СБОРНИК ДОКЛАДОВ УЧАСТНИКОВ
XVII МЕЖДУНАРОДНОГО ФОРУМА

ПАРТНЕРСТВО ГОСУДАРСТВА, БИЗНЕСА И ГРАЖДАНСКОГО ОБЩЕСТВА ПРИ ОБЕСПЕЧЕНИИ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

НАЦИОНАЛЬНАЯ АССОЦИАЦИЯ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ • NAIIS • NATIONAL ASSOCIATION OF THE INTERNATIONAL INFORMATION SECURITY
НАМИБ

18–20 СЕНТЯБРЯ 2023 г.,
МОСКВА, РОССИЯ

СБОРНИК ДОКЛАДОВ УЧАСТНИКОВ
XVII МЕЖДУНАРОДНОГО ФОРУМА

«ПАРТНЕРСТВО ГОСУДАРСТВА, БИЗНЕСА И ГРАЖДАНСКОГО ОБЩЕСТВА ПРИ ОБЕСПЕЧЕНИИ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

18–20 СЕНТЯБРЯ 2023 г.
МОСКВА, РОССИЯ

УДК 334.021(082)
ББК 65.291я43
П18

АННОТАЦИЯ

В сборнике представлены доклады и другие материалы участников XVII Международного Форума «Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности» (18–20 сентября 2023 г., г. Москва).

Форум организован Национальной Ассоциацией международной информационной безопасности (НАМИБ) и традиционно посвящен обсуждению наиболее актуальных проблем обеспечения безопасности использования глобальной ИКТ-среды и формирования системы противодействия использованию ИКТ для нарушения международного мира и безопасности. Одной из особенностей Форума было обсуждение проблем обеспечения информационной безопасности в условиях формирования многополярного мира.

В работе Форума приняли участие более 250 представителей экспертного сообщества из 20 стран, а также представители Организации Объединенных Наций, Международного союза электросвязи, Совещания по взаимодействию и мерам доверия в Азии (СВДМА), Интерпола. Особую значимость мероприятиям Форума придало представительное участие государств Африки (Алжир, Бенин, Бурунди, Гана, Египет, Мозамбик, Танзания, Эфиопия, ЮАР) и Азии (Бахрейн, Иордания, Камбоджа, КНР, Малайзия, Таиланд), а также традиционное участие экспертов Союзного государства (Россия—Белоруссия), СНГ (Азербайджан, Узбекистан), США и Франции. Это свидетельствует об активизации процессов взаимодействия экспертов как существующих международных объединений, так и новых образований, базирующихся на равноправном сотрудничестве и уважении суверенитета национальных государств.

Дискуссии на пленарном заседании и шести круглых столах были посвящены обсуждению следующих актуальных вопросов:

- защита интересов отечественного ИТ-бизнеса в современных условиях;
- установление международно-правового режима обеспечения безопасности использования ИКТ и устойчивости функционирования ИКТ-среды;
- сохранение традиционных духовно-нравственных ценностей национального общества в глобальном информационном пространстве;
- сотрудничество в области противодействия компьютерной преступности в глобальной ИКТ-среде;
- обеспечение информационной безопасности детей, подростков и молодежи в условиях цифровых трансформаций: приоритеты, принципы и механизмы обеспечения;
- развитие регионального сотрудничества в системе международной информационной безопасности.

Представленные материалы отражают позиции экспертов по приоритетным направлениям сотрудничества в следующих целях:

- расширение географии и направлений сотрудничества с дружественными странами в сфере обеспечения суверенитета национального информационного пространства, повышение в нем роли государственно-частного партнерства и ИКТ-бизнеса;
- прогрессивное развитие норм и принципов международного права, регулирующих поведение государств в области использования ИКТ-среды, и создание правовой основы системы международной информационной безопасности;
- развитие норм и принципов международного права в области противодействия использованию ИКТ в преступных целях с учетом продвигаемых Российской Федерацией инициатив;
- защита традиционных духовно-нравственных ценностей национальных обществ в глобальной ИКТ-среде;
- совершенствование политики и механизмов обеспечения информационной безопасности и когнитивного развития подрастающего поколения;
- развитие взаимодействия экспертов в области международной информационной безопасности в рамках Шанхайской организации сотрудничества, БРИКС, а также с государствами Африки и Азии.

Перевод докладов зарубежных участников для публикации осуществлен экспертом НАМИБ, кандидатом политических наук П.А. Карасевым.

Оргкомитет XVII Международного Форума «Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности

ISBN ISBN 978-5-6044055-5-0

СОДЕРЖАНИЕ

ПЛЕНАРНОЕ ЗАСЕДАНИЕ

КРУГЛЫЙ СТОЛ № 1
ГОСУДАРСТВЕННО-ЧАСТНОЕ ПАРТНЕРСТВО ПРИ РЕАЛИЗАЦИИ ГОСУДАРСТВЕННОЙ ПОЛИТИКИ В ОБЛАСТИ МИБ КАК МЕХАНИЗМ ОБЕСПЕЧЕНИЯ СУВЕРЕННЫХ ИНТЕРЕСОВ ОТЕЧЕСТВЕННОГО БИЗНЕСА В СОВРЕМЕННЫХ УСЛОВИЯХ

КРУГЛЫЙ СТОЛ № 2
ПЕРСПЕКТИВЫ ФОРМИРОВАНИЯ МЕЖДУНАРОДНО-ПРАВОВОГО РЕЖИМА РЕГУЛИРОВАНИЯ СФЕРЫ ИСПОЛЬЗОВАНИЯ ИКТ

ПЛЕНАРНОЕ ЗАСЕДАНИЕ

Ведущий:
Мирошников Б.Н., президент Национальной Ассоциации
международной информационной безопасности, вице-президент ГК «Гарда»

Б.Н. Мирошников

Президент Национальной Ассоциации международной информационной безопасности, вице-президент ГК «Гарда»

Уважаемые участники международного Форума!

Уважаемые гости!

Дамы и господа!

Доброе утро! Это для тех, кто в Москве. Добрый день, добрый вечер и даже доброй ночи — для тех, кто присоединился к нам в онлайн режиме из разных точек планеты.

Позвольте мне открыть заседание очередного XVII международного Форума «Партнёрство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности».

Прежде всего хотелось бы искренне и сердечно поприветствовать всех участников и гостей Форума. Сообщаю вам, что в работе Форума на данную минуту принимают участие более 250 ведущих ученых и специалистов из 20 стран.

Наша задача — обсудить в кругу специалистов и экспертов актуальные проблемы обеспечения международной информационной безопасности и недопущения неправомерного использования ИКТ-среды в новых геополитических условиях — в условиях формирования многополярного мира.

Наш Форум имеет свою историю. В течение 17 лет мы собираем ведущих экспертов России и других стран, чтобы честно и открыто обсуждать ситуацию в мире с информационной безопасностью. И также вместе искать решения трудных вопросов. И 16 лет бессменным Председателем Форума был первый Президент Национальной Ассоциации международной информационной безопасности Владислав Петрович Шерстюк. К сожалению, Владислава Петровиче сегодня нет в этом зале, но он участвует в работе Форума в режиме онлайн. Позвольте выразить Владиславу Петровичу нашу признательность за огромную проделанную работу и поприветствовать его нашими аплодисментами.

Спасибо!

Четвертый год подряд мы встречаемся с вами в городе Москве, в гостеприимном здании Дипломатической академии МИД России. В этой связи хотелось бы поблагодарить руководителей и сотрудников Академии и, прежде всего, ректора — Чрезвычайного и Полномочного посла Российской Федерации Александра Владимировича Яковенко за огромную практическую помощь в подготовке и проведении Форума.

Мы чрезвычайно благодарны аппарату Совета Безопасности Российской Федерации и, в первую очередь, Заместителю Секретаря Совета Безопасности Российской Федерации Олегу Владимировичу Храмову за поддержку и помощь в подготовке этого масштабного мероприятия. Мы признательны также руководителям МИДа России, а также других федеральных органов исполнительной власти России, представители которых принимают участие в нашей работе. И, конечно же, отметить большой вклад редакции журнала «Международная жизнь», в организацию и проведение нашего Форума.

Уважаемые коллеги! Какие процессы мы наблюдаем в мире?

С одной стороны, происходит беспрецедентное обострение геополитических противоречий в мире. С другой стороны, становятся все более четкими контуры нового миропорядка, многополярного мира. Этот второй процесс происходит по инициативе Российской Федерации и других заинтересованных государств.

Так, плодотворно развивается Союзное государство Беларуси и России.

В июле 2023 под председательством Индии успешно прошел 23-й саммит государств-членов Шанхайской организации сотрудничества. Как отметил в своем выступлении президент России Владимир Путин, роль ШОС в поддержании мира и стабильности, постоянно возрастает.

В августе 2023 года успешно прошел XV саммит БРИКС. В рамках саммита четко обозначилась приверженность многих государств мира к развитию отношений на основе «взаимоуважения и взаимопонимания, суверенного равенства, солидарности, демократии, открытости, укрепления сотрудничества и консенсуса». Страны БРИКС обязались «углублять взаимовыгодное сотрудничество в направлениях политики, безопасности, экономики и финансов, культурных и гуманитарных связей», «укреплять стратегическое партнерство в продвижении мира», «более представительного и справедливого международного порядка».

Это создает хорошие условия для расширения сотрудничества в области укрепления международной информационной безопасности и безопасного использования глобальной ИКТ-среды.

Безусловно, универсальной площадкой для обсуждения проблем обеспечения международной информационной безопасности в последние 25 лет является Организация Объединенных Наций. Кстати, в эти дни исполнилось ровно 25 лет как вопросы МИБ были впервые включены в повестку дня ООН по инициативе Российской Федерации.

Как показывает ход дискуссий на Генеральной Ассамблее ООН мировое сообщество все в большей степени начинает понимать важность справедливого и равноправного сотрудничества государств в области обеспечения международной информационной безопасности. Основу такой системы может составить только применение норм и принципов международного права. Это становится все более очевидным. Фактически работа по формированию системы международной информационной безопасности уже ведется.

В мае 2023 года Россия совместно с Республикой Беларусь, Корейской Народно-Демократической Республикой, Республикой Никарагуа и Сирийской Арабской Республикой внесла в качестве официального документа 77-й сессии Генеральной Ассамблеи ООН концепцию Конвенции ООН об обеспечении международной информационной безопасности. Инициаторы призвали другие государства присоединиться к обсуждению концепции Конвенции в интересах построения справедливой и всеобъемлющей системы международной информационной безопасности.

Впрочем, об инициативах России и реакции на них мы еще поговорим подробно на нашем Форуме.

В 2021 году на 76-й сессии Генеральной Ассамблеи ООН было поддержано предложение Российской Федерации «продолжить дальнейшую выработку норм, правил и принципов ответственного поведения государств и путей их имплементации» в Рабочей группе ООН открытого состава по вопросам безопасности в сфере использования информационно-коммуникационных технологий и самих ИКТ на период до 2025 года.

В августе 2022 года наша Ассоциация была аккредитована при этой группе и активно участвует в ее мероприятиях.

В частности, для обсуждения на сессиях Рабочей группы ООН (РГОС) в 2023 году предложены результаты изучения проблем применения норм ответственного поведения государств в ИКТ-среде, выполненного ведущими российскими экспертами под эгидой Ассоциации.

Надеемся, что обсуждение этих результатов, а также предложений других экспертов по данному вопросу будет способствовать успешной работе как нашего Форума, так и Рабочей группы ООН.

Мы рады, что Вам, уважаемые коллеги, удалось найти возможность принять участие в работе нашего Форума, на котором всегда поддерживается атмосфера открытости, уважения мнений всех участников, поиска взаимоприемлемых направлений совместной деятельности в целях поддержания международного мира и безопасности.

Уважаемые участники и гости!

В рамках работы Форума будет проведено одно пленарное заседание и шесть круглых столов.

