конвенция о преступности в сфере компьютерной информации».

Конвенция направлена на защиту от новых видов преступлений, а также на борьбу с традиционными преступлениями, совершаемыми с использо-

[1] Загорский А.В., Ромашкина Н.П. Указ. соч. С. 24.
[2] Конвенция о преступности в сфере компьютерной информации (ETS № 185) (Заключена в г. Будапеште 23.11.2001 г.) (с изм. от 28.01.2003) // Конвенция на английском языке опубликована не была; http://www.consultant.ru/ (дата обращения 03.03.2018).

ванием информационных технологий. Дополнительный протокол Конвенции призывает устанавливать уголовную ответственность также за акты расистского и ксенофобного характера, совершаемые через компьютерные системы.

Следует отметить, что Конвенция о киберпреступности является единственным международным договором (ратифицировали 53 страны), участниками которого стали не только страны-члены Совета Европы, но и такие государства, как Аргентина, Австралия, Израиль, Канада, США, Япония и др. В 2012 г. Белоруссия выразила желание присоединиться к Конвенции.

В то же время назвать документ универсальным международно-правовым договором нельзя, т.к., например, Россия не является участницей Конвенции о киберпреступности. Несмотря на то, что наша страна принимала участие в разработке этой Конвенции и подписала ее в 2005 г., в 2008 г. она отозвала свою подпись[1]. Российская Федерация категорически не согласна со ст. 32(b), в соответствии с которой позволено получать без согласия страны-участницы доступ к хранящимся на ее территории компьютерным данным, т.е. проводить трансграничные расследования и следственно-оперативные мероприятия. Такую формулировку, по мнению России, можно рассматривать как нарушение суверенных прав стран-участниц. Важно и то, что Конвенция о преступности в сфере компьютерной информации не предусматривает возможность для стран-участниц делать оговорки при присоединении к ней.

В противовес Будапештской конвенции, которую западные политики пытаются «истолковать» как документ «глобального» характера в вопросах кибербезопасности, в сентябре 2011 г Генеральному секретарю ООН было направлено письмо, к которому прилагались «Правила поведения в области обеспечения международной информационной безопасности», получившие название Кодекс информационной безопасности. Он был предложен к рассмотрению на 66-й сессии Генеральной Ассамблеи ООН четырьмя государ-

[1] Россия приняла решение подписать данный документ с заявлением в соответствии с Распоряжением Президента РФ от 15.11.2005 № 557-рп, которое признано утратившим силу Распоряжением Президента РФ от 22.03.2008 № 144-рп. // URL: http://www.consultant.ru

ствами - членами Шанхайской организации сотрудничества (Китаем, Таджикистаном и Узбекистаном) при ведущей роли России. В ноябре 2011 г. на конференции по киберпространству в Лондоне этими странами была представлена концепция Конвенции об обеспечении международной информационной безопасности.

Необходимость принятия данной Конвенции эти государства связывают с тем, что вопросы кибербезопасности имеют огромное значение для мирового сообщества и их следует рассматривать в рамках международного сотрудничества и в духе взаимного уважения. Конвенция предполагает юридически обязывающий характер, не ограничиваясь декларативными заявлениями и формулированием общих принципов поведения государств в информационном пространстве. Она разработана для практической защиты глобальной сети и других информационно-коммуникационных сетевых технологий от угроз и разных «уязвимостей».

Концепция Конвенции содержит ряд весьма востребованных сегодня определений: что такое информационная война, информационное оружие, международная информационная безопасность и др. В тексте Конвенции перечислены возможные угрозы миру и международной безопасности, в том числе деструктивные действия в информационном пространстве, диверсионные действия, психологические войны, информационную экспансию и др.[1]

Конвенция включает некоторые положения, которые безоговорочно принимаются большинством государств. К ним можно отнести: избегать использования ИКТ в ущерб основным правам и свободам человека, реализуемым в информационном пространстве; использование информационных технологий и средств для осуществления враждебных действий и актов агрессии и др. В то же время ряд вопросов вызвали возражение со стороны США, Великобритании и их союзников. В основу противоречия легла система взгля-

[1] Конвенция об обеспечении международной информационной безопасности (концепция) // Официальный сайт Министерства иностранных Дел Российской Федерации; URL: http://www.mid.ru/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/191666 (дата обращения 04.03.2018).

дов, так называемый «западный консенсус», по вопросам использования и управления информацией. Расхождением между российским и западными подходами к информационной безопасности связано с различием в понимании содержания «угрозы». С российской точки зрения важно учитывать влияние информационных технологий на социально-гуманитарную сферу, а наши оппоненты игнорируют данный аспект информационной безопасности.

Другим камнем преткновения в вопросах информационной безопасности стал «информационный суверенитет». Россия и ее сторонники (например, члены СНГ, ОДКБ, ШОС) поддерживают идею о том, что информационные ресурсы должны контролироваться государством в пределах его территориальных границ. Иными словами, предложенная концепция классифицирует ИКТ, включая даже такие сайты, как Twitter и Facebook, в качестве оружия, если их использование нарушает отдельные государственные законы[1].

Обосновывая точку зрения России, А.В. Даниленков пишет, что государственный суверенитет распространяется и на идеальные сегменты национальных информационных пространств, которые соединены воедино во всемирную информационно-телекоммуникационную сеть Интернет. Принадлежность участка сети Интернет к российской государственности обусловлена следующими юридически значимыми обстоятельствами:

1) непосредственная локализация на территории страны возникающих, изменяющихся или прекращающихся и подлежащих нормативному урегулированию общественных отношений (через элементы сетевой инфраструктуры);

2) наличие тесной связи интернет-правоотношения с территорий РФ; в случае с доменами «.рф» и «.ru» – по месту нахождения регистратуры и регистраторов доменных имен, а также ввиду распространения последствий соответствующих правоотношений на РФ, ее частных и публичных субъектов;

3) притяжение к своей территориально-пространственной среде неопределенного круга лиц (субъектов) и объектов воздействия, включая их следующие виды: (информационные посредники, национальная регистратура, реги-

[1] Меркурьева Е.А Указ. соч.

страторы и администраторы доменных имен второго уровня в национальных доменах «.рф» и «.ru», средства виртуальной идентификации и индивидуализации, включая доменные имена в национальных доменах и т.д.; государственные и национальные символы, достопримечательности, объекты культурного наследия, географические названия, исторически памятные события, прочно ассоциируемые и входящие в национально-культурную идентичность России, а также составляющих ее субъектов, местных сообществ и всего многонационального народа Российской Федерации)[1].

Схожая точка зрения выражена в опубликованном в 2013 г. «Таллиннском руководстве по международному праву, применимому в случае кибервойны» (Tallinn Manual on The International Law Applicable to Cyber Warfare)[2]. Согласно разд.1 гл. 1 этого документа «государство может осуществлять контроль над киберинфраструктурой и за ее деятельностью в рамках своей суверенной территории»[3].

Государственный суверенитет над киберинфраструктурой в пределах суверенной территории означает, что, во-первых, государство осуществляет нормативно-правовой контроль над объектами киберинфраструктуры; во-вторых, государство осуществляет территориально-суверенную защиту объектов киберинфраструктуры. При этом такой контроль и защита осуществляются вне зависимости от того, принадлежат ли такие объекты самому государству, частным организациям или индивидам, и вне зависимости от целей использования таких объектов. Единодушный вывод, сделанный группой экспертов в Таллиннском руководстве, что общие принципы и нормы международного права применимы к регулированию киберпространства[4].

Хотя Таллиннское руководство не является обязательным документом для международного сообщества, представляя собой итог работы междуна-

---

[1] См.: Даниленков А.В. Государственный суверенитет Российской Федерации в информационно-телекоммуникационной сети Интернет // Lex russica. 2017. № 7(128). С. 154-165.
[2] URL: www. Cambridge.org/9781107024434. Центр передового опыта НАТО по совместной защите от киберугроз (The NATO Cooperative Cyber Defence Center of Excellence), г. Таллинн.
[3] Касенова М.Б. Международное сотрудничество и управление использованием Интернета // Международное право и международные организации. 2014. № 1. С. 12.
[4] Там же.

родной группы экспертов приглашенных Центром передового опыта НАТО по совместной защите от киберугроз (The NATO Cooperative Cyber Defence Center of Excellence г. Таллин), оно однозначно доказывает, что практических результатов в вопросах создания системы информационной безопасности невозможно достичь без участия всех заинтересованных сторон.

Подписание Конвенции 2011 г. предполагает, что государства соглашаются не использовать ИКТ для вмешательства в дела, относящиеся к внутренней компетенции другого государства, воздерживаться от клеветнических утверждений, а также от оскорбительной или враждебной пропаганды для осуществления интервенции или вмешательства во внутренние дела других государств и будут принимать меры по ограничению распространения «информационного оружия» и технологий его создания. Иными словами, Китай, Россия и Индия рассматривают свободное передвижение информации в сети Интернет как потенциальную угрозу их государственности. Считаем, что с появлением технологий «цветных» революций, где ключевым фактором является управление средствами массовой информации, такие опасения являются обоснованными.

Принятие Конвенции 2011 г. крайне не выгодно США – мировому лидеру в области разработки информационных технологий. Выступая против подписания данной Конвенции, США акцентируют внимание на том, что свободное перемещение информации является основным правом, а данная Конвенция является ничем иным, как попыткой России и других стран ввести цензуру в средствах массовой информации. Бывший Государственный секретарь США Х. Клинтон заявила, что Россия «хотела бы расширить возможности каждого отдельного правительства разработать свои собственные правила, что подорвет, не только права человека, но и право на свободное перемещение информации. Правительства, предлагающие такую повестку, хотят создать национальные барьеры в киберпространстве. Такой подход будет иметь катастрофические последствия для интернет-свободы»[1].

[1] См.: Меркурьева Е.А Указ. соч.

В январе 2015 г. государствами - членами ШОС внесены в качестве официального документа в ООН новые «Правила поведения в области обеспечения международной информационной безопасности». В их основу положены подходы, одобренные по инициативе государств - членов ШОС в ходе 66-й сессии Генеральной Ассамблеи ООН в 2011 г. Ключевой особенностью инициативы 2015 г. является «миротворческий» характер положений документа, предполагающий не регулирование правил ведения «кибервойн», а предотвращение конфликтов в информационном пространстве. В нем закреплены обязательства государств - членов ООН:

1) не применять информационно-коммуникационные технологии в целях нарушения международного мира и безопасности;

2) не вмешиваться во внутренние дела других государств для подрыва их политической, экономической и социальной стабильности;

3) исполнять обязательства по воздержанию от применения силы или угрозы силой в ходе разрешения международных споров, возникающих в цифровой сфере[1].