В **пленарном** заседании принимают участие авторитетные руководители заинтересованных государственных органов Россий-

ской Федерации, представители международных организаций и зарубежных государств. Мы услышим широкую палитру мнений и взглядов наших уважаемых экспертов по различным аспектам международной информационной безопасности и не только.

Далее обсуждение некоторых важнейших тем продолжится в рамках работы круглых столов.

На заседании **Круглого стола № 1** во второй половине сегодняшнего дня, предлагается обсудить проблемы развития государственно-частного партнерства при реализации государственной политики в области МИБ в новых геополитических реалиях. Это наше новое направление в деятельности Ассоциации. Полагаем, оно соответствует требованиям времени. Уверен, что участие коммерческих компаний в мероприятиях по продвижению российских инициатив в области международной информационной безопасности будет чрезвычайно полезно, в том числе и для наших иностранных партнеров.

Модератором Круглого стола будет вице-президент Ассоциации Дмитрий Игоревич Григорьев.

На заседании **Круглого стола № 2**, который состоится завтра, 19 сентября, будут обсуждены проблемы формирования международно-правового режима безопасного использования ИКТ.

Модератором этого Круглого стола будет вице-президент Ассоциации доктор юридических и доктор технических наук, профессор Стрельцов Анатолий Александрович.

На заседании **Круглого стола № 3**, который тоже состоится завтра, 19 сентября, предлагается обсудить проблемы сохранения традиционных духовно-нравственных ценностей в глобальном информационном пространстве.

Модератором Круглого стола будет заместитель генерального директора «РЕН ТВ» Прокопенко Игорь Станиславович.

Актуальность заявленной темы также не вызывает сомнения.

20 сентября состоятся три Круглых стола. Утром на заседании **Круглого стола № 4**, предстоит обсудить вопросы противодействия компьютерной преступности в глобальной ИКТ-среде.

Модератором Круглого стола будет Вураско Александр Алексеевич — эксперт центра аналитики внешних цифровых рисков Solar AURA в «Ростелеком-Солар», в прошлом сотрудник Управления «К» МВД России.

На заседании **Круглого стола № 5** будут обсуждены вопросы обеспечения информационной безопасности детей, подростков и молодежи в условиях цифровых трансформаций, а также определения приоритетов, принципов и механизмов решения этой проблемы.

Модератором Круглого стола будет профессор МГУ им. М.В. Ломоносова, академик

Российской академии образования Солдатова Галина Владимировна.

И, наконец, на заседании **Круглого стола № 6** будут обсуждены вопросы развития регионального сотрудничества в системе международной информационной безопасности.

Модератором Круглого стола будет доктор исторических наук, профессор МГИМО МИД России, помощник Президента НАМИБ Смирнов Анатолий Иванович.

Уважаемые коллеги!

В 2010 году в г. Гармиш-Партенкирхен (Германия) по инициативе МГУ имени М.В. Ломоносова был образован Международный исследовательский консорциум по информационной безопасности. Идея была поддержана Объединенным институтом проблем информатизации Национальной Академии наук Беларуси, Интернет-сообществом Болгарии, Институтом исследований вопросов киберпреступности Германии, Индийским институтом информационных технологий, Китайским обществом дружбы с зарубежными странами, Телекоммуникационной компанией «МФИ Софт» России, Университетом штата Нью-Йорк из США и Университетом Токай из Японии.

В свое время мероприятия Консорциума, проходившие в этих организациях, способствовали подключению к дискуссиям значительного числа национальных экспертов.

Исследование проблем применения норм ответственного поведения государств в ИКТ-среде, выполненное в 2018–2020 годах с участием экспертов России, Эстонии, Финляндии, США и Швейцарии, позволило определить существо политических разногласий государств в этой области. Кстати, отчет о работе представлен на сайте НАМИБ.

Представляется, что сотрудничество экспертов различных государств под эгидой Консорциума в изучении проблем подготовки Конвенции ООН об обеспечении международной информационной безопасности, могло бы способствовать продвижению данной инициативы. Думаю, пришло время обсудить пути возрождения работы Консорциума. Очевидно, что стоящие перед нами задачи в области обеспечения МИБ требуют глубоких научных проработок и мы намерены ими заниматься.

В заключение, позвольте заверить Вас, что мы сделаем все возможное, чтобы участники могли свободно и открыто обсуждать наиболее острые вопросы международного сотрудничества в области обеспечения безопасности использования глобальной ИКТ-среды как в интересах развития национальных государств, так и международного сообщества в целом.

Благодарю за внимание. Успешной вам работы.

О.В. Храмов

Заместитель Секретаря Совета Безопасности Российской Федерации

Уважаемые коллеги!

Национальная Ассоциация международной информационной безопасности в очередной раз собирает ведущих экспертов для обсуждения ключевых проблем противодействия угрозам в информационной сфере.

В центре внимания XVII форума — актуальные задачи развития сотрудничества по формированию безопасного глобального информационного пространства в новых геополитических реалиях.

В рамках тематических круглых столов будут рассмотрены проблемные вопросы государственно-частного партнерства в данной области, перспективы формирования международно-правового режима использования информационных технологий, противодействия компьютерной преступности, сохранения традиционных духовно-нравственных ценностей и другие важные вопросы.

Вы знаете, что современное состояние международных отношений характеризуется глобальным противостоянием стран Запада не только с Россией, но и с другими странами, которые защищают свои национальные интересы.

Это затронуло и информационную сферу. Как следствие, «Интернет» и все информационное пространство вместо безопасной среды для экономического развития суверенных стран стали ареной геополитического противостояния.

Наглядный пример западного механизма нарушения суверенитета других стран — ставка Вашингтона на проведение экстерриториальных расследований киберпреступлений.

Мы видим, как США назойливо стремятся использовать принцип экстерриториальности в борьбе с киберпреступностью для преследования граждан иностранных государств во всех уголках мира в угоду американским интересам. И при этом игнорировать двусторонние договоренности в сфере противодействия уголовной преступности.

Вместе с тем очевидно, что для борьбы с информационными угрозами необходимо выстраивать равноправные партнерские отношения и развивать доверие к международному сотрудничеству.

Показательно, что большинство стран мира разделяют российские подходы, понимают нашу общую ответственность за реализацию принципа мирного сосуществования в информационном пространстве на основе уважения суверенитета, национального законодательства и традиций отдельных государств.

Это в полной мере подтвердили итоги работы XI Международной встречи высоких представителей, курирующих вопросы безопасности, которая прошла в мае 2023 г. в Подмосковье под эгидой Совета Безопасности Российской Федерации.

На форум прибыло 112 делегаций из 101 страны и ряда международных организаций.

В рамках встречи был проведен круглый стол по теме «Формирование системы международной информационной безопасности как основы предотвращения межгосударственных конфликтов в киберпространстве».

Данное мероприятие продемонстрировало заинтересованность международного сообщества в выстраивании практически значимых механизмов, прежде всего направленных на защиту критической информационной инфраструктуры от компьютерных атак.

На профильных площадках ООН сформированы добровольные правила поведения государств в глобальном информационном пространстве, но как показала многолетняя практика, их необязательный характер не позволяет обеспечить эффективное регулирование сферы использования информационно-коммуникационных технологий.

США при поддержке своих союзников активно продвигают идею регулирования киберпространства так называемыми «правилами ответственного поведения государств».

Расчет строится на том, что навязывание этих правил дает возможность Вашингтону и его союзникам диктовать условия другим государствам и избирательно определять, для кого правила являются обязательными, а для кого они носят рекомендательный, ни к чему не обязывающий характер. Мы же предлагаем переводить их в юридические обязательства.

Именно универсальный юридически обязывающий договор позволит создать систему международно-правового регулирования глобального информационного пространства на условиях равноправного стратегического партнерства.

Россия в соавторстве с Белоруссией, Венесуэлой, КНДР, Никарагуа и Сирией внесла в качестве официального документа 77-й сессии Генеральной Ассамблеи ООН концепцию Конвенции об обеспечении международной информационной безопасности (опубликована Секретариатом ООН 19 июня 2023 г.). Завершается подготовка проекта самой Конвенции об обеспечении международной информационной безопасности. Мы планируем обсудить этот проект с нашими ближайшими союзниками и партнерами.

Считаем необходимым совместно добиваться формирования международно-правового режима для цифровой среды, основанного на принципах суверенного равенства государств и невмешательства во внутренние дела. Результативность этой работы будет иметь решающее значение для повышения уровня защищенности национальных информационных ресурсов.

Убежден, что сегодняшний форум выполнит свою главную задачу — достижение взаимопонимания по ключевым проблемным вопросам формирования системы обеспечения международной информационной безопасности.

Желаю всем успешной и плодотворной работы!

Б. Гафур

Председатель Рабочей группы ООН открытого состава по вопросам безопасности в сфере использования ИКТ и самих ИКТ

Ваши Превосходительства, уважаемые делегаты. Доброе утро из Нью-Йорка. Для меня большая честь выступать сегодня перед вами в качестве председателя Рабочей группы Организации Объединенных Наций открытого состава по вопросам безопасности в сфере использования ИКТ и самих ИКТ на 2021–2025 годы, которая также известна как РГОС.

Хочу начать с большой благодарности Министерству иностранных дел Российской Федерации за предоставленную мне возможность принять участие в этой важной встрече. Я надеюсь, что смогу внести свой вклад в ваши сегодняшние дискуссии, предоставив обновленную информацию о последних событиях в РГОС, а также рассказать вам о текущих дискуссиях в ООН.

Согласно мандату, изложенному в принятой в декабре 2020 г. резолюции 75/240 Генеральной Ассамблеи, целью РГОС является решение вопросов, касающихся безопасности ИКТ в контексте международного мира и безопасности. При реализации своего мандата РГОС опирается на более чем 20-летнюю работу ООН в этой области. Фактически, в этом году мы отмечаем 25-летие инициативы Российской Федерации начать переговоры по безопасности ИКТ под эгидой ООН. Успех обсуждения этой темы за последние 25 лет действительно является свидетельством дальновидности и видения, а также лидерства Российской Федерации. Поэтому все мы должны поблагодарить Россию за инициативу и постоянное лидерство в этом очень важном вопросе для ООН.

Уважаемые делегаты, РГОС является единственным инклюзивным, универсальным и прозрачным форумом для обсуждения вопросов безопасности ИКТ, который открыт для всех государств-членов ООН. И именно благодаря этим аспектам РГОС достаточно хорошо зарекомендовала себя как механизм ООН. В этом отношении такой процесс, как РГОС, имеет огромную ценность, поскольку он позволяет всем государствам — большим и малым, развитым и развивающимся — быть услышанными и работать вместе для достижения общего понимания на глобальном уровне.

В июле, на фоне очень сложной геополитической обстановки, РГОС удалось консенсусом принять ежегодный доклад о ходе работы. Фактически, это был второй подобный доклад. Принятие в таких сложных обстоятельствах очень предметного документа демонстрирует, что, несмотря на политические разногласия, возможно достичь консенсуса и прогресса по теме безопасности ИКТ, пока государства сохраняют приверженность совместной работе в духе взаимного уважения и взаимного доверия.

Я хочу дать вам представление о некоторых результатах работы РГОС, достигнутых в прошлом году. Приведу семь существенных достижений по различным направлениям мандата Рабочей группы открытого состава.

Первое. Государства определили ряд существующих и потенциальных угроз, включая возникающие угрозы, что было впервые признано в консенсусном докладе ООН. Ландшафт угроз продолжает развиваться, и поэтому важно продолжать целенаправленное обсуждение этого аспекта мандата безопасности в сфере ИКТ.

Во-вторых, государства договорились созвать специальную межсессионную встречу для дальнейшего обсуждения норм, правил

и принципов ответственного поведения государств, включая перспективу внесения изменений или разработки дополнительных правил поведения государств.

В-третьих, государства, с учетом прошлогодних дискуссий, также выработали новое согласованное понимание того, как международное право применимо в отношении использования ИКТ. Кроме того, была признана возможность разработки в будущем дополнительных юридических обязательств, а также отмечено предложение, представленное Российской Федерацией и группой государств, по обновленной концепции конвенции[1].

Четвертый результат касается наращивания потенциала. Государства обратились к председателю РГОС с просьбой созвать глобальный круглый стол по наращиванию потенциала в области безопасности ИКТ. Государства также согласились, что председатель будет взаимодействовать со всеми соответствующими структурами ООН и международными организациями и призывать их согласовать свои программы по наращиванию потенциала с целью поддержки усилий государств по внедрению механизма ответственного поведения государств в области безопасности ИКТ. Это очень важный результат, потому что наращивание потенциала также во многом является мерой укрепления доверия, и это также было признано всеми государствами.

Пятый результат касается регулярного институционального диалога. Государства впервые достигли принципиальной договоренности о наборе общих элементов, которые станут основой будущего механизма регулярного институционального диалога. Общие элементы закладывают очень хорошую основу для дальнейшего обсуждения этого вопроса на следующем заседании Рабочей группы открытого состава.

Шестой субстантивный результат касается мер укрепления доверия или «МД». Очень важно, что государства впервые согласовали первоначальный список добровольных глобальных мер укрепления доверия. И этот список может стать основой, которая позволит государствам удвоить усилия по созданию отношений доверия и взаимного уважения в контексте международного мира и безопасности.

Седьмым существенным результатом и, возможно, наиболее важным результатом последнего на текущий момент заседания РГОС является соглашение, достигнутое государствами по набору элементов для разработки и введения в действие глобального реестра контактных пунктов по обмену информацией о компьютерных атаках. В прошлом году государства договорились создать такой реестр, а в этом году согласовали детали внедрения и введения его в действие, что очень существенно и важно. Эти элементы позволят всем государствам общаться друг с другом в случае инцидентов с безопасностью ИКТ и так контролировать их, чтобы не допустить обострения и угрозы международному миру и безопасности. Теперь, когда элементы для введения в действие глобального реестра согласованы, Секретариат ООН, Управление ООН по разоружению, начнут работу по его созданию и обеспечению полной работоспособности к 2024 г. По завершении этого процесса у международного сообщества будет глобальный реестр с универсальным членством открытый для всех государств. Этот результат воплощает в жизнь идею, которая обсуждалась более 10 лет. Здесь также можно отметить вклад Российской Федерации, потому что она предложила саму идею создания реестра.

Я хочу особо поблагодарить Российскую Федерацию и признать ее вклад в достижение консенсуса по второму ежегодному докладу в ходе встречи в июле. За последний год Россия сыграла очень активную роль, представив различные предложения и концептуальные документы, в том числе документ о глобальном реестре контактных пунктов по обмену информацией. Эти идеи и предложения внесли важный вклад в построение диалога, а также укрепление доверия и взаимного уважения в Рабочей группе открытого состава.

Принимая во внимание существенный прогресс, которого мы достигли во Втором ежегодном докладе, у меня, как председателя РГОС, есть два приоритета на следующий год. Во-первых, продолжать диалог и целенаправленные дискуссии, чтобы найти точ-

1 Конвенция об обеспечении международной информационной безопасности.

ки соприкосновения, области, в которых мы можем шаг за шагом добиться прогресса. И, во-вторых, найти пути реализации многих решений и результатов, согласованных в Рабочей группе открытого состава. Важно, чтобы мы добивались результатов, показывали странам всего мира, что наши усилия конкретны и могут принести отдачу. И поэтому, как председатель Рабочей группы открытого состава, я буду продолжать усердно работать, тесно сотрудничать со всеми вами и со всеми делегациями, чтобы продолжить дискуссии на официальных заседаниях, а также на неофициальных межсессионных встречах для выполнения мандата РГОС.

Подводя итог, я хочу поблагодарить всех вас, уважаемые делегаты из разных стран и групп, которые присутствуют на этой важной конференции, организованной Российской Федерацией. Благодарю вас за интерес к работе РГОС. Я с нетерпением жду встречи с вами в Нью-Йорке и рассчитываю на сотрудничество со всеми делегациями для продвижения наших дискуссий в ООН. Большое спасибо, и желаю вам продуктивной и успешной конференции.

Чен Жимин

Председатель Всекитайской Ассоциации по содействию дружбы

Приветствие председателя Китайского общества дружбы с зарубежными странами Чен Жиминя (КНР)XVII Международному форуму “Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности”.

中国友谊促进会

致第十七届“国家、企业和民间团体：构建伙伴关系 携手保障国际信息安全”国际论坛的贺信

尊敬的俄罗斯国际信息安全联合会主席米洛什尼科夫先生，尊敬的各位嘉宾，

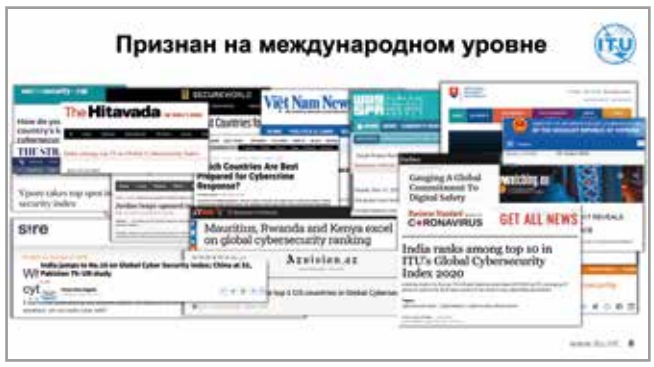
大家好！首先，我谨代表中国友谊促进会，并以我个人名义，对第十七届“国家、企业和民间团体：构建伙伴关系 携手保障国际信息安全”国际论坛成功召开表示衷心的祝贺！

自2007年以来，“国家、企业和民间团体：构建伙伴关系 携手保障国际信息安全”国际论坛关注互联网和信息通信领域面临的威胁与挑战，汇聚政府、国际组织、研究机构和业界企业代表的智慧和力量，致力于凝聚维护网络空间安全的国际共识，为推动国际社会加强网络安全国际合作发挥了重要作用。

2023年7月，中国国家主席习近平在全国网络安全和信息化工作会议上强调要坚持统筹发展和安全，构建大网络安全工作格局，坚持筑牢国家网络安全屏障，发挥信息化驱动引领作用。信息安全作为全球安全治理领域的重要内容，与全球经济、贸易金融、生态生活环境、资源安全等发展领域深度交织、相互渗透、交互影响，深刻影响着人类的安全与

Н.В. Мочу

Региональный директор МСЭ (Международного союза электросвязи) для региона СНГ



GCI 2020 (v4)

Country Name	Overall Score	Regional Rank
Russian Federation	98.06	1
Kazakhstan	93.15	2
Azerbaijan	88.31	3
Uzbekistan	71.11	4
Belarus	50.57	5
Armenia**	50.47	6
Kyrgyzstan	49.64	7
Tajikistan**	17.1	8
Turkmenistan**	14.48	9

* no data

** no response to the questionnaire/data collected by GCI Team

www.itu.int 10

GCI 2020

Российская Федерация

Development Level:
Developed Country

Area(s) of Relative Strength
Legal, Cooperative Measures, Capacity Development
Area(s) of Potential Growth
Organizational Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
98.06	20.00	19.08	18.98	20.00	20.00

www.itu.int 11

GCIv5: текущий статус

Работа экспертной группы и рассылка вопросника

Профильные собрания

Вопросник направлен странам

Сбор данных и определение весовых коэффициентов

Страны представляют заполненные вопросники

Экспертная группа встречается, члены представляют рекомендации по весовым коэффициентам

Проверка и анализ качества данных

Представленные вопросники проходят перекрестную проверку

Странам предлагается комментировать несоответствия

Результаты оцениваются и взвешиваются

Публикация отчета

Текущая фаза

www.itu.int 14

GCIv5: экспертная группа

141 участник Исследовательской комиссии

67 рекомендаций по весовым коэффициентам

Несколько собраний экспертной группы

Предложения по определению уровней от 5 стран

Предложения о формате представления данных

www.itu.int 15

GCIv5: особенности

- ✓ Расширенное описание каждого вопроса
- ✓ Использование платформы опросов Qualtrics по аналогии с процессом сбора статистики МСЭ по ИКТ
- ✓ Среднее время ответа на сообщения <48 часов
- ✓ Введение уровней (tiers) на основе рекомендаций экспертной группы

www.itu.int 16

GCIv5: как наглядно показать результаты без рейтинга?

- ✓Мы планируем рассчитать уровни на основе прошлого отчета, чтобы можно было выделить страны, которые перешли с одного уровня на другой
- ✓В индивидуальном порядке страны по-прежнему будут иметь рейтинг. Об абсолютных изменениях в баллах можно сообщить на уровне страны по запросу
- ✓Средние показатели по регионам поддаются расчету. Страны могут сравнивать себя с другими странами или в целом по региону

www.itu.int 17

GCIv5: сроки

#	Процесс	Начало	Окончание
1	**Официальное приглашение странам и другим Членам МСЭ-D** • Назначение странового координатора • Представители в группу экспертов GCI • Координация с другими организациями	Апрель	Апрель
2	**Обследование и сбор данных** • Публикация вопросника на шести языках • Доступ к онлайн платформе • Ответы на вопросник и подтверждающие документов/ссылки	Апрель	Июль
3	**Дополнение данных** • Дополнительный сбор данных, не предоставленных странами • Уточнение данных с координаторами	Июнь	Август
4	**Проверка и подтверждение** • Закрытие вопросника • Окончательная верификация со странами • Расчет итоговых оценок	Апрель	Октябрь
5	**Публикация отчета**		TBD

www.itu.int 18

Национальная стратегия кибербезопасности (NCS)

https://ncsguide.org/the-guide/

www.itu.int 20

Эффективная стратегия

- ✓ Четко сформулируйте цели национальной кибербезопасности!
- ✓ Установите четкие национальные приоритеты в области кибербезопасности, основанные на связанных с ними рисках.
- ✓ Определить необходимость разработки плана действий.
- ✓ Установите процессы для мониторинга и измерения всего, что связано с приоритетами кибербезопасности.
- ✓ Обеспечьте разработку, внедрение и поддержание эффективных процессов.
- ✓ Обеспечивать развитие и поддержание культуры кибербезопасности – поощрять внедрение контуров обратной связи.
- ✓ Продвигайте общую ответственность – сделайте кибербезопасность делом каждого.

www.itu.int 21

Общие руководящие принципы

Видение	Устойчивость	Политика
Инклюзивность	Права человека	Четкое лидерство
Доверие	Управление рисками	Комплексный подход и приоритеты
Социальное процветание	Экономическое процветание	И другие ...

www.itu.int 22

Примеры – системы управления

- ***Швеция*** *: имеет децентрализованное управление кибербезопасностью – нет единого агентства, ответственного за кибербезопасность, а скорее многие агентства несут ответственность за свои собственные домены*
- ***Австрия*** *: применяется концепция организаций внутреннего и внешнего круга: во внутренний круг входят правительственные учреждения, а во внешний круг входят другие организации, включая частный сектор и CERT*
- ***Франция*** *: ANSSI, Французское агентство сетевой и информационной безопасности (ANSSI) – межминистерское агентство, является национальным органом по защите информационных систем, подчиняющимся канцелярии премьер-министра*
- ***ОАЭ*** *: Регуляторный орган электросвязи возглавляет этот процесс. Стратегия была запущена 24 июня 2019 года*
- ***Кот-д'Ивуар:*** *Министерство ИКТ берет на себя ведущую роль в координации действий на национальном уровне*

Киберщит Казахстана

http://adilet.zan.kz/rus/docs/P1700000407#z15

Киберщит Казахстана


https://www.itu.int/ru/ITU-D/Regional-Presence/CIS/Pages/News/20210810.aspx

Роль национального CIRT

- Обеспечивать общую координацию деятельности на национальном уровне
- Помогать операторам снижать риски связанные с кибербезопасностью
- Создавать надежный канал коммуникации между всеми заинтересованными
- Раннее оповещение о киберугрозах
- Координация реагирования на национальном уровне
- Помощь операторам в создании собственных возможностей реагирования
- Тестирование и измерение уровня зрелости и рекомендации по совершенствованию
- Продвижение культуры кибербезопасности на национальном уровне