«Правила поведения в области обеспечения международной информационной безопасности» 2015 г. в отличие от 2011 г. имеют особенности, к которым следует отнести расширение раздела о правах человека. Устанавливается, что права, которые человек имеет в оффлайновой среде, должны защищаться и в онлайновой среде, при этом пользование данными правами может быть сопряжено с некоторыми ограничениями в соответствии со ст. 19 Международного пакта о гражданских и политических правах 1966 г.[2] Особе внимание также уделено интернационализации управления сетью Интернет. Подчеркнута важность «наращивания потенциала» в сфере информационной

---

[1] Об инициативе стран-членов ШОС «Правила поведения в области обеспечения международной информационной безопасности» // Официальный сайт МИД РФ. – Режим доступа: URL: http://www.mid.ru/mezdunarodnaa-informacionnaa-bezopasnost/-/asset_publisher/UsCUTiw2pO53/content/id/916241 (дата обращения 05.03.2018).

[2] Международный пакт о гражданских и политических правах (Нью-Йорк, 19 декабря 1966 г.) // Сборник действующих договоров, соглашений и конвенций, заключенных с иностранными государствами. – М., 1978 г. Вып. XXXII. С. 44

безопасности и оказания развивающимся странам содействия в преодолении «цифрового разрыва».

К сожалению, российские инициативы по формированию международной системы информационной безопасности не всегда находят поддержку, что зачастую вызвано политическими амбициями и соперничеством государств. Разногласия и взаимное недоверие на площадке ООН препятствуют консолидации сил в координации действий по созданию международной коалиции.

Несмотря на это, Россия продолжает продвигать идею налаживания сотрудничества по укреплению информационной безопасности. Так, в июле 2016 г. Санкт-Петербурге на XV Совещании руководителей специальных служб, органов безопасности и правоохранительных органов иностранных государств состоялась презентация российского проекта универсальной Конвенции «О сотрудничестве в сфере противодействия информационной преступности»[1]. Предложенная Конвенция, носящая по содержанию всеобъемлющий характер, сфокусирована на преступлениях в сфере использования ИКТ и направлена на обеспечение ответственности. Проект обсуждали на закрытом мероприятии под эгидой ООН в Вене, но в открытом доступе 52-страничный документ пока не опубликован.

Как подчеркивают в МИД, документ учитывает многочисленные происшедшие с 2001 г. (с момента принятия Будапештской конвенции) в сфере IT-преступлений изменения и приемлем для всех членов ООН, а не только для западных стран. Главной целью Конвенции является «содействие принятию и укреплению мер, направленных на эффективное предупреждение преступлений и иных противоправных деяний в сфере информационно-коммуникационных технологий и борьбу с ними»[2].

В число таких преступлений согласно Конвенции входят: неправомерный доступ к информации в электронной форме; неправомерный перехват

---

[1] О презентации российского проекта универсальной конвенции о сотрудничестве в сфере противодействия информационной преступности // Официальный сайт Министерства иностранных дел Российской Федерации от 28.07.2016; URL: http://www.mid.ru/foreign_policy/news/-/asset_publisher/cKNonkJE02Bw/content/id/2375819 (дата обращения 04.02.2018).

[2] Та же.

или воздействие на информацию; нарушение функционирования ИКТ; создание, использование и распространение вредоносных программ, распространение спама; незаконный оборот устройств; хищение с использованием ИКТ; преступления, связанные с детской порнографией; сбор информации в электронной форме путем введения пользователя в заблуждение; преступления, связанные с охраняемой внутригосударственным правом информацией. При этом документ не предусматривает возможности деятельности спецслужб в сетях других стран и содержит отдельную статью, касающуюся защиты суверенитета.

В документе подробно описывается порядок оказания взаимной правовой и технической помощи по уголовным делам, связанным киберпреступностью. Кроме того, одна из статей Конвенции предусматривает создание круглосуточного контактного центра, предназначенного для оказания неотложной помощи в целях расследований киберпреступлений.

К элементам «мягкого права» при формировании основ взаимного сотрудничества государств в данной сфере можно отнести принятые в сентябре 2011 г. Комитетом министров Совета Европы ряд важных документов. Речь не идет о международном договоре или резолюции Совета Безопасности ООН, которые имеют обязательную юридическую силу. Но поскольку Россия и большинство стран Европы являются членами Совета Европы, рекомендательные нормативные документы являются отличным примером возможного компромисса. Так, Совет Европы принял декларацию Комитета министров о принципах управления Интернетом[1], в которой были одобрены рекомендации для государств - членов СЕ в области защиты и развития всеобщего, целостного и открытого характера Интернета. Декларация содержит десять принципов управления Интернетом, среди которых на государства возлагается роль по обеспечению защиты общественных интересов в между-

[1] Рекомендация CM/Rec (2011) 8 Комитета министров государствам-членам о защите и продвижении универсального характера, целостности и открытости Интернета (Принята Комитетом министров 21.09. 2011г.) [Электронный ресурс]// Councul of Europe http://hr-online.org.ua/npanel/webdata/299/12_rekomendatsiya_cmrec(2011)8.pdf (дата обращения 05.03.2018).

народной публичной политике, связанной с Интернетом. Таким образом, Совет Европы создал прецедент, установив принцип ответственности за нанесения трансграничного ущерба.

Еще одной составляющей «мягкого права» являются акты некоторых международных организаций, занятых в нормотворчестве в области информационного права, например, Организации экономического сотрудничества и развития (ОЭСР), которая хотя и не является всемирной организацией, но объединяет тридцать четыре государства. Ей приняты следующие рекомендательные документы: Руководящие указания о защите частной жизни и трансграничном перемещении персональных данных 1980 г., Министерская декларация по защите неприкосновенности частной жизни в глобальных сетях 1998 г., Министерская декларация о цифровой экономике: инновации рост и социальное процветание 2016 г. и др.[1]

В 2007 г. Международный союз электросвязи предложил создать Глобальную программу кибербезопасности, которая представляет собой основу международного сотрудничества, созданную с целью разработать предложения по стратегии поиска решений в области укрепления доверия и безопасности в условиях информационного общества. Хотя Программа представляет собой рамочную основу, но в то же время уделяется внимание и текущей работе с различными странами, чтобы обеспечить оперативное реагирование на национальные, региональные и глобальные киберугрозы. Важным направлением выступает Международное многостороннее партнерство против киберугроз (ИМПАКТ), к которому присоединились уже более 140 стран. Некоторые государства получают от МСЭ помощь в создании на национальном уровне групп и центров реагирования на компьютерные угрозы[2].

В качестве рекомендаций для стран Евросоюза в 2013 г. разработана Стратегия кибербезопасности Европейского Союза: открытое, безопасное и защищенное киберпространство (Cybersecurity Strategy of the European Union:

---

[1] Цит по: Талапина Э.В. О возможностях правового регулирования Интернета // Труды Института государства и права Российской академии наук. 2016. № 3(55). С. 63.

[2] См.: Глобальная программа кибербезопасности МСЭ. Указ. соч.

An Open, Safe and Secure Cyberspace) (Брюссель, 7 февраля 2013 г.)[1]. Хотя документ и не имеет официального статуса, но он вызвал бурное обсуждение как в странах НАТО, так и в России.

Положения Таллиннского руководства при определенных условиях санкционируют применение неограниченно широкого спектра кинетического оружия против источника киберугрозы, силовые действия военных в отношении гражданских лиц, причастных к кибератакам (за счет причисления их к статусу комбатантов), а также военные кибероперации, направленные против критической инфраструктуры, включая АЭС и дамбы плотин. По мнению О.В. Демидова, наличие подобных положений дает основание утверждать, что Таллиннское руководство дает государствам международно-правовую основу для ведения наступательной кибервойны. В тексте документа усматривается попытка легитимизации конфликтов в киберпространстве как формы поведения государств и действующих в их интересах посредников (англ. proxy actors) на мировой арене[2].

Резюмируя, отметим, что сегодня параллельно происходит формирование двух конкурирующих моделей информационной безопасности, которые строятся на разных основополагающих принципах. Разногласия по важным вопросам обеспечения информационной безопасности не позволяет оппонентам прийти к консенсусу и принять международный документ глобального характера. Актуальность сотрудничества стран по разработке и принятию такого акта подчеркивает Ю.В. Жилкина, «сегодня необходимо создать концепцию глобальной информационной безопасности, т.к. безопасность достигается в современном мире не за счет другого государства, а одновременно с безопасностью других причастных государств»[3].

---

[1] Стратегия кибербезопасности Европейского союза была представлена Совместным информационным докладом Европейскому Парламенту, Совету Европы, Европейскому экономическому и социальному комитету и Комитету регионов. – URL: http:// eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf (неофициальный перевод О.В. Демидова и М.Б. Касеновой).

[2] Кибербезопасность и управление интернетом: Документы и материалы для российских регуляторов и экспертов /Отв. ред. М.Б. Касенова; сост. О.В. Демидов и М.Б. Касенова. М., 2013. С. 62.

[3] Жилкина Ю.В. Международная безопасность в эпоху глобализации мировой экономики // Национальные интересы: приоритеты и безопасность. 2010. № 25. С. 65.

Считаем, что в круг вопросов, которые следует обсудить на международном уровне, должны входить:

1) нахождение консенсуса между странами в использовании терминологического аппарата в сфере информационной безопасности. Сегодня на первый план выходит обсуждение вопросов единообразия применяемых терминов и понятий, адекватность переводов этих понятий на другие языки мира, включая русский, а также правовая квалификация используемых понятий и их содержательное значение;

2) выявление факторов, влияющих на состояние международной информационной безопасности с учетом наличия угроз террористического, криминального и военного характеров. Государствам необходимо прийти к согласию по вопросам, связанным с различием в понимании содержания «информационная угроза», т.к. с российской точки зрения важно учитывать влияние информационных технологий на социально-гуманитарную сферу, а наши оппоненты игнорируют данный аспект информационной безопасности;

3) определение путей и взаимоприемлемых мер предотвращения использования информационных технологий в террористических и других преступных целях, а также мер по ограничению применения информационного оружия в отношении критически важных инфраструктур других государств;

4) закрепление принципа государственного суверенитета над «национальными сегментами» глобальной сети Интернет.

Инициативы Российской Федерации за последние двадцать лет в данной сфере, наглядно показывают, что наша страна стремиться к выработке многостороннего и взаимоприемлемого международно-правового документа, направленного на минимизацию информационных угроз глобальному миру и национальной безопасности государств.

2.2. Региональное и двустороннее сотрудничество России в сфере обеспечения информационной безопасности

При отсутствии международного регулирования рассматриваемой проблемы страны разрабатывают национальные документы, которые могут способствовать принятию международных актов в области обеспечения информационной безопасности. Так, Международная стратегия по действиям в киберпространстве, подписанная Президентом США в мае 2011 г. закрепляет, что «разработка норм, регулирующих поведение государства в киберпространстве, как не требует изобретения заново международного права, так и не делает действующие международно-правовые нормы утратившими силу. Существующие международно-правовые нормы, регулирующие поведение государств в мирное время или в период конфликтов, также применяются к киберпространству. Тем не менее, уникальные свойства, присущие сетевым технологиям, требуют дополнительной работы для уточнения того, как указанные нормы применяются и какие дополнительные толкования могут быть необходимы для их восполнения»[1].