Структура программы CIRT

- Фокусируется на создании возможностей реагирования на национальном уровне
- Соответствует FIRST Service Framework

Фаза оценки

CIRT Assessment

	Оценка
Описание	Пересмотр текущего уровня возможностей реагирования на национальном уровне
Действия	• Заполнение вопросника CIRT • Анализ ответов • Визит в страну для финализации • Страновой семинар
Результаты	Отчет с оценкой и рекомендациями
Модальность	Удаленно и физически
Затраты	Покрываются МСЭ или спонсором

Базовые услуги национального CIRT

Сотрудничество с национальным CERT Кыргызстана

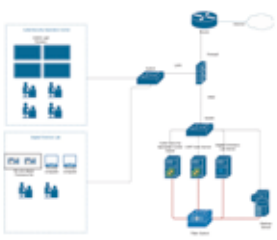
Национальный тренинг «Использование Open Source ПО для построения национального CIRT» (Бишкек, Кыргызстан, 4-7 марта 2019)

Сотрудничество с национальным CERT Кыргызстана

Первые национальные киберучения «Цифровой Кыргызстан 2021» (28-29 апреля 2021)


Проект по созданию CIRT в Кыргызстане

Совместный проект МСЭ, Всемирного Банка и Министерства цифрового развития



Глобальные и региональные учения

1	Совершенствование возможностей через глобальное и региональное сотрудничество и координацию
2	Повышение осведомленности и возможностей стран принимать участие и вносить вклад в создание стратегий реагирования на киберугрозы
3	Усиление международного сотрудничества между Государствами-Членами для обеспечения устойчивого совместного противодействия киберугрозам
4	Улучшение возможностей реагирования и коммуникации Государств-Членов
5	Помощь Государствам-Членам в разработке и реализации операционных процедур для реагирования на различные виды киберугроз

Структура учений

- **День 1-2:** целевые тренинги, например по обратному инжинирингу
- **День 3:** высокоуровневый форум по политике в области кибербезопасности
- **День 4-5:** работа в командах над конкретными сценариями кибератак

https://www.itu.int/en/ITU-D/Cybersecurity/Pages/cyberdrills.aspx

Региональные учения для Региона СНГ

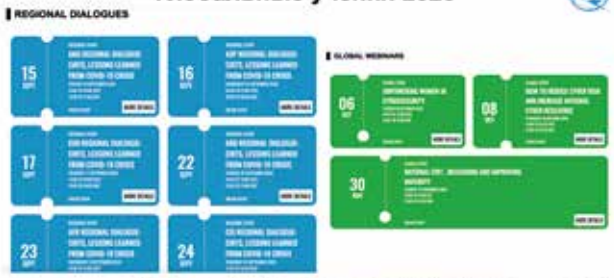
2018 (Баку, Азербайджан)

https://www.itu.int/ru/ITU-D/Regional-Presence/CIS/Pages/Events/2018/09_Baku/09_Baku.aspx

Межрегиональные учения для Азиатско-Тихоокеанского региона и СНГ

2019 (Куала-Лумпур, Малазия)

Глобальные учения 2020



https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Cyberdrills-2020.aspx

Глобальные учения 2020

https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Cyberdrills-2020.aspx

Глобальные учения 2021

https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Cyberdrills-2021.aspx

Глобальные учения 2021

Межрегиональные учения для стран СНГ и Арабского региона

2022 (Алма-Ата, Казахстан)

Правительственная сессия на PHDays 2023

Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации

positive technologies

О.С. Макаров

Директор БИСИ (Белорусский институт стратегических исследований)

На сегодняшний день мы не наблюдаем прорыва в сфере правового регулирования информационных отношений. Вероятно, это обусловлено рядом взаимосвязанных тенденций.

Во-первых, мы являемся свидетелями отката в научном и дипломатическом подходе к международно-правовому обеспечению международной информационной безопасности. Все больше внимания уделяется правилам и нормам.

Во-вторых, усиливается цифровое неравенство, которое, по всей видимости, становится целью санкционной политики. Ускоряется островизация информационных отношений, на уровне отдельных регионов идет процесс создания закрытых информационных систем и цифровых платформ.

В-третьих, мы видим процессы «коконизации» информационного пространства. Вокруг граждан формируются информационные коконы, которые не просто фильтруют, ограничивают и формируют вокруг людей информационную повестку, одновременно снижая порог критического восприятия информации, но и выполняют качественно новую функцию — конструируют новые смыслы.

В-четверных, государства-участники крупных объединений проявляют все большую готовность рассматривать деструктивные информационные воздействия, направленные на провоцирование конфликтной поляризации общественного сознания, отдельно от кибервоздействий, целью которых является нарушение функционирования информационной инфраструктуры.

В-пятых, наблюдается восходящая динамика тренда по милитаризации информационного пространства. Активно развиваются наступательные информационные потенциалы. Субъектами ответственности становятся сами государства. Оценка киберпреступлений исходит не международно-правовых норм, а с точки зрения обеспечения военной безопасности.

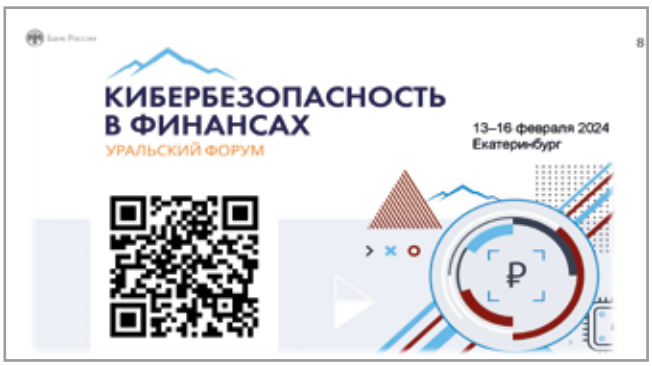
В-шестых, мы видим изменения правового поля. Постепенно исчезает бумажный документооборот, изменяется форма сделок, юридическая сила сделок без бумажных документов. В Республике Беларусь вплотную подошли к осмыслению такой сложной темы, как право на забвение.

Сегодня становится очевидной восходящая динамика тренда по формированию **региональных правовых режимов** обеспечения информационной безопасности. Особую важность приобретает региональное нормотворчество в целях согласования отвечающих приоритетам региональных государств правил и принципов регулирования международно-правовых отношений в информационной сфере.

Вместе с тем важно подчеркнуть, что широкая поддержка и мандат, зафиксированный в резолюции Генассамблеи ООН остаются безусловным преимуществом РГОС, которая является **основным межгосударственным переговорным форматом под эгидой ООН** для обсуждения вопросов безопасности в сфере использования ИКТ, в частности, связанных с установлением международно-правового режима обеспечения безопасности в информационной сфере.

В.А. Уваров
Директор Департамента информационной безопасности, Банк России

АКТУАЛЬНЫЕ ВОПРОСЫ МЕЖДУНАРОДНОГО СОТРУДНИЧЕСТВА БАНКА РОССИИ В СФЕРЕ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ФИНАНСОВЫХ ИНСТИТУТОВ



Д.И. Григорьев

Вице-президент Национальной Ассоциации международной информационной безопасности, генеральный директор АНО «Центр Координации государственно-частного партнерства в области международной информационной безопасности» (АНО «КОМИБ»)

Одним из важнейших национальных интересов Российской Федерации во внешнеполитической сфере является содействие устойчивому развитию российской экономики на новой технологической основе, а отрасль информационной безопасности на сегодня является одним из локомотивов технологического развития современного мира.

Для обеспечения экономической безопасности, экономического суверенитета, устойчивого экономического роста, повышения международной конкурентоспособности национальной экономики, сохранения ведущих позиций России в мировой экономике, а также в связи с недружественными действиями иностранных государств и их объединений, важно уделять приоритетное внимание укреплению российского присутствия на мировых рынках продуктов и услуг информационной безопасности. При этом, мы должны ориентироваться на государства, проводящие конструктивную и нейтральную политику в отношении Российской Федерации.

Продвижение импортозамещающих отечественных решений и услуг в области информационной безопасности на внешние рынки безусловно является важным элементом обеспечения безопасного и стабильного функционирования глобальной информационной сети, что способствует укреплению государственного суверенитета как России, так и дружественных стран. Кроме того, эта деятельность создает условия для недопущения иностранного контроля над национальными сегментами информационного пространства.

Сейчас важно, опираясь на прагматичные интересы российского бизнеса, определить:

- актуальные направления и приоритеты развития двустороннего сотрудничества с дружественными странами на уровне операторов связи, провайдеров и поставщиков ИКТ-услуг, а также производителей товаров и услуг в сфере информационной безопасности;
- стратегические интересы и приоритеты при развитии сотрудничества в рамках международных организаций: СНГ, БРИКС и пр.;
- цели и приоритетные задачи участия отечественного бизнеса в работе международных технологических организаций (МСЭ, ICANN, IEEE и др.) в современных условиях.

Происходящие тектонические изменения во внешнеполитической ситуации ставят перед нами новые вызовы: возникли ограничения по форматам нашей деятельности, существенно изменился состав наших зарубежных партнеров.

Задействование потенциала коммерческих компаний, их международных связей может и должно стать отдельным направлением по продвижению российских инициатив при формировании системы международной информационной безопасности.

Сегодня перед Национальной Ассоциацией международной информационной безопасности руководством страны поставлена задача по целенаправленному повышению эффективности государственно-частного партнерства в сфере информационной безопасности.

В качестве инструмента и операционного механизма для решения поставленной задачи создана автономная некоммерческая организация — «Центр координации государственно-частного партнерства в области международной информационной безопасности» (АНО КОМИБ).

Приоритетом деятельности АНО КОМИБ является ориентация на потребности и интересы операторов связи, провайдеров, поставщиков ИТ-услуг, а также производителей товаров и услуг в сфере информационной безопасности. Так в Уставе АНО КОМИБ закреплены следующие основные цели:

- координация практического взаимодействия государственно-ориентированных профильных российских коммерческих организаций, в том числе в целях развития ими партнерских отношений с зарубежными компаниями, по вопросам международной информационной безопасности;
- содействие национальным коммерческим компаниям, участвующим в соответствии с законодательством Российской Федерации в реализации государственной политики в области международной информационной безопасности.

Наша команда обладает серьезным опытом работы в области информационной безопасности в крупных промышленных структурах, финансовых институтах, компаниях телекома. Сертифицированные специалисты обладают необходимыми техническими и управленческими компетенциями и экспертизой. Понимая «изнутри» потребности бизнеса, а также используя политический потенциал НАМИБ, мы будем стремиться сделать АНО КОМИБ эффективным медиатором во взаимодействии коммерческих организаций с государственными структурами.

Считаем актуальным отходить от практики содействия отдельным компаниям и развивать системный подход государственной поддержки отрасли ИБ в целом, включая разработку комплекса мер по укреплению российского присутствия на мировых рынках технологий, продуктов и услуг обеспечения ИБ.

Мы видим свою задачу в содействии национальным поставщикам ИБ-решений и услуг, в установлении, поддержании и расширении деловых контактов с зарубежными партнёрами из дружественных стран, продвижении отечественных ИБ-продуктов на доступные внешние рынки.

Важным направлением работы считаем создание элементов инфраструктуры в интересах ИТ-компаний и повышение информационной безопасности российского бизнеса, включая платформы взаимодействия специалистов коммерческих компаний России и дружественных стран для консультаций и взаимной партнерской поддержки в решении операционных проблем обеспечения ИБ.

С учетом квалификации и потенциала нашей команды, мы видим свое место, в том числе, и в оказании консалтинговых услуг отечественному бизнесу ИБ при его внешнеэкономической деятельности.