Среди потенциальных угроз в Стратегии указаны экономические, военные, техногенные угрозы экономике, бизнесу, обществу и национальной безопасности. Особое внимание (отдельный параграф) посвящен вопросам информационного сдерживания. В ответ «на кибератаки США готовы использовать любые средства – дипломатические, экономические и военные»[2].

Приняты похожие Стратегии еще в ряде стран, например, Стратегия кибербезопасности Финляндии 2013 г, Национальная политика кибербезопасности Индии 2013 г. и др.[3]

---

[1] Цит. по: Даниленков А.В. Государственный суверенитет Российской Федерации в информационно-телекоммуникационной сети Интернет // Lex russica. 2017 . № 7. С. 160.

[2] См.: Кибербезопасность и управление интернетом: Документы и материалы для российских регуляторов и экспертов /Отв. ред. М.Б. Касенова; сост. О.В. Демидов и М.Б. Касенова. М.: Статут, 2013. С. 188-208.

[3] Там же.

В России действуют Основы государственной политики РФ в области международной информационной безопасности на период до 2020 г. В документе среди основных направлений государственной политики в данной сфере отмечено продвижение российской инициативы в разработке и принятии под эгидой ООН Конвенции о сотрудничестве в сфере противодействия информационной преступности, а также активизация работы по вопросам сотрудничества в сфере региональной безопасности. По инициативе России проблематика международной информационной безопасности рассматривается в рамках ОБСЕ, ШОС, ОДКБ, Международного союза электросвязи, в ходе Всемирной встречи на высшем уровне по вопросам информационного общества, в рамках СНГ. Работа также ведётся «на полях» таких форумов, как «Группа восьми», «Группа двадцати», БРИКС[1].

Особенно показательная в этом плане нормотворческая деятельность регионального уровня с участием России, имеющая тенденцию к нарастанию. Большую работу по формированию общего правового информационного пространства проводит Межпарламентская Ассамблея государств-участников СНГ (МПА СНГ). Одним из первых актов, относящихся к информационной сфере, стало Соглашение «О сотрудничестве в области информации» и Рекомендательный законодательный Акт «О принципах регулирования информационных отношений в государствах - участниках Межпарламентской Ассамблеи» (1993 г.). В 1996 г. была принята Концепция формирования информационного пространства Содружества Независимых Государств[2]. В 2002 г. был разработан и принят Модельный закон СНГ «О международном информационном обмене», предусматривающий защиту интересов участников при международном информационном обмене.

Советом глав правительств СНГ в 2008 г. была утверждена Концепция сотрудничества государств - участников Содружества Независимых Государств в сфере обеспечения информационной безопасности, которая пред-

[1] См.: Зиновьева Е.С. Указ. соч.
[2] Стратегический вектор обеспечения международной информационной безопасности Сборник / [сост. М.А. Вус, О.С. Макаров] / Предисловие: чл.-кор. РАН Р.М. Юсупов. СПб., 2016. С.10.

ставила совокупность согласованных официальных взглядов о целях, принципах и основных направлениях межгосударственного сотрудничества в сфере информационной безопасности.

Для реализации Концепции была предусмотрена разработка Рекомендаций по совершенствованию и гармонизации национального законодательства государств - участников СНГ. Рекомендации с некоторым запозданием нашли своё отражение в Перспективном плане модельного законотворчества СНГ на 2011–2015 гг. [1]

В 2012 г. была утверждена Стратегия сотрудничества государств - участников Содружества Независимых Государств в построении и развитии информационного общества до 2015 г., которая сегодня заменена Стратегией сотрудничества государств - участников СНГ в построении и развитии информационного общества на период до 2025 г.[2] Оба документа отражают общее видение построения информационного пространства и общества для стран СНГ.

В ноябре 2013 г. подписано Соглашение о сотрудничестве государств - участников СНГ в области обеспечения информационной безопасности[3], направленное на проведение совместных скоординированных мероприятий по обеспечению информационной безопасности в государствах - участниках данного Соглашения. Соглашение способствует гармонизации норм права государств СНГ и усилению роли правовых институтов при разработке мер по обеспечению информационной безопасности.

В рамках мероприятий Программы сотрудничества государств - участников СНГ по борьбе с терроризмом и иными насильственными проявления-

---

[1] Вус М.А., Макаров О.С. К вопросу о разработке рекомендаций по совершенствованию и гармонизации национального законодательства государств - участников СНГ в сфере обеспечения информационной безопасности // Информатизация и связь. 2012. № 1. С. 5-8.

[2] Стратегия сотрудничества государств – участников СНГ в построении и развитии информационного общества на период до 2025 года [Электронный ресурс] (от 28 октября 2016 г.) // Официальный Интернет-портал СНГ; URL: http://www.e-cis.info/page.php?id=22902 (дата обращения 06.03.2018).

[3] Распоряжение Правительства РФ от 15 ноября 2013 г. № 2120-р «О подписании Соглашения о сотрудничестве государств - участников Содружества Независимых Государств в области обеспечения информационной безопасности // Собрание законодательства РФ. 2013. № 47. Ст. 6135.

ми экстремизма в 2013 г. разработаны Рекомендаций по правовому регулированию эксплуатации открытых телекоммуникационных сетей (ОТКС) для предупреждения их использования в террористических и иных противоправных целях[1]. Документ, успешно прошедший экспертизу в парламентах государств - участников СНГ, также принят Межпарламентской Ассамблеей.

В 2014 г. Постановлением МПА СНГ принят базовый модельный закон «Об информации, информатизации и обеспечении информационной безопасности»[2], консолидирующий порядок формирования и использования ИКТ и информационных ресурсов государств СНГ, нацеленный на обеспечение процессов информатизации на новом этапе безопасного и более эффективного взаимодействия субъектов в едином информационном пространстве СНГ.

По мнению В.И. Ступакова, такие международные акты необходимы государствам СНГ для защиты национального суверенитета в информационном пространстве, противодействия нарушениям конфиденциальности информации, целостности и доступности компьютерных систем и сетей и компьютерной информации, для предотвращения злоупотреблений такими системами, сетями и информацией. Особое внимание в них должно быть уделено мерам административной и уголовной ответственности за противоправные деяния, направленные на подрыв информационной безопасности на национальном и международном уровнях, и предоставлению государственным органам и органам СНГ полномочий, достаточных для эффективной борьбы с правонарушениями в информационной сфере[3].

Региональный уровень сотрудничества России в рассматриваемой сфере представлен также Программой совместных действий государств - членов Организации Договора о коллективной безопасности (ОДКБ). Учитывая

---

[1] Постановление МПА СНГ от 20.11.2013 № 39-25 «Рекомендаций по правовому регулированию эксплуатации открытых телекоммуникационных сетей (ОТКС)» // Информационный бюллетень МПА СНГ. 2014. № 60. С. 458-477.

[2] Модельный закон СНГ «Об информации, информатизации и обеспечении информационной безопасности (Постановление МПА СНГ от 28.11.2014 г. № 41-15) [Электронный ресурс]// URL: http://www.parliament.am/library/modelayin%20orenqner/310.pdf (дата обращения 06.03.2018)

[3] Ступаков В.И. Инициативы евразийских государств по обеспечению международной и региональной информационной безопасности // Международное сотрудничество Евразийских государств: политика, экономика, право. 2015. № 3. С. 78.

важность проблемы, в 2010 г. обеспечение информационной безопасности, как актуальное направление сотрудничества, было закреплено в ст. 8 Устава ОДКБ, согласно которой государства - члены взаимодействуют в сфере информационной безопасности[1]. В том же году Совет коллективной безопасности ОДКБ утвердил Положение о сотрудничестве государств - членов ОДКБ в сфере информационной безопасности.

Для реализации мероприятий, предусмотренных Положением о сотрудничестве, были разработаны Рекомендации по сближению и гармонизации законодательства государств - членов ОДКБ в сфере информационно-коммуникационной безопасности, принятые Парламентской Ассамблеей ОДКБ в 2014 г.[2] В документе акцентировано внимание на необходимости активной согласованной информационной политики государств - членов ОДКБ и создании совместного потенциала по противодействию информационным угрозам.

Тесное сотрудничество по созданию системы информационной безопасности ведется в рамках Шанхайской организации сотрудничества. В июне 2006 г. ШОС приняла Заявление глав государств-членов по международной информационной безопасности[3]. В этом документе выражена озабоченность тем, что в настоящее время появляется реальная опасность использования ИКТ в целях, способных нанести серьезный ущерб безопасности человека, общества и государства в нарушение основополагающих принципов равноправия и взаимного уважения, невмешательства во внутренние дела суверенных государств, мирного урегулирования конфликтов, неприменения силы, соблюдения прав человека. При этом угрозы использования информационных технологий в преступных, террористических и военно-

---

[1] Устав Организации Договора о коллективной безопасности (Кишинев, 7 октября 2002 г.) // Собрание законодательства РФ. 2004. № 3. С. 163.

[2] Для совершенствования системы информационной безопасности в ОДКБ /М.А. Вус, М.М. Кучерявый, О.С. Макаров, Г.И. Перекопский // Власть. 2014. № 8. С.37-40.

[3] О подписании итоговой декларации саммита Шанхайской организации сотрудничества, Шанхай, 15 июня 2006 г. [Электронный ресурс] // Официальный портал Министерства иностранных дел РФ. URL: http://www.mid.ru/sanhajskaa-organizacia-sotrudnicestva-sos-/-/asset_publisher/0vP3hQoCPRg5/content/id/400410 (дата обращения 06.03.2018).

политических целях, несовместимых с обеспечением международной безопасности, могут реализовываться как в гражданской, так и в военной сферах и привести к тяжелым политическим и социально-экономическим последствиям в отдельных странах, регионах и в мире в целом, к дестабилизации общественной жизни государств. Главная цель документа – намерение государств скоординировано принимать меры для реагирования на угрозы безопасности в информационной сфере.

В ходе последующих мероприятий ШОС принимались новые документы, регламентирующие поведение государств в информационном пространстве и ответственное использование ИКТ, однако намерение действовать, полагаясь на единые меры доверия между странами, оставалось неизменным.

В 2009 г. между Правительствами государств-членов ШОС заключено Соглашение «О сотрудничестве в области обеспечения международной информационной безопасности»[1]. Соглашение открыто для присоединения любых других государств. Приложение № 2 к Соглашению содержит перечень основных угроз в области международной информационной безопасности, среди которых:

1) разработка и применение информационного оружия, подготовка и ведение информационной войны;

2) информационный терроризм;

3) информационная преступность;

4) использование доминирующего положения в информационном пространстве в ущерб интересам и безопасности других стран;

5) распространение информации, наносящей вред общественно-политической и социально-экономической системам, духовной, нравственной и культурной среде других государств.

[1] Распоряжение Правительства РФ от 16 июля 2009 г. № 984-р «Об утверждении Соглашения между правительствами государств - членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности» (вступило в силу с 05.01.2012)// Текст распоряжения официально опубликован не был; http://www.consultant.ru/

6) угрозы безопасному, стабильному функционированию глобальных и национальных информационных инфраструктур, имеющие природный и (или) техногенный характер.

Шанхайская организация сотрудничества играет важную роль в создании глобальной системы информационной безопасности, ведь именно эта региональная межправительственная организация предлагала на рассмотрение Генеральной Ассамблеи ООН в 2011 г. и в 2015 г. универсальные Кодексы информационной безопасности.

В последние годы активизировался процесс сотрудничества в данной сфере со странами БРИКС. В июле 2017 г. в Ханчжоу (Китай) была проведена встреча министров стран БРИКС, отвечающих за регулирование отрасли информационно-коммуникационных технологий, на которой принята Декларация третьей встречи министров связи стран БРИКС[1]. В п. 13 Декларации отмечено, что страны-члены БРИКС на основе тесной координации действий стремятся углублять сотрудничество в решении проблем, относящихся к безопасности при использовании ИКТ, укреплять диалоги и обмены, отстаивать создание международных правил, управляющих использованием инфраструктуры, защитой данных и использованием Интернета, улучшать механизмы управления и реагирования на чрезвычайные ситуации, которые устраняют международные угрозы при использовании ИКТ, и совместно строить безопасную и защищенную сеть.

Россия стремится к установлению как многосторонних, так и двусторонних партнерских отношений в сфере обеспечения безопасности использования ИКТ. Первым документом стало Совместное российско-американское заявление об общих вызовах безопасности на рубеже XXI века, которое в сентябре 1998 г. подписали президенты двух стран[2]. Но на том этапе добить-

[1] Декларация третьей встречи министров связи стран БРИКС от 27 июля 2017 года [Электронный ресурс] // Официальный сайт Министерства связи и массовых коммуникаций Российской Федерации. URL: http://minsvyaz.ru/ru/events/37255/ (дата обращения 06.03.2018).
[2] Демидов О.В. Указ. соч. С. 55.

ся существенных успехов не удалось, т.к. документ не содержал четкой программы международного сотрудничества.

Дальнейшее развитие данное направление сотрудничества получило лишь спустя 13 лет, с появлением Stuxnet, когда мировой рынок киберпреступности стал измеряться миллиардами долларов США, а китайский кибершпионаж стал рассматриваться в качестве одной из приоритетных угроз национальной безопасности США. Итогом консенсуса между странами стал пакет из трех соглашений, подписанный в ходе встречи В.В. Путина и Б. Обамы на полях саммита G8 в Дублине (Ирландия, 17 июня 2013 г.)[1].

В рамках заключенных соглашений предполагается реализация ряда мер доверия в области использования ИКТ и, прежде всего, организация оперативного обмена данными через каналы национальных центров реагирования на компьютерные инциденты (CERT). Такой обмен направлен, в первую очередь, на предупреждение угроз критически важной информационной инфраструктуры.

На сегодняшний момент двусторонние соглашения, задающие вектор национальной и международной политике стран в области обеспечения информационной безопасности в киберпространстве, Россия заключила с Бразилией[2], Белоруссией[3], Индией[4], Китаем[5] и др.

---

[1] Демидов О.В. Указ. соч. С. 55.

[2] Соглашение между Правительством Российской Федерации и Правительством Федеративной Республики Бразилии о сотрудничестве в области обеспечения международной информационной и коммуникационной безопасности (Москва, 14 мая 2010 г.) // Текст Соглашения официально опубликован не был; URL: http://base.garant.ru/70226648/ (дата обращения 06.03.2018).

[3] Соглашение между Правительством Российской Федерации и Правительством Республики Беларусь о сотрудничестве в области обеспечения международной информационной и коммуникационной безопасности (25 декабря 2013 г.) // Информационный портал Республики Беларусь;. URL: http://naviny.org/2013/12/25/by4525.htm (дата обращения 06.03.2018).

[4] Соглашение между Правительством Российской Федерации и Правительством Республики Индии о сотрудничестве в области обеспечения безопасности в сфере использования информационно-коммуникационных технологий (15 октября 2016 г.) // Официальный портал Министерства иностранных дел РФ; URL: http://www.mid.ru/foreign_policy/international_contracts/2_contract/-/storage-viewer/bilateral/page-9/51667 (дата обращения 06.03.2018).

[5] О подписании Соглашения между Правительством Российской Федерации и Правительством Китайской Народной Республики о сотрудничестве в области обеспечения международной информационной безопасности (8 мая 2015 г.) //Официальный портал Министерства иностранных дел РФ; URL: http://www.mid.ru/ru/maps/cn/-/asset_publisher/WhKWb5DVBqKA/content/id/1257295

Плодотворный диалог России в рамках СНГ, ШОС, БРИКС наглядно свидетельствует об эффективности выстраивания межгосударственного общения на основе принципов равноправия, учета интересов друг друга и уважения права государств на выбор собственной модели информационной безопасности.

2.3. Взаимодействие государств по созданию системы международной информационной безопасности

Согласно п. 7 Основ государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года «под системой международной информационной безопасности понимается совокупность международных и национальных институтов, призванных регулировать деятельность различных субъектов глобального информационного пространства»[1].

Вопросами информационной безопасности занимаются ведущие международные и региональные организации, среди которых Организация Объединенных Наций, Азиатско-Тихоокеанское экономическое сотрудничество (АТЭС, Asia-Pacifi c Economic Cooperation); Ассоциация государств Юго-Восточной Азии (АСЕАН, Association of SouthEast Asian Nations); Совет Европы (Council of Europe), Европол (Europol); Интерпол (Interpol, International Criminal Police Organization); Альянс НАТО (NATO, North Atlantic Treaty Organization); Организация американских государств (ОАГ, Organization of American states); Организация экономического сотрудничества и развития (ОЭСР, Organisation for Economic Cooperation and Development); Международный союз электросвязи (МСЭ, International Telecommunication Union); Форум по управлению Интернетом (Internet Governance Forum); Междуна-

[1] Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года (утв. Президентом РФ 24 июля 2013 № Пр-1753 // Официальный сайт Совета Безопасности РФ; URL: http://www.scrf.gov.ru. (дата обращения 18.02.2018).

родная некоммерческая организация (ICANN, Internet Corporation for Assigned Names and Numbers) и др.[1]

Анализ всех структур и органов международных и региональных организаций, занимающихся вопросами информационной безопасности, ввиду значительного их объема не представляется возможным, поэтому остановимся на некоторых их них.

К органам международного уровня, занимающимся разработкой нормотворческой базы в сфере информационной безопасности, следует отнести Генеральную Ассамблею ООН, Группу правительственных экспертов, а также проводимые под патронажем ООН и Международного союза электросвязи саммиты, ВВУИО и др.

Среди международных организаций при ООН важную роль играет, созданный в 2006 г. по инициативе МЭС, Форум по управлению Интернетом (IGF, Internet Governance Forum). Руководство IGF осуществляет Многосторонняя консультационная группа – MAG (Multistakeholder Advisory Group), формируемая Секретариатом ООН из представителей правительств, частного сектора, научных сообществ и общественности. Для обсуждения вопросов и принятия решений MAG собирается три раза в год на очные двухдневные закрытые собрания в Женеве. Среди тем, рассматриваемых на форуме, большое внимание уделяется вопросам информационной безопасности и пресечения киберпреступности[2].

Для привлечения к участию в IGF разных регионов, стран и сообществ в его структуре предусмотрены «инициативы» (regional and national initiatives), представляющие собой региональные и национальные форумы IGF, осуществляющие поддержку глобальных инициатив IGF на местах. Примером может служить Российский Форум по управлению Интернетом,

---

[1] Петренко А.А., Петренко С.А. Киберучения: методические рекомендации // Вопросы кибербезопасности. 2015. № 3(11). С. 3.

[2] Focus session (security): legal and other frameworks: spam, hacking and cybercrime 23 October 2013 // Internet Governance Forum: http://www.intgovforum.org/cms/2013-bali/igf-2013-transcripts/121-igf-2013/preparatory-process-42721/1401-focus-session-security-legal-and-other-frameworks-spam-hacking-and-cybercrime (дата обращения 09.03.2018).

организованный в 2010 г. 6 апреля 2018 г. в Санкт-Петербурге состоится Девятый российский форум по управлению Интернетом (RIGF 2018), одна из секций которого будет посвящена вопросам глобальной информационной безопасности[1].

Значимую роль в контроле над именами и адресами Интернета, а также координации работ по выработке параметров Интернет-протоколов осуществляет частная некоммерческая организация ICANN (Internet Corporation for Assigned Names and Numbers), зарегистрированная в штате Калифорния и подчиняющаяся законам США. Подобная ситуация не может не вызывать озабоченности у других государств, в том числе у России, которая выступает за интернационализацию функций ICANN и передачу их Международному союзу электросвязи. В 2009 г. подписан Меморандум о взаимопонимании между ICANN и российским общегосударственным объединением «Ассоциация документальной электросвязи», в результате которого Россия стала первой страной интернационализированного имени на кириллице «.рф»[2].

Ведущей организацией Евросоюза в данной области является Европейское агентство сетевой и информационной безопасности (ENISA, European Network and Information Security Agency), учрежденное в 2004 г. Все государства-участники ЕС представлены в агентстве одним офицером связи от каждой из стран ЕС и Европейской экономической зоны, а также представителями от Европейской Комиссии и Совета ЕС. Согласно ст. 2 Регламента ENISA основными целями организации являются:

1) расширение возможностей Евросоюза и международного делового сообщества по своевременному и качественному решению проблем кибербезопасности;

2) повышение общего уровня компетенции Европейской Комиссии и стран ЕС по вопросам кибербезопасности;

---

[1] Девятый российский форум по управлению интернетом (RIGF 2018) состоится 6 апреля 2018 г. в Санкт-Петербурге // Официальный Интернет-портал http://rigf.ru/about/ (дата обращения 09.03.218)

[2] См.: Загорский А.В. Указ. соч. С. 38

3) повышение общей культуры осведомленности Евросоюза по вопросам кибербезопасности;

4) содействие Европейской Комиссии в вопросах развития законодательства в области кибербезопасности и разработки соответствующей организационно-распорядительной и технической документации[1].

В ENISA создана Команда экстренного компьютерного реагирования Евросоюза (European Union Computer Emergency Response Team), которая отражает кибератаки нацеленные на институты Евросоюза и органы государственной власти и оказывает помощь государствам-членам в случае информационных сбоев. Поддержку ENISA оказывают и другие автономные агентства Евросоюза, например, агентство безопасности морского сообщения (EMSA, штаб-квартира в Лиссабоне); агентство авиационной безопасности (EASA, штаб-квартира в Кельне); агентство по судебному сотрудничеству и полицейское ведомство (Eurojust и Europol, штаб-квартиры в Гааге) и др.