КРУГЛЫЙ СТОЛ № 1

ГОСУДАРСТВЕННО-ЧАСТНОЕ ПАРТНЕРСТВО ПРИ РЕАЛИЗАЦИИ ГОСУДАРСТВЕННОЙ ПОЛИТИКИ В ОБЛАСТИ МИБ КАК МЕХАНИЗМ ОБЕСПЕЧЕНИЯ СУВЕРЕННЫХ ИНТЕРЕСОВ ОТЕЧЕСТВЕННОГО БИЗНЕСА В СОВРЕМЕННЫХ УСЛОВИЯХ

Ведущий:

Григорьев Д.И., вице-президент Национальной Ассоциации международной информационной безопасности, генеральный директор АНО «Центр Координации государственно-частного партнерства в области международной информационной безопасности» (АНО «КОМИБ»)

М.А. Громова

Директор по развитию бизнеса Security Vision

1 слайд: Уважаемый вице-президент НАМИБ, уважаемые коллеги, добрый день!

В первую очередь, благодарим организаторов за возможность презентовать сегодня свои идеи в рамках данного круглого стола. От лица компании «Security Vision» мы бы хотели сегодня выдвинуть предложение о создании коробочных центров мониторинга и реагирования информационной безопасности, также известных как секьюрити оперейшн центры (далее SOC) с поддержкой от государства, в качестве драйверов обеспечения технологического суверенитета и информационной безопасности Российской Федерации и дружественных стран. Наша компания представлена на данном заседании генеральным директором — Рахметовым Русланом Гиззатовичем и мной, Громовой Мариной Александровной, директором по развитию бизнеса. Прежде чем приступить к описанию нашего предложения, позвольте мне сказать несколько слов о нашей компании и ее продукции, а также сформировать актуальность озвученной концепции.

2 слайд: Наша компания является правообладателем платформенного комплекса по автоматизации ИБ. Платформа является 100% российской разработкой и включена в Единый реестр российских программ для ЭВМ и БД. На базе нашей платформы реализованы модули, относящиеся к различным ключевым направлениям информационной безопасности, таким как управление инцидентами, анализ угроз, киберразведка, поведенческий анализ, управление рисками и многие другие.

После начала специальной военной операции Российской Федерации на территории Украины большинство международных компаний в сфере информационной безопасности ушли из Российской Федерации. Как известно, введение санкций против Российской Федерации началось еще в 2014 году после вхождения Крыма в состав Российской Федерации. Наша компания вела разработки с 2010 года и вслед за упомянутыми событиями в 2015 году вывела на рынок ПОЛНОСТЬЮ отечественный продукт, импортозамещающий продукты таких международных компаний, как IBM, CISCO, Anomali, Fortinet и многих других, которые ранее обеспечивали информационную безопасность в нашей стране. Наш продукт не имеет никакой зависимости от иностранных систем. Все, иностранное, что в нем есть — это буквы в программном коде!

В настоящий момент мы и наши коллеги по индустрии, в том числе компании, присутствующие на данном заседании (уважаемые «Код Безопасности», «Ростелеком Солар» и другие) смогли обеспечить высокий уровень информационной безопасности как для частных клиентов, так и для ключевых промышленных предприятий и государственных ведомств. Хотелось бы обратить внимание, что совокупно все представители индустрии имеют в своем портфеле решения, технологически превосходящие иностранные аналоги.

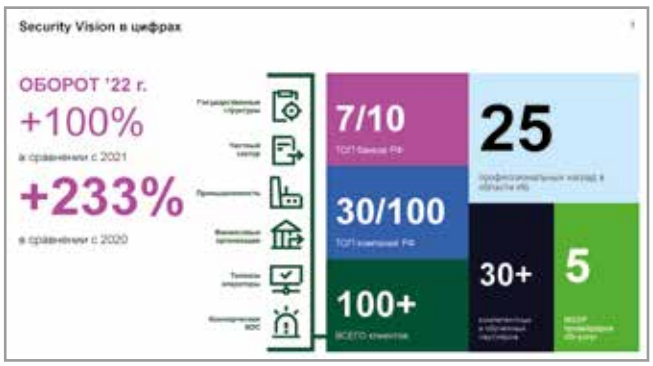
3 слайд: Продолжая знакомить вас с «Security Vision», хотелось бы углубиться в цифры, чтобы подтвердить успех конкретно нашей компании на отечественном рынке. За прошедший 2022 год нам удалось увеличить оборот компании вдвое. Если сравнивать с результатами 2020 года, то мы увидим рост на 233%. При этом оборот складывался из продаж предприятиям всех ключевых отраслей и секторов экономики. Имели место как непосредственные замещения иностранных аналогов, так и продажи решений в рамках потребностей заказчиков в защите инфраструктуры в новых реалиях.

Всего за годы коммерческой деятельности мы благополучно внедрили наши решения в более чем 100 организациях. Любопытно отметить, что внутри этой статистики. 7 из 10 Топ банков Российской Федерации являются нашими действующими заказчиками. Если говорить про Топ-100 компаний Российской Федерации, то мы поставляем наше решение уже в 30 организаций страны из данного списка. Имеем более 25 профессиональных наград в области ИБ. Более 30 обученных партнеров, которые также несут свою экспертизу по нашему решению в организации, с которыми они взаимодействуют. Также за годы нашей деятельности в нашей схеме бизнеса прочно и качественно укрепился такой формат, как продажи услуг по информационной безопасности через сервисную модель предоставления услуг (также известную в бизнес сообществе как MSSP). Тут мы имеем 5 действующих и востребованных контрактов с ключевыми российскими центрами предоставления услуг по мониторингу и реагированию на инциденты информационной безопасности (SOC-провайдерами).

4 слайд: Отдельно хотелось бы обратить внимание на наших уважаемых действующих заказчиков, которые согласовали размещение своих логотипов в публичных презентациях. В подтверждение моих предыдущих слов вы можете увидеть на слайде как представителей крупной промышленности, так и топ-банки, госструктуры, региональные правительства. Также на слайде представлены наши партнеры — SOC-провайдеры, которые упоминались чуть ранее. Отдельно хотелось бы выделить компанию «Ростелеком Солар», с которой мы имеем долгосрочное партнерство в данном направлении. На данной тематике хотелось бы остановиться чуть позднее в деталях.

5 слайд: В настоящее время продукты российских производителей ПО являются высокотехнологичными решениями в сфере ИБ. В связи с этим в нашу компанию обращались и на постоянной основе проявляют интерес представители бизнеса из таких стран, как Объединенные Арабские Эмираты, Сирия, Саудовская Аравия, Египет, Перу, Бангладеш, Индия, Иран, Катар, Пакистан и многие другие. Согласно проекту рейтинга АНО «Цифровая экономика», большинство из перечисленных стран являются приоритетными для экспорта российской ИТ-продукции в текущих геополитических условиях.

Наша компания уже имеет благоприятный опыт по внедрению собственной продукции в страны СНГ. Мы имеем технологические возможности и экспертизу для масштабирования своего опыта на другие дружественные государства. Однако в ходе точечных моновендорных встреч с иностранными представителями



была выявлена проблематика, относящаяся в основном к культурно-политической специфике ведения бизнеса в восточных государствах, а именно, необходимость постоянной представленности компании на территории данных государств. К представленности иностранные коллеги относят либо действующий филиал организации вендора на территории страны, либо постоянное присутствие представителя вендора на территории иностранного государства. Это здравое и логичное требование, учитывая восточный менталитет. Однако хаотичное открытие офисов всех игроков отечественного рынка в разных государствах может привести только к оттоку денежных средств из страны. Тут требуется единый подход — не каждого отдельного вендора со своими интересами, а всех игроков рынка как одной машины по обеспечению технологического суверенитета дружественных стран.

Интерес данных государств именно к российским решениям был вызван несколькими факторами, к которым можно отнести лидерство российской разработки в мировом масштабе, независимость ее от американских разработок и технологий. К американским технологиям данные государства относятся настороженно в связи с агрессивной политической позицией США.

Мы, совместно с коллегами из индустрии, объединив экспертизы и выйдя единым фронтом с поддержкой государства, могли бы повторить успех по построению качественного уровня информационной безопасности в России, масштабируя его на дружественные страны, тем самым укрепляя экономику страны и способствуя притоку денежных средств в Российской Федерации.

Отдельно стоит отметить, и уверена, коллеги согласятся с нашим утверждением: по опыту множества встреч на международном уровне и попыток выхода за рубеж, коммерческому блоку Российской Федерации невероятно сложно продвигать свои решения не только из-за вопросов присутствия «на земле», а главным образом из-за разности уровней коммуникации. Модель, при которой бизнес продвигает решение на государственный уровень других стран, показала себя несостоятельной. Единственно верная тут горизонталь взаимодействия — это модель сотрудничества от государства к государству и далее от бизнеса к бизнесу.

6 слайд: Нам необходима единая точка входа в дружественные страны, возможно, на уровне кластеров. Как пример — Египет, как хаб для стран Африки и Ближнего Востока. Это лишь пример, совета тут мы бы хотели просить как раз у государства.

На данном слайде представлена примерная схема такого взаимодействия. Аналогия с газовой трубой проведена неслучайно. Это

отработанная концепция упомянутой схемы — взаимодействия государства с государством, и, далее, бизнеса с бизнесом для экспорта продукции.

Как я упоминала в начале выступления, в качестве инструмента по реализации данной концепции мы видим продвижение коробочных SOC (центров предоставления услуг по мониторингу и реагированию на инциденты информационной безопасности) за пределами РФ. В нашей концепции со стороны государства необходима поддержка отечественного центра — эксперта в области построения SOC на международном уровне (в странах или хабах). Мы видим, что данный центр, имея готовую экспертизу «на земле», мог бы обеспечивать развитие бизнеса уже путем взаимодействия с местными интеграторами для предоставления услуг конечным заказчикам, в том числе государственным, на территориях дружественных стран.

Также мы представили на слайде классическую схему SOC. Центр сочетает в себе сильнейшие технологии крупнейших игроков рынка ИБ, обеспечивая защиту организаций заказчиков от угроз любого уровня сложности. Благодаря работе подобного центра осуществляется разведка и раннее предупреждение об угрозах, оценка рисков и управление уязвимостями, используются расширенные возможности мониторинга и анализа событий информационной безопасности в режиме 24/7, осуществляется противодействие атакам на ранней стадии. Также SOC позволяет осуществить оперативное техническое расследование, ликвидацию последствий и устранение причин возникновения инцидентов. Наша технология в данной модели выступает «зонтиком» — звеном, которое интегрируется с любой существующей на рынке ИТ и ИБ системой, объединяет все продукты и позволяет выстроить реагирование, значительно сократив при этом физические человеческие затраты на обработку информации и исключив ошибки при осуществлении действий.

Имея многолетний опыт по интеграции с SOCами, а также непосредственные продажи во всех отраслях, мы считаем, что на рынки дружественных стран необходимо выходить с уже сформированной экспертизой, которая может быть разбита по пакетам в зависимости от отрасли, которой предлагается данный пакет. Условно говоря, для банков мы можем продавать набор экспертизы, помимо прочего включающий в себя модуль по взаимодействию с регуляторами, по аналогии с отечественным ФИНЦЕРТ. Для госструктур в пакет можем включать экспертизу по взаимодействию с НКЦКИ. Повторюсь, что данная модель невероятно востребована на российском рынке во всех отраслях.

7 слайд: В качестве шагов со своей стороны, для обеспечения функционирования данных центров мы можем предложить различного рода экспертизу. В первую очередь экспертизу собственного учебного центра, а также ВУЗов-партнеров, которые строят свои образовательные программы на базе нашей платформы и на базе продуктов других известных игроков ИБ-рынка. Это такие крупнейшие российские ВУЗы, как: Московский государственный технический университет им. Н.Э. Баумана, Национальный исследовательский ядерный институт МИФИ, Сибирский государственный университет науки и технологии имени академика М.Ф. Решетнева, Новосибирский государственный технический университет, АНО Иннополис. Тут мы могли бы выступить единым фронтом для обеспечения базой знаний отечественного интегратора, выходящего на международные рынки с поддержкой государства. Со стороны поддержки иностранных интеграторов, мы могли бы задействовать также опыт и ресурс нашего образовательного партнера АНО Иннополис, который осуществляет обучение полностью на английском языке и имеет в штате множество иностранных специалистов, в том числе из стран Ближнего Востока, которые могут осуществить посильную помощь в образовании игроков местного рынка на родном языке.