Важную роль в борьбе с киберпреступностью на территории Европейского Союза играет структурное подразделение Европола – Европейский центр по борьбе с киберпреступностью (European Cybercrime Centre, ECC), который действует с января 2013 г.

ECC занимается созданием оперативных и аналитических мощностей, необходимых для обеспечения быстрого реагирования на киберпреступления, а также организацией взаимодействия официальных ведомств ЕС и стран-членов с международными партнерами. Мандат Центра определяет следующие сферы ответственности:

- борьба с преступлениями, совершаемыми организованными преступными группами, целью которых является получение незаконных доходов в особо крупных размерах (с такими преступлениями как мошенничество с кредитными картами или банковскими операциями);

[1] Петренко А.А., Петренко С.А. Киберучения: методические рекомендации // Вопросы кибербезопасности. 2015. № 3 (11). С. 4.

- борьба с преступлениями, наносящими серьезный вред жертве, в частности с растлением и совращением малолетних;
- борьба с действиями, направленными на причинение вреда или выведение из строя инфраструктуры и информационных систем ЕС[1].

Центр занимается сбором и обработкой данных, оказанием информационной, технической и криминалистической поддержки соответствующим подразделениям правоохранительных органов стран-членов ЕС, координацией совместных расследований, обучением и подготовкой специалистов. European Cybercrime Centre содействует проведению необходимых исследований и созданию программного обеспечения (R&D), занимается оценкой и анализом существующих и потенциальных угроз и рисков, составлением прогнозов и предупреждений. В сферу деятельности Центра также входит помощь судьям и прокурорам.

В повестке НАТО вопрос об обеспечении кибербезопасности был поднят на саммите в Праге в ноябре 2002 г., когда лидеры стран Альянса выразили готовность усилить возможности по оказанию противодействия информационным атакам. Одним из первых практических шагов в данном направлении стало создание в 2008 г. Управления по осуществлению кибероборо-ны. Функционально Управление призвано инициировать и координировать ответные действия в случае кибератаки, направленной против кого-либо из государств-членов НАТО или же самой НАТО[2].

Созданный в октябре 2008 г. в Таллине Центр передового опыта по совместной защите от киберугроз получил аккредитацию при НАТО и статус международной военной организации. Хотя Центр и не наделен оперативными функциями, а служит в качестве исследовательского и обучающего органа, он «аккумулирует, создает и распространяет знание по ключевым вопросам кибербезопасности внутри НАТО, между государствами Альянса и его партнерами». Эксперты из Центра киберзащиты НАТО рассматривают мили-

[1]Там же. С. 5.
[2] Казаковцев А.В. НАТО и кибербезопасность // Вестник Волгоградского государственного университета. Серия 4: История. Регионоведение. Международные отношения. 2012. № 2. С. 110.

таризацию Интернета в качестве одного из главных и наиболее опасных трендов развития мирового киберпространства: «современные военные структуры готовы использовать информационное пространство как «параллельное поле битвы» в конфликтах будущего»[1]. В 2013 г. принято Таллиннское руководство по международному праву, применимому к кибервойнам, в котором эксперты определили правила и действия, которые должны быть выполнены государствами в процессе ведения кибератак на их территории или территории других государств.

Согласно «Стратегической концепции обороны и обеспечения безопасности членов Организации Североатлантического договора» (2010 г.) обеспечение безопасности киберсистем относится к числу приоритетных направлений деятельности Альянса. Сегодня созданием централизованной системы киберзащиты занимается Агентство НАТО по связи и информации (NCIA), учрежденное в 2012 г.[2]

НАТО консолидирует усилия по обеспечению информационной безопасности с другими международными организациями. Так, в 2016 г. было подписано Техническое соглашение между Центром НАТО по реагированию на компьютерные инциденты (NATO Computer Incident Response Capability, NCIRC) и группой реагирования на компьютерные происшествия Европейского союза (Computer Emergency Response Team of the European Union)[3].

Важную роль в создании региональной системы информационной безопасности играет сотрудничество в рамках СНГ. Согласно ст. 14 Модельного закона СНГ 2014 г. «Об информации, информатизации обеспечении информационной безопасности»[4] разрабатывают и принимают перспективные программы и планы развития отрасти ИКТ, а также контролируют их исполнение Правительства государств - участников СНГ. В соответствии со ст. 18

---

[1] Казаковцев А.В. Указ. соч. С. 112.

[2] Эволюция кибероборонны НАТО [Электронный ресурс] // URL: http://nk.org.ua/geopolitika (дата обращения 12.03.2018).

[3] Там же.

[4] Модельного закона СНГ «Об информации, информатизации обеспечении информационной безопасности» (принят Постановлением от 28.11.2014 г. Межпарламентской Ассамблей государств - участников СНГ) //Официальный Интернет-портал СНГ; URL: http://www.e-cis.info/

данного акта обеспечение информационной безопасности включает систему мер правового, организационно-технического и организационно-экономического характера по выявлению угроз информационной безопасности, предотвращению их реализации, пресечению и ликвидации последствий реализации таких угроз.

Профильным органом в обсуждаемой сфере до 2011 г. была Комиссия по информационной безопасности, созданная по решению Координационного совета государств - участников СНГ по информатизации при Региональном содружестве в области связи (РСС) в декабре 2004 г.

В 2011 г. она была преобразована в Комиссию РСС по информационной безопасности, а затем в 2016 г. ее функции переданы Рабочей группе высокого уровня по развитию информационного общества (РГВУ)[1]. Среди приоритетных направлений РГВУ выделены:

- выработка рекомендаций по взаимодействию участников Координационного совета в области информационной безопасности на основе анализа международного опыта, современных технических средств и информационных технологий, разработка предложений по их нормативно-правовому обеспечению;
- организация обмена опытом в создании систем и средств обеспечения информационной безопасности информационно-телекоммуникационных систем и сетей;
- подготовка предложений по приоритетным направлениям и формам совместной деятельности в вопросах межгосударственного сотрудничества в области обеспечения информационной безопасности СНГ;
- подготовка рекомендаций по разработке межгосударственных программ в сфере информационной безопасности или соответствующих разделов в межгосударственных программах в области информатизации;

[1] Рабочая группа высокого уровня по развитию информационного общества (РГВУ) // Официальный сайт Регионального содружества в области связи;URL: http://www.rcc.org.ru/

- выработка предложений по гармонизации национального законодательства государств-участников СНГ на основе определения общих критериев и принципов государственного регулирования в сфере защиты информации;
- разработка рекомендаций по прогнозированию потенциальных угроз информационной безопасности государств-участников СНГ и методам защиты от этих угроз или противодействию им[1].

Немаловажным аспектом деятельности РГВУ является сотрудничество с международными организациями в области ИКТ. Рабочая группа наладила взаимодействие с Международным союзом электросвязи (МСЭ) в рамках Глобальной Инициативы по кибербезопасности и прорабатывает возможность оказания помощи в реализации проектов в данной области странам регионального содружества[2].

Вопросами сотрудничества в сфере противодействия информационной преступности занимается Бюро по координации борьбы с организованной преступностью и иными опасными видами преступлений на территории государств - участников СНГ[3], созданное на основании Решения Совета глав правительств СНГ от 24 сентября 1993 г. БКБОП является постоянно действующим органом, предназначенным для обеспечения эффективного взаимодействия министерств внутренних дел и госорганов государств - участников СНГ в борьбе с организованной преступностью, терроризмом, незаконным оборотом наркотических средств и психотропных веществ и иными опасными видами преступлений.

В рамках ШОС создана группа экспертов государств - членов ШОС по международной информационной безопасности с участием представителей

---

[1] Рабочая группа высокого уровня по развитию информационного общества (РГВУ) // Официальный сайт Регионального содружества в области связи;URL: http://www.rcc.org.ru/

[2] См.: Агапов П.В., Ефремова М.А. Международно-правовые основы обеспечения информационной безопасности участников Содружества независимых государств // Юридическая наука и правоохранительная практика. 2015. № 1 (31). С. 176-182.

[3] Бюро по координации борьбы с организованной преступностью и иными опасными видами преступлений на территории государств - участников Содружества Независимых Государств// Официальный Интернет-портал СНГ; RUL: http://vafainculo.e-cis.info/page.php?id=13820

секретариата Организации и исполкома Региональной антитеррористической структуры для выработки плана действий по обеспечению информационной безопасности и определению возможных путей и средств решения проблем ее обеспечения[1].

В рамках сотрудничества стран БРИКС создаются информационные инструменты, например совместный сайт Министерств иностранных дел государств - участников БРИКС. В 2011 г. в целях реализации договоренностей, достигнутых на саммитах БРИКС, создан Национальный комитет по исследованию БРИКС, который призван способствовать формированию единого информационного поля в области исследований БРИКС. На VI саммите БРИКС в июле 2014 г. в Форталезе Россия предложила совместно выработать в рамках БРИКС соглашение о сотрудничестве в области управления Интернетом и обеспечения информационной безопасности[2].

В рамках ОДКБ реализуется утвержденная президентами Программа совместных действий по формированию системы информационной безопасности. Программа охватывает такие направления как совместные научные и исследовательские разработки и обмен информацией о достижениях в этой области, подготовка кадров, унификация нормативно-правовой базы, совместное обеспечение безопасности жизненно важных объектов, проведение совместных мероприятий, направленных на борьбу с преступлениями в сфере информационных технологий. С 2009 г. в рамках ОДКБ проводятся специализированные учения под названием «ПРОКСИ» («Противодействие криминалу в сфере информации»), направленные на отработку опыта совместного противодействия информационной преступности[3].

Российская система регулирования и контроля в области информационной безопасности включает в себя деятельность как общегосударственных,

---

[1] Заявление глав государств-членов ШОС по международной информационной безопасности (г. Шанхай, 15 июня 2006 г.) [Электронный ресурс] // Центральный Интернет-портал ШОС; UTL: http://www.infoshos.ru/ru/?id=94 (дата обращения 21.03.2018).

[2] Панова В.В. Проблемы безопасности и перспективы саммита БРИКС в Уфе // Вестник международных организаций: образование, наука, новая экономика. 2015. Т. 10. № 2. С 133.

[3] См.: Зиновьева Е.С. Указ. соч. С. 50

так и специализированных структур и органов, непосредственно занимающихся вопросами обеспечения информационной безопасности.

Возглавляет всю систему, определяя основные направления государственной политики в области информационной безопасности, Президент РФ. Среди нормативных актов, отражающих официально принятую в России систему взглядов на проблемы обеспечения информационной безопасности, методы и средства защиты жизненно важных интересов личности, общества, государства в информационной сфере, можно выделить: Указ Президента РФ от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы», «Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года», Указ Президента РФ от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» и др.

Кроме того Президент России руководит Советом Безопасности РФ; определяет организационную структуру системы обеспечения информационной безопасности в России; в соответствии с законодательством формирует, реорганизует и упраздняет подчиненные ему органы и силы по обеспечению информационной безопасности РФ; определяет в ежегодных посланиях Федеральному Собранию приоритетные направления государственной политики в области обеспечения информационной безопасности РФ, а также меры по реализации Доктрины информационной безопасности РФ[1].

Согласно п. 33 Доктрины информационной безопасности Российской Федерации организационную основу системы обеспечения информационной безопасности составляют: Государственная Дума Федерального Собрания РФ, Совет Федерации Федерального Собрания РФ, Правительство РФ, Совет Безопасности РФ, федеральные органы исполнительной власти, Центральный банк РФ, Военно-промышленная комиссия РФ, межведомственные органы,

[1] Арламов Е.А., Панасюк Г.О. Анализ состояния информационной безопасности в современной России [Электронный ресурс] // Экономика и менеджмент инновационных технологий. 2016. № 12; URL: http://ekonomika.snauka.ru/2016/12/13291 (дата обращения: 21.03.2018).

создаваемые Президентом и Правительством РФ, органы исполнительной власти субъектов Российской Федерации, органы местного самоуправления, органы судебной власти, принимающие в соответствии с законодательством Российской Федерации участие в решении задач по обеспечению информационной безопасности.

Парламент России формирует законодательную базу по вопросам обеспечения информационной безопасности. Специализироваными законами в данной области являются: Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»; Федеральный закон от 28 декабря 2010 г. № 390-ФЗ «О безопасности»[1]; Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» и др.

Согласно пп. «э» ч. 1 ст. 20 Регламента Государственной Думы[2] в ней образован Комитет Государственной Думы по информационной политике, информационным технологиям и связи, занимающийся вопросами разработки правового обеспечения в сфере инфокоммуникационных технологий.

Правительство РФ в пределах своих полномочий координирует деятельность федеральных органов исполнительной власти и органов исполнительной власти субъектов РФ; предусматривает при формировании проектов федерального бюджета выделение средств, необходимых для реализации федеральных программ в данной области.

Важным элементом в организационной структуре является Совет Безопасности РФ, возглавляемый Президентом России. Непосредственным решением задач, связанных с обеспечением информационной безопасности, занимается Межведомственная комиссия Совета Безопасности РФ по информационной безопасности. Согласно Положению о Межведомственной ко-

---

[1] Федеральный закон от 28 декабря 2010 г. № 390-ФЗ (изм. и доп. от 05.10.2015 № 285-ФЗ) «О безопасности» // Собрание законодательства РФ. 2011. № 1. Ст. 2; 2015. № 41. Ст. 5639.

[2] Постановление Государственной Думы ФС РФ от 22 января 1998 г. № 2134 II ГД «О Регламенте Государственной Думы Федерального Собрания Российской Федерации (с изм. от 21.12. 2017) // Собрание законодательства РФ. 1998. № 7. Ст. 801.

миссии Совета Безопасности РФ по информационной безопасности[1] к ее функциям отнесены: подготовка предложений и рекомендаций Совету Безопасности по выработке и реализации основных направлений государственной политики в области обеспечения информационной безопасности РФ; анализ состояния информационной безопасности ИКС и сетей критически важных объектов инфраструктуры и выработка предложений и рекомендаций федеральным органам исполнительной власти по повышению уровня их защищенности; анализ состояния информационной безопасности ИКС и сетей критически важных объектов инфраструктуры и выработка предложений и рекомендаций федеральным органам исполнительной власти по повышению уровня их защищенности и др.

Следующим органом, осуществляющим реализацию государственной политики, организацию межведомственной координации и взаимодействия, специальные и контрольные функции в области государственной информационной безопасности является Федеральная служба по техническому и экспортному контролю (ФСТЭК России). В соответствии с Положением о ФСТЭК России[2] в ее полномочия входят:

1) обеспечение безопасности информации в системах информационной и телекоммуникационной инфраструктуры, оказывающих существенное влияние на безопасность государства в информационной сфере, в том числе в функционирующих в составе критически важных объектов РФ информационных системах и телекоммуникационных сетях, деструктивные информационные воздействия на которые могут привести к значительным негативным последствиям;

2) противодействие иностранным техническим разведкам на территории РФ;

3) обеспечение защиты информации, содержащей сведения, составляющие государственную тайну, иной информации с ограниченным доступом,

[1] Указ Президента РФ от 6 мая 2011 г. № 590 «Вопросы Совета Безопасности Российской Федерации» // Собрание законодательства РФ. 2011. № 19. Ст. 2721.

[2] Указ Президента РФ от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю» // Собрание законодательства РФ. 2004. № 34. Ст. 3541.

предотвращения ее утечки по техническим каналам, несанкционированного доступа к ней, специальных воздействий на информацию (носители информации) в целях ее добывания, уничтожения, искажения и блокирования доступа к ней на территории Российской Федерации.

В составе Федеральной службы безопасности РФ действует специализированное подразделение, занимающееся обеспечением информационной безопасности, Центр информационной безопасности ФСБ России, который входит в состав службы контрразведки ФСБ[1].

Участие в разработке и проведении государственной политики в сфере информационной безопасности осуществляет созданная в 2003 г. Служба специальной связи и информации при Федеральной службе охраны Российской Федерации (Спецсвязь России).

Согласно Указа Президента РФ от 7 августа 2004 г. № 1013 «Вопросы Федеральной службы охраны Российской Федерации»[2] в задачи Спецсвязи России входят: разработка, создание, эксплуатация и развитие федеральных информационных систем для специального информационного обеспечения государственных органов, а также обеспечение надежного функционирования и информационной безопасности этих систем, в том числе в военное время и при чрезвычайных ситуациях; участие в реализации государственной политики в области международной информационной безопасности и проведение мероприятий по информационному противоборству, обнаружению, предупреждению и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации и др.

В структуре Министерства внутренних дел РФ создан Департамент информационных технологий, связи и защиты информации МВД России, среди подразделений которого значительную роль играет Управление защи-

---

[1] Официальный сайт Федеральной службы безопасности РФ; URL: http://clsz.fsb.ru/ (дата обращения 21.03.2018)

[2] Указ Президента РФ от 7 августа 2004 г. № 1013 «Вопросы Федеральной службы охраны Российской Федерации» (с изм. от 27.02.2018) // Собрание законодательства РФ. № 2004. № 32. Ст. 33.14

ты информации[1]. Одной из главных функций этого Управления является организация обеспечения мероприятий по технической защите государственной тайны и информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну.

Блокировка сайтов с запрещённым контентом в России отнесена к ведению Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор). Причем блокировка возможна как в досудебном, так и в судебном порядке. Роскомнадзор, получая жалобу на Интернет-ресурс, содержащий запрещённую информацию, направляет уведомление хостинг-провайдеру, который обязан потребовать от владельца сайта удалить запрещённую информацию в течение трёх дней. Если владелец не выполняет требования, то сайт попадает в реестр запрещённых в соответствии с Постановлением Правительства Российской Федерации от 26 октября 2012 г. № 1101 «О единой автоматизированной информационной системе «Единый реестр доменных имен, указателей страниц сайтов в информационно-телекоммуникационной сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в информационно-телекоммуникационной сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено» [2] и блокируется. Для устранения различных толкований понятия запрещенной информации утверждены критерии оценки материалов, которые относят к таковым [3].

---

[1] Официальный сайт Министерства внутренних дел РФ; URL: https:// i/mvd/structure1/Departamenti/Departament_informacionnih_tehnologij_sv (дата обр.21.03.2018)

[2] Постановление Правительства Российской Федерации от 26 октября 2012 г. № 1101 «О единой автоматизированной информационной системе «Единый реестр доменных имен, указателей страниц сайтов в информационно-телекоммуникационной сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в информационно-телекоммуникационной сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено» // Собрание законодательства Российской Федерации. 2012 г. № 44. Ст. 6044.

[3] Приказ от 18 мая 2017 года №84/292/351/ММВ-7-2/461С «Об утверждении критериев оценки материалов и (или) информации, необходимых для принятия решений Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций, Министерством внутренних дел Российской Федерации, Федеральной службой по надзору в сфере защиты прав потребителей и благополучия человека, Федеральной налоговой службой о включении доменных имен и (или) указателей страниц сайтов в информационно-телекоммуникационной сети «Интернет» // Официальный интернет-портал правовой информации (www.pravo.gov.ru) 29.06.17 г. (дата обращения 22.03.2018)

В 2016 г. по данным Роскомнадзора, гораздо больше сайтов были заблокированы в судебном порядке. В суд, как правило, обращаются представители прокуратуры с требованием о блокировке сайта[1].

Подводя итог, следует отметить, что на сегодняшний момент сложилась достаточно разветвленная сеть органов и структур международного, регионального уровня и национального уровня, в рамках которых государства взаимодействуют друг с другом по вопрос безопасности пользования информационно-коммуникационных технологий.

Более тесное сотрудничество Россия осуществляет в рамках региональных и двусторонних договорённостей между специализированными органами, занимающимися предотвращением, пресечением и ликвидацией последствий реализации угроз информационной безопасности.

[1] Официальный сайт Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций [Электронный ресурс] // http://eais.rkn.gov.ru/feedback/ (дата обращения 25.03.2018).

ЗАКЛЮЧЕНИЕ

На сегодняшний день мировое сообщество не может прийти консенсусу относительно терминологии и содержания понятия «информационная безопасность». Западные страны (члены Международного союза электросвязи) и США используют термин «cybersecurity». Россия и государства - члены региональных организаций СНГ и ШОС используют дефиницию «информационная безопасность». Разницу в формулировках сопровождает и разное наполнение содержательной сущности данных терминов. Так, Российская Федерация придерживается широкого подхода к определению структуры информационной безопасности и включает в нее как информационно-техническую сферу, так и информационно-психологическую (психофизическую) составляющую. Западные страны и США придерживаются более узкого подхода, ограничиваясь только технической сферой.

Для эффективного и плодотворного международного сотрудничества государств по созданию системы информационной безопасности необходимо прийти не только к консенсусу при использовании идентичных дефиниций и сущностных характеристик понятий, но необходимо также своевременно проводить анализ угроз, которые могут возникнуть при применении современных информационно-коммуникационных технологий. При этом следует обратить внимание, что угрозы в области обеспечения информационной безопасности обладают специфическими особенностями, отличающими их от всех существующих видов международных угроз. Так, среди особенностей выделяют то, что ресурсы, необходимые для создания информационной угрозы, не могут контролироваться государством, т.к. для создания возможностей использования информационных ресурсов в качестве угрозы достаточно применения технологий, имеющихся в свободной продаже. Значительная степень анонимности информационного пространства также существенно осложняет международное расследование информационных правонарушений. Постоянно эволюционирующий характер угроз затрудняет их прогнозирование, что связано как с быстрым развитием информационных техно-

логий, так и с разнообразием сфер жизнедеятельности, для которых эти угрозы опасны. Это приводит к проблеме отставания нормативно-правового регулирования механизмов контроля информационных угроз.