8 слайд: Уважаемые коллеги, благодарю вас за внимание. Закончить свою презентацию хотелось бы, перефразируя слова великого Архимеда: «Дайте нам точку опоры, и мы перевернем мир информационной безопасности на международном уровне, как уже сделали это на внутригосударственном уровне. Готовы к вопросам с вашей стороны».

КРУГЛЫЙ СТОЛ № 2
ПЕРСПЕКТИВЫ ФОРМИРОВАНИЯ МЕЖДУНАРОДНО-ПРАВОВОГО РЕЖИМА РЕГУЛИРОВАНИЯ СФЕРЫ ИСПОЛЬЗОВАНИЯ ИКТ

Ведущий:
Стрельцов А.А., доктор технических наук, доктор юридических наук, профессор МГУ им. М.В. Ломоносова, вице-президент Национальной Ассоциации международной информационной безопасности

А.А. Стрельцов
Доктор технических наук, доктор юридических наук, профессор, вице-президент Национальной Ассоциации международной информационной безопасности, ведущий научный сотрудник факультета вычислительной математики и кибернетики МГУ имени М.В. Ломоносова

О ПРОБЛЕМАХ ФОРМИРОВАНИЯ СИСТЕМ ОБЕСПЕЧЕНИЯ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1. В соответствии с Программой Круглого стола хотел бы поделиться размышлениями о проблемах формирования систем международной информационной безопасности.

Международное сообщество продолжает в целом придерживаться идеи создания на основе реализации потенциала ИКТ глобального информационного общества. Об этом можно судить, например, по резолюциям Генеральной Ассамблеи ООН по вопросу о достижениях в области информатизации и коммуникаций в контексте международной безопасности, а также некоторым другим документам. Построение глобального информационного общества в документах Всемирной встречи на Высшем уровне (2003–2005 гг.; Женева, Тунис) было объявлено глобальной задачей нового тысячелетия. Лейтмотивом понимания глобального информационного общества, предложенного в Декларации принципов Всемирной встречи, его теоретической основой, как представляется, являются два положения.

Первое положение утверждает, что «общение является одним из основополагающих социальных процессов, одной из базовых человеческих потребностей и фундаментом любой социальной организации».

Второе положение утверждает, что «использование потенциала ИКТ может позволить решить наиболее острые социальные проблемы современного мира — «нищета и голод, получение образования, равенство мужчин и женщин, сокращение детской смертности, борьба с заболеваниями, экологическая устойчивость, формирование глобального партнерства для обеспечения более мирного, справедливого и процветающего мира».

Трудно усомниться в справедливости этих положений. Однако за прошедшее время стало понятно, что все не так просто.

Во-первых, «общение» не является обезличенным и бесцельным процессом. «Общение» состоит из актов обмена социально значимой информацией между субъектами социального взаимодействия.

Можно показать, что цель «общения», т.е. обмена социально значимой информацией, заключается в организации и реализации социального взаимодействия между субъектами жизнедеятельности национальных обществ — граждан, организаций и государств. В рамках этого «общения» осуществляется согласование целей и условий социального взаимодействия, представлений о справедливом разделении результатов совместной деятельности, о механизмах контроля соблюдения достигнутых договоренностей, а также о механизмах разрешения возникающих споров. Например, международное сотрудничество государств в области формирования глобального информационного общества базируется, с одной стороны, на понимании близости их национальных интересов, а с другой — на близости представлений о способах применения международного права к деятельности государств в ИКТ-среде, направленной на удовлетворение национальных интересов. В результате обсуждения этих вопросов на различных международных площадках, а также опыте

практического сотрудничества выяснилось наличие существенных противоречий между национальными интересами США, других «западных» государств, и национальными интересами большинства государств мира.

Одновременно выявилось существенное расхождение представлений о добросовестности применения норм и принципов международного права к отношениям государств в ИКТ-среде. В результате началась трансформация однополярного механизма формирования глобального информационного общества в многополярный. В многополярном глобальном информационном обществе представления о справедливости в ИКТ-среде будут вырабатываться на основе равноправного общения суверенных государств мира.

Другими словами, прошедшее время показало, что выделенная в Декларации принципов информационного общества потребность субъектов социальной жизни «создавать информацию и знания, иметь к ним доступ, пользоваться и обмениваться ими, с тем чтобы дать отдельным лицам, общинам и народам возможность в полной мере реализовать свой потенциал, содействуя своему устойчивому развитию и повышая качество своей жизни» не является единственной потребностью, обусловливающей международное сотрудничество государств в области интеграции в глобальное информационное общество. Не менее важной потребностью, стимулирующей интеграцию современных национальных обществ в глобальное информационное общество, является соблюдение равенства и справедливости.

Во-вторых, стало понятно также, что использование ИКТ само по себе не приносит мира, да и процесс формирования глобального партнерства зависит не только от применения ИКТ.

Выяснилось также, что ИКТ-среда как пространство реализации социального взаимодействия, существенно отличается от привычного физического пространства. Так, социально значимая информация, представленная в цифровой форме, приобретает виртуальный характер. Соответственно субъекты взаимодействия теряют возможность лично контролировать как корректность процесса передачи и понимания этой информации другими субъектами, так и реальность существования самих субъектов взаимодействия. Они вынуждены полагаться на добросовестность организаций и государств, обеспечивающих функционирование глобальной ИКТ-среды, а также на корректность реализации процессов сбора, обработки, передачи, хранения и распространения информации.

В то же время эффективность привычных механизмов обеспечения добросовестности поведения субъектов социального взаимодействия — этических норм поведения, национального и международного права существенно снижается. У субъектов отсутствует возможность визуального контроля за поведением государств в ИКТ-среде. Отсутствие этой возможности не может быть компенсировано развитием мер доверия, применением добровольных необязательных, по существу, этических, норм ответственного поведения государств. Примером может служить проблема разрешения спорных ситуаций в ИКТ-среде. Несмотря на значительное количество ситуаций, возникающих по подозрению в недобросовестности поведения некоторых государств, пока не известны случаи признания государствами себя стороной этих спорных ситуаций. Соответственно для разрешения этих ситуаций затруднительно применить мирные средства, предусмотренные ст. 33 Устава ООН.

Таким образом, одним из принципов построения глобального информационного общества должен стать принцип безопасности информационного взаимодействия субъектов жизнедеятельности национального общества в ИКТ-среде (принцип информационной безопасности).

2. В рамках реализации этого принципа международное сообщество должно стимулировать принятие государствами мер по противодействию угрозам недобросовестного поведения субъектов социального взаимодействия граждан, организаций и государств в ИКТ-среде.

Деятельность в этом направлении логично дополнит предпринимаемые усилия по наращиванию потенциала и развитию системы мер доверия, включенных в мандат Рабочей Группы ООН открытого состава по вопросам безопасности в сфере использования ИКТ и самих ИКТ 2021–2025 гг.

Как известно, Российская Федерация, Республика Беларусь, Корейская Народно-Демократическая Республика, Республика Никарагуа и Сирийская Арабская Республика внесли концепцию Конвенции ООН об обеспечении международной информационной безопасности в качестве официального документа 77-й сессии Генеральной Ассамблеи ООН. Другим странам было предложено присоединиться к этому документу. Тем самым дан старт ее международному обсуждению. Впервые с инициативой подготовки такой Конвенции в 2011 году выступил Секретарь Совета Безопасности Российской Федерации Николай Платонович Патрушев. Осенью 2011 года концепция Конвенции была представлена в Екатеринбурге, на II Международной встрече высоких представителей, курирующих вопросы безопасности.

Необходимо отметить, что потребность в подготовке Конвенции об обеспечении международной информационной безопасности сейчас ощущается особенно остро, так как международное сообщество выходит на новый этап обсуждения проблемы формирования систем международной информационной безопасности. Представляется, что на этом этапе обсуждение актуальности данной проблемы сменится обсуждением предложений по ее решению. В отличие от многих появившихся в последнее время инициатив, таких как подготовка Декларации за будущее Интернета (США); Дорожная карта по цифровому сотрудничеству (Генеральный Секретарь ООН); Программа действий по поощрению ответственного поведения государств в киберпространстве, а также целей проведения Саммита за демократию, концепция Конвенции содержит такие предложения.

Положения концепции Конвенции представляют собой комплексную систему взглядов на систему обеспечения безопасности глобального информационного общества на основе взаимодействия суверенных государств. Каждое из этих государств представляет национальное общество, которое стремится на основе сохранения национальной системы духовных и культурных ценностей и международного сотрудничества решить проблемы «нищеты и голода, получения образования, равенства мужчин и женщин, сокращения детской смертности, борьбы с заболеваниями, экологической устойчивости, формирования глобального партнерства для обеспечения более мирного, справедливого и процветающего мира».

Структурно концепция Конвенции включает преамбулу, заключительную часть и пять глав основного материала.

В первой главе сформулированы предложения по предмету и целям предлагаемой Конвенции, а также используемые термины.

Во второй главе изложены подходы к формированию механизма предотвращения и разрешения военных конфликтов в информационном пространстве.

В третьей главе предлагается система мер по противодействию использованию информационного пространства в террористических целях.

В четвертой главе изложены предложения по системе мер, направленных на противодействие правонарушениям в информационном пространстве.

В пятой главе изложены предложения по организации сотрудничества государств в области международной информационной безопасности.

Существенным вкладом в обсуждение предложений, представленных в концепции Конвенции, могло бы стать проведение российскими и зарубежными экспертами совместного исследования путей реализации положений концепции. Определенный опыт проведения подобных исследований у Национальной Ассоциации международной информационной безопасности имеется.

Так, под эгидой Национальной Ассоциации международной информационной безопасности в 2022 году выполнена работа по изучению ряда проблем применения международного права в ИКТ-среде. В работе принимали участие ведущие российские эксперты в области международного права и обеспечения безопасности использования ИКТ. Инициатором выполнения работы был первый Президент Ассоциации Владислав Петрович Шерстюк. Основные результаты работы изложены в монографии, выпущенной на русском и английском языках, электронная версия которой размещена на сайте Ассоциации.

Под эгидой Международного исследовательского консорциума по информационной безопасности, созданного по инициативе

участников Международного Форума «Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности» (2010 г.), экспертами из Российской Федерации, Эстонии, Финляндии, США и Швейцарии была проведена работа по изучению проблем применения норм ответственного поведения государств в ИКТ-среде (2018–2020 гг.). Отчет о результатах работы представлен на сайте Ассоциации. При наличии заинтересованности экспертов государств-членов региональных организаций и образований международного сотрудничества представляется возможным осуществить под эгидой Консорциума исследование проблем формирования региональных систем обеспечения международной информационной безопасности (Союзное государство, БРИКС, ШОС и другие).

Д.В. Бабекин
Заместитель директора Департамента международного права и сотрудничества, Минюст России

ВОПРОСЫ ПРИМЕНИМОСТИ ОБЩЕПРИЗНАННЫХ ПРИНЦИПОВ МЕЖДУНАРОДНОГО ПРАВА К СФЕРЕ ИСПОЛЬЗОВАНИЯ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ С УЧЕТОМ СПЕЦИФИКИ ДАННЫХ ТЕХНОЛОГИЙ

Общепризнанные принципы и нормы международного права являются юридической основой деятельности государств по поддержанию международного мира и безопасности и предотвращению конфликтов,

а также ключевым фактором укрепления доверия между государствами

в данной сфере.