Сегодня ключевые игроки международной политики придерживаются совершенно противоположных подходов к обеспечению информационной безопасности. Так, США и страны Европейского Союза к главным угрозам кибербезопасности относят кибертерроризм и киберпреступность, а проблемы межгосударственного противоборства, по их мнению, должны регулироваться международным гуманитарным правом. Их оппоненты (Россия, Китай, Бразилия и др.) придерживаются взглядов о необходимости полной демилитаризации информационного пространства, что предполагает заключение международной договоренности об отказе стран от создания средств информационного воздействия и осуществления любых возможных агрессивных действий в информационном пространстве.

Несмотря на значительное количество принятых Генеральной Ассамблеей ООН резолюций и работу Группы правительственных экспертов на сегодняшний момент единой концепции создания глобальной системы информационной безопасности пока не принято. Связано это с тем, что параллельно происходит формирование двух конкурирующих моделей информационной безопасности, которые строятся на разных основополагающих принципах. Разногласия по важным вопросам обеспечения информационной безопасности не позволяет государствам прийти к консенсусу и принять международный документ универсального характера.

В целях выработки многостороннего, взаимоприемлемого международно-правового документа, направленного на укрепление информационной безопасности, в соответствии с которым государства и другие субъекты международного права должны будут нести международную ответственность за деятельность в информационном пространстве, осуществляемую ими или с территорий, находящихся под их юрисдикцией, считаем необходимым обсудить на международном уровне следующие вопросы:

1) нахождение консенсуса между странами в использовании терминологического аппарата в сфере информационной безопасности;

2) выявление факторов, влияющих на состояние международной информационной безопасности с учетом наличия угроз террористического, криминального и военного характера;

3) определение путей и взаимоприемлемых мер предотвращения использования информационных технологий в террористических и других преступных целях, а также мер по ограничению применения информационного оружия в отношении критически важных инфраструктур других государств;

4) закрепление принципа государственного суверенитета над «национальными сегментами» глобальной сети Интернет;

5) рассмотрение возможных путей международного взаимодействия правоохранительных органов по предотвращению и пресечению правонарушений в информационном пространстве, в частности, по выявлению источников информационной агрессии;

6) обсуждение вопросов оказания международной помощи странам, которые стали жертвами информационных атак, в целях смягчения последствий нарушения нормальной деятельности, прежде всего, объектов критических инфраструктур государств.

Плодотворный диалог России в рамках СНГ, ШОС, БРИКС, ОДКБ наглядно свидетельствует о возможности эффективного выстраивания межгосударственного общения на основе принципов равноправия, учета интересов друг друга и уважения права государств на выбор собственной модели информационной безопасности.

Главной целью мирового сообщества в данной сфере должно стать создание всеобъемлющей международной системы информационной безопасности, включающей в себя совокупность международных, региональных и национальных институтов, призванных обеспечить эффективное противодействие угрозам информационной безопасности.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ И ЛИТЕРАТУРЫ

Международные правовые акты

1. Международный пакт о гражданских и политических правах (Нью-Йорк, 19 декабря 1966 г.) // Сборник действующих договоров, соглашений и конвенций, заключенных с иностранными государствами. – М., 1978 г. Вып. XXXII. С. 44.

2. Конвенция о преступности в сфере компьютерной информации (ETS № 185) (Заключена в г. Будапеште 23.11.200 г.) (с изм. от 28.01.2003) // Конвенция на английском языке опубликована не была; http://www.consultant.ru/ (дата обращения 25.02.2018).

3. Резолюция ГА ООН (A/RES/53/70) от 4 декабря 1998 г. «Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности»// Официальный сайт ООН; URL: http://www.un.org/ru (дата обращения 28.02.2018).

4. Резолюция ГА ООН (A/RES/54/49) от 1 декабря 1999 г. // Официальный сайт ООН; URL: http://www.un.org/ru/development/ict/res.shtml (дата обращения 28.02.2018).

5. Резолюция ГА ООН A/RES/65/41 от 8 декабря 2010 г. «Достижения в сфере информатизации и коммуникаций в контексте международной безопасности»// URL: http://www.scrf.gov.ru/news/720.html$http(дата обращения: 02.03.2018).

6. Рекомендация CM/Rec (2011)8 Комитета министров государствам-членам о защите и продвижении универсального характера, целостности и открытости Интернета (Принята Комитетом министров 21.09.2011г.) // Councul of Europe http:// hr-online.org.ua/npanel/webdata/299/12_rekomendatsiya-(2011)8.pdf (дата обращения 01.03.2018).

7. Модельный закон СНГ «О международном информационном обмене» (Принят постановлением Межпарламентской Ассамблеи государств-участников СНГ от 26 марта 2002 г. № 19-7) // Информационный бюллетень

Межпарламентской Ассамблеи государств-участников СНГ. 2002. № 29. URL: http://base.garant.ru/2569410/

8. Модельный закон СНГ «Об информации, информатизации и обеспечении информационной безопасности (Постановление МПА СНГ от 28.11.2014 г. № 41-15) [Электронный ресурс]// URL: http://www.parliament.am/library/modelayin (дата обращения 06.03.2018).

9. Соглашение между правительствами государств - членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности (Екатеринбург, 16 июня 2009 г.) [Электронный ресурс]: http://www.conventions.ru/view_base.php?id=1979

10. Соглашение между Правительством Российской Федерации и Правительством Федеративной Республики Бразилии о сотрудничестве в области обеспечения международной информационной и коммуникационной безопасности (Москва, 14 мая 2010 г.) // Текст Соглашения официально опубликован не был; URL: http://base.garant.ru/7022664 (дата обращения 06.03.2018).

11. Соглашение между Правительством Российской Федерации и Правительством Республики Индии о сотрудничестве в области обеспечения безопасности в сфере использования информационно-коммуникационных технологий (15 октября 2016 г.) // Официальный портал Министерства иностранных дел РФ. URL: http://www.mid.ru/foreign_policy/international_contracts/2_contract/-/storage-viewer/bilateral/page-9/51667 (дата обращения 06.03.2018).

Нормативно-правовые акты Российской Федерации

1. Конституция Российской Федерации. Принята всенародным голосованием 12 декабря 1993 г. (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008, 30.12.2008, 05.02.2014 , 21.07.2014) //Российская газета. 2014, 23 июля.

2. Федеральный закон от 27 июля 2006 г. № 149-ФЗ (ред. 25.11.2017 № 327-ФЗ) «Об информации, информационных технологиях и о защите ин-

формации» // Собрание законодательства Российской Федерации. 2006. № 31 (часть I) Ст. 3448; 2017. № 48. Ст. 7051.

3. Федеральный закон от 28 декабря 2010 г. № 390-ФЗ (с изм. и доп. от 05.10.2015 № 285-ФЗ) «О безопасности» // Собрание законодательства РФ. 2011. № 1. Ст. 2; 2015. № 41. Ст. 5639.

4. Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» // Официальный интернет-портал правовой информации (www.pravo.gov.ru) 27 июля 2017 г. (дата обращения 21.02.2018).

5. Указ Президента РФ от 7 августа 2004 г. № 1013 «Вопросы Федеральной службы охраны Российской Федерации» (с изм. от 27.02.2018) // Собрание законодательства РФ. № 2004. № 32. Ст. 33.14

6. Указ Президента РФ от 6 мая 2011 г. № 590 «Вопросы Совета Безопасности Российской Федерации» // Собрание законодательства РФ. 2011. № 19. Ст. 2721.

7. Указ Президента РФ от 31 декабря 2015 г. № 683 «О Стратегии национальной безопасности Российской Федерации» // Собрание законодательства Российской Федерации. 2016. № 1 (часть II). Ст. 212; Официальный интернет-портал правовой информации (www.pravo.gov.ru) 31 декабря 2015 г. (дата обращения 18.02.2018).

8. Указ Президента РФ от 30 ноября 2016 г. № 640 «Об утверждении Концепции внешней политики Российской Федерации» // Официальный интернет-портал правовой информации (www.pravo.gov.ru) 01 декабря 2016 г. (дата обращения 18.02.2018).

9. Указ Президента РФ от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // Собрание законодательства Российской Федерации. 2016. № 50. Ст. 7074.

10. Указ Президента РФ от 09 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы» //

Официальный интернет-портал правовой информации (www.pravo.gov.ru) 10 мая 2018 г. (дата обращения 18.02.2018).

11. Распоряжение Правительства РФ от 16 июля 2009 г. № 984-р «Об утверждении Соглашения между правительствами государств - членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности» (вступило в силу с 05.01. 2012) [Электронный ресурс] // Текст Распоряжения официально опубликован не был; URL: http://www.garant.ru (дата обращения 25.02.2018).

12. Распоряжение Правительства РФ от 28 мая 2012 г. № 856-р «О подписании Соглашения о сотрудничестве государств-участников Содружества Независимых Государств в области обеспечения информационной безопасности» // Собрание законодательства РФ. 2012. № 23. Ст. 3058.

13. Распоряжение Правительства РФ от 15 ноября 2013 г. № 2120-р «О подписании Соглашения о сотрудничестве государств - участников Содружества Независимых Государств в области обеспечения информационной безопасности» // Собрание законодательства РФ. 2013. № 47. Ст. 6135.

14. Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года (утв. Президентом РФ 24 июля 2013 № Пр-1753 // Официальный сайт Совета Безопасности РФ; URL: http://www.scrf.gov.ru. (дата обращения 18.02.2018).

Научная литература

1. Агапов П.В., Ефремова М.А. Международно-правовые основы обеспечения информационной безопасности участников Содружества независимых государств // Юридическая наука и правоохранительная практика. 2015. № 1 (31). С. 176-182.

2. Арламов Е.А., Панасюк Г.О. Анализ состояния информационной безопасности в современной России // Экономика и менеджмент инновационных технологий. 2016. № 12 [Электронный ресурс]. URL: http://ekonomika.snauka.ru/2016/12/13291 (дата обращения 21.03.2018).

3. Баринов С.В. О правовом определении понятия «информационная безопасность личности» // Актуальные проблемы российского права. 2016. № 4. С. 97-105

4. Баришполец В.А. Информационно-психологическая безопасность: основные положения // Радиоэлектроника. Наносистемы. Информационные технологии. 2012. № 5. С. 62-104.

5. Бачило И.Л., Бондуровский В.В. О совершенствовании и гармонизации национального законодательства государств - участников СНГ в сфере обеспечения информационной безопасности / И.Л. Бачило, В.В. Бондуровский, М.А. Вус, М.М. Кучерявый, О.С. Макаров // Информационное право. 2013. № 1 (32). С. 24-27.