Необходимо соблюдение общепризнанных принципов и норм международного права, прежде всего закрепленных в Уставе ООН и Декларации о принципах международного права, касающихся дружественных отношений и сотрудничества между государствами в соответствии с Уставом ООН от 24 октября 1970 г., применительно к сфере использования ИКТ:

- принципа суверенного равенства государств;
- принципа неприменения силы и угрозы силой;
- принципа разрешения международных споров мирными средствами;
- принципа невмешательства во внутренние дела государств;
- принципа равноправия и самоопределения народов;
- принципа добросовестного выполнения обязательств
- по международному праву;
- принципа нерушимости государственных границ;
- принципа территориальной целостности государств;
- а также обязанности государств сотрудничать друг с другом и действовать в целях предотвращения и устранения угрозы миру, нарушения мира и актов агрессии в соответствии с Уставом ООН.

Применение указанных принципов и норм международного права в сфере использования ИКТ не должно осуществляться автоматически ввиду особой правовой природы информационной среды. Речь, в частности, о таких особенностях, как трансграничный и всепроникающий характер ИКТ, анонимность их использования, возможность их применения для целей двойного назначения, возможность наличия скрытых от пользователей уязвимостей и вредоносных функций.

При этом представляется целесообразным исходить из следующей трактовки отдельных принципов международного права применительно к информационной среде.

Принцип суверенного равенства государств

Все государства пользуются суверенным равенством в ИКТ-среде, т.е. должны иметь одинаковые права и обязанности и являться ее равноправными субъектами независимо от различий экономического, политического, технологического или иного характера.

Суверенное равенство в ИКТ-среде означает, что все государства пользуются в ней равными правами, свободно выбирают и развивают свою ИКТ-инфраструктуру, обеспечивают ее безопасность и устойчивость функционирования, уважают неприкосновенность ИКТ-инфраструктуры других государств, полностью и добросовестно выполняют свои

международные обязательства, связанные с использованием ИКТ-среды, и живут в мире с другими государствами.

Суверенитет государства в информационном пространстве подразумевает под собой суверенное право государств определять свою политику и осуществлять регулирование в сфере использования ИКТ на своей территории и (или) под своей юрисдикцией.

Принцип разрешения международных споров мирными средствами

Государства должны стремиться к скорейшему и справедливому разрешению своих международных споров, связанных с использованием ИКТ, в соответствии с Уставом ООН.

Государства, являющиеся сторонами в международном споре, связанном с использованием ИКТ, а также другие государства должны воздерживаться от любых действий, которые могут обострить положение настолько, что будет поставлено под угрозу поддержание международного мира и безопасности, и должны действовать в соответствии с целями и принципами ООН.

Принцип невмешательства во внутренние дела других государств

Ни одно государство или группа государств не имеет права вмешиваться прямо или косвенно с использованием ИКТ по какой бы то ни было причине в дела, входящие во внутреннюю компетенцию другого государства.

Все формы вмешательства во внутренние дела государств или любые угрозы, направленные против правосубъектности государства или против его конституционных, политических, экономических и культурных основ, совершенные с использованием ИКТ, являются нарушением международного права.

Государства не должны организовывать, поощрять, разжигать, финансировать, подстрекать или допускать деятельность с использованием ИКТ, направленную против конституционного строя другого государства, равно как и способствовать ей.

Государства не должны применять или поощрять применение противоправных односторонних принудительных мер с целью добиться каких бы то ни было преимуществ в ИКТ-среде.

Принцип сотрудничества государств

В целях поддержания международного мира и безопасности при использовании ИКТ государства независимо от различий в их политических, экономических и социальных системах обязаны сотрудничать друг с другом.

Государства должны стремиться к созданию наиболее благоприятных условий для функционирования международной взаимоувязанной сети электросвязи, выработке в рамках компетентной международной межправительственной организации согласованных стандартов ее использования, а также совершенствованию протоколов связи, позволяющих однозначно определять источники электронных сообщений.

С.А. Комов
Эксперт, Минобороны России

О ПРИМЕНИМОСТИ МЕЖДУНАРОДНОГО ПРАВА В ВОЕННО-ПОЛИТИЧЕСКОМ ИЗМЕРЕНИИ В ИНФОРМАЦИОННОЙ СФЕРЕ[1]

Уважаемые коллеги!

Тема совершенствования международного права, регулирующего применение военной силы, имеет непреходящее значение для сохранения мира, обеспечения международной безопасности и стратегической стабильности. Она неразрывно связана с историей становления и развития ряда основных положений международного права, к которым относятся: принципы неприменения силы и угрозы силой, невмешательства во внутренние дела другого государства, а также право на самооборону, принципы и нормы международного гуманитарного права.

В современных условиях рассмотрение данных положений применительно к глобальному информационному пространству имеет чрезвычайную актуальность.

В первую очередь, это касается **принципа неприменения силы и угрозы силой.**

Агрессивная война как апогей применения силы была впервые названа международным преступлением по итогам Первой мировой войны, унесшей жизни 9,4 млн человек. После Второй мировой войны, в которой погибло уже более 50 млн человек, принцип запрещения агрессивной войны трансформировался во всеобъемлющий принцип неприменения силы и угрозы силой в международных отношениях. Важной вехой на этом пути явился Устав ООН, который установил, что «все члены Организации Объединенных Наций воздерживаются в их международных отношениях от угрозы силой или ее применения как против территориальной неприкосновенности или политической независимости любого государства, так и каким-либо другим образом, несовместимым с Целями Организации Объединенных Наций» (п. 4 Ст. 2). В 2023 году мировое сообщество в лице Рабочей группы открытого состава ООН по вопросам безопасности в сфере использования ИКТ и самих ИКТ (РГОС) пришло к согласию в отношении того, что данное положение целиком и полностью распространяется на использование ИКТ. Это закреплено во втором промежуточном докладе РГОС[2].

Вместе с тем, само понятие «сила» ни в Уставе, ни в других международно-правовых актах прямо не раскрывается. Полагаем, что для понимания логики авторов Устава ООН нужно представить, что они вкладывали в его содержание в контексте окончания самой страшной мировой войны, в финале которой было впервые применено ядерное оружие.

По нашему мнению, в послевоенной обстановке под «силой» понималась, в первую очередь, военная сила. В свою очередь, основным ее проявлением считалось «вооруженное нападение», т.е. применения оружия, которое ведет к человеческим жертвам и разрушениям.

Убеждены, что именно с такой меркой нужно подходить к квалификации использования информационно-коммуникационных технологий (ИКТ) в военных целях. Наличие жертв

1 Выступление подготовлено коллективом военных экспертов в составе В.О.Запивахин, С.П.Юниченко, В.В.Филиппов, А.Л.Шевченко, С.А. Комов.

2 Пункт c) статьи 30 Второго ежегодного промежуточного доклада Рабочей группы открытого состава ООН по вопросам безопасности в сфере использования ИКТ и самих ИКТ, представленный на 78 сессии Генеральной Ассамблеи ООН в соответствии с резолюцией 75/240.

и разрушений однозначно подтверждает факт совершения вооруженного нападения, даже если это результат проведения компьютерной или иной информационной атаки.

Здесь уместно обсудить вопрос реагирования на вооруженное нападение с использованием ИКТ, т.е. применимость **права на самооборону** как единственного законного исключения из общего правила запрета применения силы.

В соответствии со ст. 51 Устава ООН индивидуальная или коллективная самооборона в ответ на вооруженное нападение отнесена к правомерным случаям применения силы. Разъяснение относительно того, создает ли данное положение основу для проведения ответных военных действий против государства, не применяющих оружие, дал Международный суд ООН в деле «Никарагуа против США». В своем решении он определил, что государства не имеют права на применение военной силы в ответ на действия, которые не составляют вооруженного нападения[3]. Поэтому, если компьютерные атаки, не будут квалифицированы как вооруженное нападение, пострадавшая сторона не будет иметь законного права на самооборону с использованием обычного вооружения.

Резюмируя вышесказанное следует отметить, что по смыслу Устава ООН практически весь массив совершаемых в настоящее время компьютерных и иных информационных атак не является вооруженным нападением, т.к. не ведет к каким-либо жертвам и разрушениям. Поэтому невозможно обоснованно приписать авторам этих атак участие в совершении преступления агрессии, как это периодически пытаются делать отдельные иностранные властные структуры.

Говоря о применимости **принципа невмешательства во внутренние дела других государств**, следует в первую очередь, отметить, что **вооруженное вмешательство** является синонимом агрессии[4] и все вышеприведенные рассуждения справедливы для него.

Невооруженное вмешательство несомненно также является нарушением международного права. В этом же контексте следует рассматривать применение ИКТ для совершения актов невооруженного вмешательства во внутренние дела других государств. Однако, как показывает углубленное исследование данного вопроса, подобный вид вмешательства в настоящее время широко используется в международных отношениях. Одной из очевидных причин такого положения можно считать отсутствие в международном праве жестких норм об ответственности за эти нарушения.

Международное гуманитарное право (МГП) также сформировалось в доинформационную эру и поэтому действие его принципов и норм не может быть безоговорочно распространено на все варианты использования ИКТ в ходе вооруженного конфликта.

По нашему мнению, ключевым критерием, определяющим возможность объективного решения этой задачи, являются жертвы и разрушения, в том случае, если они возникли непосредственно вследствие использования ИКТ.

Все иные виды ущерба не могут быть признаком применимости МГП к использованию ИКТ в ходе вооруженного конфликта. Поэтому блокирование Интернета, отсутствие связи, сбой навигации, дезорганизация управления и т.п. не могут свидетельствовать о нарушении норм и принципов МГП. Соответственно и деяния, вызвавшие этот ущерб, не подпадают под действие соответствующих решений Нюрнбергского трибунала.

Таким образом, принцип неприменения силы и угрозы силой, принцип невмешательства во внутренние дела других государств, право на самооборону, а также принципы и нормы МГП могут быть применены только к такому использованию ИКТ, которое создает ущерб сопоставимый с ущербом от использования обычных видов оружия. Из истории известен только один случай такого использования ИКТ — атака вируса Stuxnet на ядерные объекты Ирана в 2010 году. Все остальные виды военного использования ИКТ, в том числе наступательного характера не являются применением оружия и не подпадают под применение названных институтов международного права.

3 Дело о военной и военизированной деятельности в Никарагуа и против Никарагуа (Никарагуа против Соединённых Штатов Америки). Решение от 27 июня 1986 г., ICJ Reports, 1986, p. 195, 232.

4 Декларация о недопустимости вмешательства во внутренние дела государств, об ограждении их независимости и суверенитета. Принята резолюцией 2131 (XX) Генеральной Ассамблеи от 21 декабря 1965 года.

В заключение следует отметить, что помимо установления критерия тяжести гуманитарных последствий применения ИКТ, к условиям, определяющим реальность применения существующего международного права в информационной сфере, следует отнести выработку мер преодоления анонимности и скрытности действий в этой сфере, а также формирование универсальной методологии расследования фактов агрессивного или иного враждебного использования ИКТ, позволяющих оперативно и достоверно определять источник их совершения.

Благодарю за внимание!

А.Я. Капустин
Доктор юридических наук, профессор, заслуженный деятель науки РФ, заведующий кафедрой международного права ИЗИСП

КОНЦЕПЦИЯ СОТРУДНИЧЕСТВА ГОСУДАРСТВ ПО ПРИМЕНЕНИЮ СИСТЕМЫ МЕР ДОВЕРИЯ И МЕР ПО НАРАЩИВАНИЮ ПОТЕНЦИАЛА В ИКТ-СРЕДЕ: МЕЖДУНАРОДНО-ПРАВОВЫЕ ПРОБЛЕМЫ

Доверие является этической категорией, своего рода мерой добросовестного, честного, порядочного поведения каких-либо субъектов деятельности (человека и иных контролируемых людьми существ). В этом своем качестве добросовестность выступает и мерилом ответственного поведения в международных отношениях. Недаром, сам термин в новейшее время обязан своему происхождению военно-политическому сотрудничеству государств, относящихся к соперничающим блокам или группам. Впервые термин «меры укрепления доверия» был употреблен в Заключительном акте Совещания по сотрудничеству и безопасности в Европе (СБСЕ) 1975 года[1]. Опыт СБСЕ был воспринят ООН, ее системой, а также рядом других международных организаций, в том числе региональных, в целях сохранения и упрочения международного мира и стабильности в различных сферах[2].