6. Бейсли-Уокер Б., Боммелер К., Международная информационная безопасность и глобальное управление Интернетом: взгляд из Женевы глазами российских и международных экспертов / Б. Бейсли-Уокер, К. Боммелер, В.Л. Васильев, Р. Вебер, В.В. Львович, В.А. Орлов и др. // Индекс безопасности. 2013. Т.19. № 1 (104). С. 185-205.

7. Брылева Е.А. Право на использование Интернета как одно из «неотъемлемых» прав человека? // Информационное право. 2017. № 2. С. 23-26.

8. Валиахметова Г.Н. Проблемы информационной безопасности в Азии // Известия Уральского федерального университета. 2015. № 1 (137). С. 128-136.

9. Вус М.А., Макаров О.С. К вопросу о разработке рекомендаций по совершенствованию и гармонизации национального законодательства государств - участников СНГ в сфере обеспечения информационной безопасности // Информатизация и связь. 2012. № 1. С. 5-8.

10. Вус М.А. Макаров О.С. Стратегический вектор обеспечения международной информационной безопасности на пространстве СНГ [Электронный ресурс]// Юридические науки: проблемы и перспективы. – Казань, Бук. 2016. С. 40-43. URL: https://moluch.ru/conf/law/archive/223/11056/;

11. Грибков Д.Г. О формировании системы международной информационной безопасности // Международная жизнь. 2015. № 8. С. 86-92.

12. Даниленков А.В. Государственный суверенитет Российской Федерации в информационно-телекоммуникационной сети Интернет // Lex russica. 2017. № 7(128). С. 154-165.

13. Для совершенствования системы информационной безопасности в ОДКБ / М.А. Вус, М.М. Кучерявый, О.С. Макаров, Г.И. Перекопский // Власть. 2014. № 8. С.37-40.

14. Есиева Д.Г., Саханский Ю. В. Анализ угроз информационной безопасности в современном цифровом пространстве [Электронный ресурс]// Научные исследования и перспективные проекты 2017; http://old.fa.ru/fil/chair-matinf-vladik/Pages/nirs.aspx(дата обращения 24.02.2018)

15. Еркин А.В. Понятия «информация» и «информационная безопасность»: от индустриального общества к информационному // Информационное общество. 2012. № 1. С. 68-74.

16. Жилкин В.А. Международная безопасность и роль России в борьбе с международным терроризмом и информационной безопасностью // Международное публичное и частное право. 2017. № 4. С. 24-27.

17. Жилкина Ю.В. Международная безопасность в эпоху глобализации мировой экономики // Национальные интересы: приоритеты и безопасность. 2010. № 25. С. 62-68.

18. Закупень Т.В. Понятие и сущность информационной безопасности и ее место в системе обеспечения национальной безопасности Российской Федерации // Информационные ресурсы России. 2009. № 4. С. 28-34.

19. Зиновьева Е.С. Анализ внешнеполитических инициатив России в области международной информационной безопасности // Интернет-Политика. 2014. № 6 (39). С. 47-52.

20. Зиновьева Е.С. Международная информационная безопасность: монография / Моск. гос. ин-т междунар. отношений МИД России. – М.: МГИМО-Университет, 2014. 194 с.

21. Зиновьева Е.С. Международное сотрудничество по обеспечению информационной безопасности //Право и управление XXI. 2014. № 4. С. 44- 52.

22. Ильичев И.Е. Проблемы обеспечения информационной безопасности личности, общества и государства в современной России // Проблемы правоохранительной деятельности. Наука. Теория. Практика. 2015. № 2. С. 13-21.

23. Казаковцев А.В. НАТО и кибербезопасность // Вестник Волгоградского государственного университета. Серия 4: История. Регионоведение. Международные отношения. 2012. № 2. С. 109-114.

24. Казарин О.В., Шаряпов Р.А. Вредоносные программы нового поколения – одна из существенных угроз международной информационной безопасности // Вестник РГГУ. Информатика, защита информации, информационная безопасность. 2015. № 12 (155). С 9-23.

25. Казарин О.В., Скиба В.Ю., Шаряпов Р.А. Новые разновидности угроз международной информационной безопасности // Вестник РГГУ. Информатика, защита информации и информационная безопасность. 2016. № 1 (3). С. 54-72.

26. Капустин А.Я. Угрозы международной информационной безопасности: формирование концептуальных подходов // Журнал российского права. 2015. № 8. С. 89-100.

27. Касенова М.Б. Трансграничное управление Интернетом: основные термины и понятия [Электронный ресурс] // Юридический мир. 2014. № 2. (206). С. 58-63; URL: http://geum.ru/lav/index-42965.php (дата обращения 22.02.2018).

28. Касенова М.Б. Международное сотрудничество и управление использованием Интернета // Международное право и международные организации. 2014. № 1. С. 6-15.

29. Кванталиани И.Э., Жданов Н.Б. Информационная безопасность – важнейший аспект интегральной безопасности // Журнал научных публикаций аспирантов и докторантов. 2011. № 10 (64). С. 41-43.

30. Кванталиани И.Э. Необходимость разработки и принятия универсальной международной конвенции в сфере обеспечения информационной без-

опасности // Вестник Российского университета дружбы народов. 2012. № 2. С. 241-244.

31. Кибербезопасность и управление интернетом: Документы и материалы для российских регуляторов и экспертов /Отв. ред. М.Б. Касенова; сост. О.В. Демидов и М.Б. Касенова. М.: Статут, 2013. 465 с.

32. Лопатин Ю.Н. Информационная безопасность в России: проблемы, поиски решений // Гуманитарные исследования в Восточной Сибири и на Дальнем Востоке. 2008. № 2. С. 51-57.

33. Мазуров В.А., Невинский В.В. Понятие и принципы информационной безопасности // Известия Алтайского государственного университета. 2003. № 2. С. 57-63.

34. Меркурьева Е.А. Международное сотрудничество России в области обеспечения информационной безопасности [Электронный ресурс] // Центр стратегических оценок и прогнозов:. URL: http://csef.ru/ru/nauka-i-obshchestvo/445/mezhdunarodnoe-sotrudnichestvo-rossii-v-oblasti-obespecheniya-informaczionnoj-bezopasnosti (дата обращения 04.03.2018).

35. Международное право: учебник /Отв. ред. д.ю.н. С.А. Егоров. – М.: Статут, 2018. 848 с.

36. Молчанов Д.А. Дифференциация содержания понятия «информационная безопасность» в национальном законодательстве Российской Федерации и Соединенных Штатов Америки как сдерживающий фактор прогрессивного развития международно-правового регулирования [Электронный ресурс]// Право: современные тенденции: материалы IV Междунар. науч. конф. (г. Краснодар, февраль 2017). Краснодар: Новация, 2017. С. 122-125; URL https://moluch.ru/conf/law/archive/225/11706/ (дата обращения: 22.02.2018).

37. Молчанов Н.А., Матевосова Е.К. Доктрина информационной безопасности Российской Федерации (новелла законодательства) // Актуальные проблемы российского права. 2017. № 2. (75). С. 159-165.

38. Охрименко С.А., Черней Г.А. Угрозы безопасности автоматизированным информационным системам (программные злоупотребления) // Научно-

техническая информация. Серия 1: Организация и методика информационной работы. 1996. № 5.

39. Панова В.В. Проблемы безопасности и перспективы саммита БРИКС в Уфе // Вестник международных организаций: образование, наука, новая экономика. 2015. Т. 10. № 2. С 119-139.

40. Перчаткина С.А., Цирин А.М., Цирина М.А., Цомартова Ф.В. Социальные Интернет-сети: правовые аспекты // Журнал российского права. 2012. № 5. С. 14-24.

41. Петренко А.А., Петренко С.А. Киберучения: методические рекомендации // Вопросы кибербезопасности. 2015. № 3(11). С. 2-14.

42. Проблемы информационной безопасности в международных военно-политических отношениях / Под. ред. А.В. Загорского, Н.П. Ромашкиной. М.: ИМЭМО РАН, 2016. 183 с.

43. Сарычев Н.В., Мельниченко Д.В. Внешние и внутренние угрозы информационной безопасности России // Российский психологический журнал. 2010. № 5. С. 108-114.

44. Смирнов В.П. Правовое регулирование сети Интернет на международном и национальном уровнях в Республике Беларусь и зарубежных странах // XI Машеровские чтения: материалы международной научно-практической конференции студентов, аспирантов и молодых ученых. Витебск, 2017. С. 421-423.

45. Соколов М.С. Информационная безопасность. К вопросу о содержании понятия «информационная безопасность» // Закон и право. 2011. № 5. С. 9-14

46. Стратегический вектор обеспечения международной информационной безопасности Сборник / [сост. М.А. Вус, О.С. Макаров] / Предисловие: чл.-кор. РАН Р.М. Юсупов. СПб.: СПИИРАН, 2016. 122 с.

47. Ступаков В.И. Инициативы евразийских государств по обеспечению международной и региональной информационной безопасности // Международное сотрудничество Евразийских государств: политика, экономика, право. 2015. № 3. С. 72-83.

48. Талапина Э.В. О возможностях правового регулирования Интернета // Труды Института государства и права Российской академии наук. 2016. № 3(55). С. 57-75.

49. Урсул АД. Информационная стратегия и безопасность в концепции устойчивого развития // Научно-техническая информация. Серия 1: Организация и методика информационной работы. 1996. № 1. С. 6-10.

50. Чеботарева А.А. Правовое обеспечение информационной безопасности личности в глобальном информационном пространстве // Юридический мир. 2016. № 8. С. 63.-66.

Электронные ресурсы

1. Выступление Президента РФ В.В. Путина на заседании Совета Безопасности 26 октября 2017 г., Москва, Кремль [Электронный ресурс] // Официальный сайт Президента России. URL: http://www.kremlin.ru/events/president/news/55924 (дата обращения 28.02.2018)

2. Глобальная программа кибербезопасности МСЭ. Основа для международного сотрудничества в области кибербезопасности [Электронный ресурс] // URL: http://www.ifap.ru/pr/2008/080908aa.pdf (дата обращения 02.03.2018)

3. Декларация третьей встречи министров связи стран БРИКС от 27 июля 2017 года [Электронный ресурс] // Официальный сайт Министерства связи и массовых коммуникаций Российской Федерации. URL: http://minsvyaz.ru/ru/events/37255/ (дата обращения 06.03.2018)

4. Шариков П.А. Политика США в области информационной безопасности [Электронный ресурс]: автореф. дисс.… канд. полит. наук. М, 2009. 25 с. URL: http://cheloveknauka.com/politika-ssha-v-oblasti-informatsionnoy-bezopasnosti (дата доступа 28.02.2018)

5. International Strategy For Cyberspace, Washington DC. Prosperity, Security, and Openness in a Networked World // The White House : offic. website. 2011. May. 25 p. URL: http://www.whitehouse.gov/sites/default/files/rss_viewer/international_ strategy_for_cyberspace.pdf (дата обращения 28.02.2018).