В резолюции Генеральной Ассамблеи ООН «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» 53/70 от 4 января 1999 г. отмечалась необходимость совместного сотрудничества всех государств-членов ООН в борьбе с разнообразными угрозами в информационной среде. Впоследствии Генеральная Ассамблея ООН (далее — ГА ООН) в резолюциях с аналогичным названием — «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» (например, в резолюции ГА ООН 74/29 от 12 декабря 2019 г.[3]) отмечает, что ООН должна поощрять меры по укреплению доверия и повышению транспарентности в сфере ИКТ, а также способствовать наращиванию потенциала и распространению передового опыта).

В дальнейшем разработка вопросов мер по укреплению доверия и наращивания потенциала стала предметом рассмотрения и подготовки рекомендаций вначале в 2004 г. рабочей группы правительственных экспертов (РГЭ), шестая по счету завершила работу в мае 2021 г. принятием на основе консенсуса отчета. Возникновение разногласий на переговорах в ходе раунда 2016–2017 гг. привело к тому, что в 2018 г. ГА ООН приняла поддержанную Россией резолюцию о создании Рабочей группы ООН открытого состава (РГОС), и поддержанную США резолюцию новой РГЭ.

В Докладе Группы правительственных экспертов по поощрению ответственного поведения государств в киберпространстве в контексте международной безопасности мерам укрепления доверия посвящен раздел V, а вопросам наращивания потенциала в области ИКТ раздел VI («Международное сообщество и помощь по линии обеспечения безопасности и наращивания потенциала в области

1 Совещание по безопасности и сотрудничеству в Европе. Заключительный Акт. Хельсинки, 1975.// 2. Документ по мерам укрепления доверия и некоторым аспектам безопасности и разоружения. Подробнее см..: Тузмухамедов Б.Р. Меры по укреплению доверия//Международное право и международная безопасность. Диалог советских и американских экспертов. М., 1991, с.317.

2 Так, в отношении космической деятельности термин «меры доверия» используется в резолюциях Генеральной ассамблеи ООН с 1990 г.

3 См.: Дос. ООН: A/RES/74/29, 18 December 2019.

ИКТ»)[4]. В нем в частности было подчеркнуто значение мер по укреплению доверия в области ИКТ для благоприятствования укреплению доверия, сотрудничества, транспарентности и предсказуемости, тем самым они могут способствовать стабильности и снижению риска недопонимания, эскалации и конфликта. В то же время высказано понимание, что укрепление доверия нельзя рассматривать как одномоментное решение, напротив, оно представляет собой долгосрочную и последовательную работу, требующую постоянного вовлечения государств, при поддержке со стороны ООН, региональных и субрегиональных органов и других заинтересованных сторон.

Концептуально меры укрепления доверия выражены в двух взаимосвязанных комплексах действий: совместных мерах государств и мерах по обеспечению транспарентности. Совместные меры включают назначение компетентных координаторов на политическом и техническом уровнях для обеспечения надежной и прямой связи между государствами в целях предотвращения и урегулирования серьезных инцидентов в сфере ИКТ и ослабления напряженности в кризисных ситуациях. Предполагается, что наделение координаторов соответствующими средствами и коммуникация между ними смогут помочь снизить напряженность и предотвратить недопонимание и неверное толкование, которые могут возникнуть в результате инцидентов в сфере ИКТ, в том числе затрагивающих критически важную инфраструктуру и имеющих национальное, региональное или глобальное значение.

Дополнением к институционному механизму выступает предложение о поддержании диалога в рамках двусторонних, субрегиональных, региональных и многосторонних консультаций и взаимодействия, что может способствовать углублению взаимопонимания между государствами, укреплению доверия и содействию более тесному сотрудничеству между ними в деле смягчения воздействия инцидентов в сфере ИКТ при одновременном снижении рисков недопонимания и эскалации. Другие заинтересованные стороны, такие как частный сектор, научные и технические круги и гражданское общество, могут внести значительный вклад в содействие проведению таких консультаций и налаживанию такого взаимодействия.

В Докладе подчеркнуто особое значение для укрепления доверия и предсказуемости, сокращения возможностей для неправильного толкования и эскалации и оказания помощи отдельным лицам и организациям в принятии правильных решений в области управления рисками обеспечение транспарентности на добровольной основе путем обмена национальными мнениями и опытом по инцидентам, связанным с безопасностью ИКТ, и другим связанным с ними угрозам, а также путем обнародования связанных с ИКТ советов по обеспечению безопасности, рекомендаций, руководящих указаний, фактологической базы и подтверждающих данных для принятия решений.

В разделе о наращивании потенциала подчеркивается важность международного сотрудничества и помощи в области информационно-коммуникационной безопасности и создания потенциала, а также их важности для всех элементов мандата Группы. Активизация сотрудничества наряду с более эффективной помощью и наращиванием потенциала в области информационно-коммуникационной безопасности с участием других заинтересованных сторон, таких как частный сектор, научные круги, гражданское общество и технические круги, могут помочь государствам применять принципы ответственного поведения государств при использовании ими ИКТ. Они имеют решающее значение для преодоления существующих разногласий внутри государств и между ними по политическим, правовым и техническим вопросам, касающимся безопасности ИКТ. Они также могут способствовать достижению других целей международного сообщества, таких как цели в области устойчивого развития.

Группа рекомендовала и далее укреплять международное сотрудничество и помощь в области безопасности ИКТ и создания потенциала для помощи государствам, в том числе в области разработки и осуществление национальных директив, стратегий и программ в сфере ИКТ; создание и укрепление потенциала групп реагирования CERT/CSIRT и укрепление меха-

4 См.: Док. ООН A/76/135 (14 July 2021): Доклад Группы правительственных экспертов по поощрению ответственного поведения государств в киберпространстве в контексте международной безопасности.

низмов сотрудничества между такими группами; повышение безопасности, жизнестойкости и защиты объектов критически важной инфраструктуры; создание или укрепление технического, правового и политического потенциала государств для выявления, расследования и урегулирования инцидентов в сфере ИКТ, в том числе посредством инвестиций в развитие людских ресурсов, институтов, отказоустойчивых технологий и образовательных программ; углубление общего понимания вопросов применимости международного права к использованию ИКТ государствами и содействие обмену мнениями на эту тему между государствами, в том числе в рамках обсуждений в ООН; укрепление технического и правового потенциала всех государств в вопросах расследования и урегулирования серьезных инцидентов в сфере ИКТ и соблюдение согласованных добровольных и необязывающих норм ответственного поведения государств.

Рабочая группа открытого состава информатизации и телекоммуникациям в контексте международной безопасности подготовила 10 марта 2021 г. «Окончательный субстантивный отчет», также содержащий раздел о мерах укрепления доверия[5]. К таковым отнесены меры прозрачности, сотрудничества и стабильности, которые могут способствовать предотвращению конфликтов, недопущению неправильного восприятия и недопонимания, а также снижению напряженности. Они являются конкретным выражением международного сотрудничества. Обладая необходимыми ресурсами, потенциалом и вовлеченностью, меры укрепления доверия могут упрочить общую безопасность, жизнестойкость и мирное использование ИКТ. Меры укрепления доверия могут также способствовать внедрению норм ответственного поведения государств, поскольку они укрепляют доверие и обеспечивают большую ясность, предсказуемость и стабильность в использовании ИКТ государствами. Вместе с другими составляющими основы ответственного поведения государств, меры укрепления доверия могут также способствовать достижению общего понимания между государствами, тем самым способствуя созданию более мирной международной обстановки. В отчете подчеркивается добровольный характер обязательств, устанавливаемых мерами укрепления доверия, что позволит им стать первым шагом к устранению недоверия, возникающего из-за недопонимания между государствами, путем установления связи, наведения мостов и инициирования сотрудничества по достижению общей цели, представляющей взаимный интерес. Отмеченное качество мер укрепления доверия может послужить реализации нормотворческих и правотворческих инициатив в будущем.

Подтверждалось, что сам по себе диалог в рамках Рабочей группы открытого состава является мерой укрепления доверия, поскольку он стимулирует открытый и транспарентный обмен мнениями о восприятии угроз и уязвимостей, ответственном поведении государств и других субъектов и передовой практике, тем самым в конечном итоге поддерживая коллективную разработку и внедрение рамок на ответственное поведение государств при использовании ими ИКТ. Подчеркнута решающая роль ООН в разработке и поддержке внедрения глобальных мер укрепления доверия. Несмотря на то, что в экспертной среде высказываются различные оценки последствий участия региональных организаций в реализации мер по укреплению доверия, были отмечены их значительные усилия по разработке мер укрепления доверия, адаптации их к своим конкретным контекстам и приоритетам, повышению осведомленности и обмену информацией между своими членами. Кроме того, допускалось, что региональные, межрегиональные и межорганизационные обмены могут открыть новые возможности для взаимодействия, кооперации и взаимного обучения.

Отмечено важное значение национальных и региональных механизмов и структур, а также создание адекватных ресурсов и потенциала, таких как национальные группы реагирования на компьютерные чрезвычайные ситуации для обеспечения того, чтобы меры укрепления доверия служили установленной цели. Поддержано мнение, что создание национальных пунктов связи само по себе является мерой укрепления доверия, а также является полезной мерой для внедрения многих других мер укрепления доверия и имеет неоценимое значение во времена кризиса.

5 См.: Док. ООН: A/AC/290/2021/CRP.2.

Отмечено значение наращивания потенциала для развития навыков, людских ресурсов, политики и институтов, которые повышают устойчивость и безопасность государств, с тем чтобы они могли в полной мере пользоваться преимуществами цифровых технологий. Оно играет важную стимулирующую функцию для содействия соблюдению норм международного права и реализации норм ответственного поведения государств, а также для поддержки внедрения мер укрепления доверия. В мире цифровой взаимозависимости выгоды от наращивания потенциала распространяются не только на первоначальных получателей, но и способствуют созданию более безопасной и стабильной среды ИКТ для всех. Обеспечение открытой, безопасной, стабильной, доступной и мирной среды ИКТ требует эффективного сотрудничества между государствами в целях снижения рисков для международного мира и безопасности. Наращивание потенциала является важным аспектом такого сотрудничества и добровольным актом, как донора, так и получателя.

Наращивание потенциала в отношении использования ИКТ государствами в контексте международной безопасности, по мнению авторов отчета, должно основываться на принципах, характеризующих процесс и цель этой деятельности, а также характер складывающихся между участниками отношений и требования к соблюдению прав и свобод человека. Процесс наращивания потенциала должен быть устойчивым, включающим конкретные мероприятия, осуществляемые различными субъектами и для них. Конкретные мероприятия должны иметь четкую цель и быть ориентированы на результат, поддерживая при этом общую цель создания открытой, безопасной, стабильной, доступной и мирной среды ИКТ. К мероприятиям по наращиванию потенциала предъявляется требование основываться на фактических данных, быть политически нейтральными, прозрачными, подотчетными и без каких-либо условий. Подчеркивается, что наращивание потенциала должно осуществляться при полном уважении принципа государственного суверенитета и возможного облегчения доступа к соответствующим технологиям.

Партнерские отношения в этой деятельности должны основываться на взаимном доверии, определяться спросом, соответствовать выявленным на национальном уровне потребностям и приоритетам и осуществляться при полном признании национальной ответственности. Подчеркивается добровольный характер партнерства по наращиванию потенциала и общая, но дифференцированная ответственность, включая сотрудничество в разработке, осуществлении, мониторинге и оценке мероприятий по наращиванию потенциала. Отмечается, что конфиденциальность национальной политики и планов должна быть защищена и соблюдаться всеми партнерами. Особо подчеркивается, что наращивание потенциала должно быть инклюзивным, универсальным и недискриминационным, в процессе наращивания должны соблюдаться права человека и основные свободы, учитываться гендерные аспекты, без уточнения характера и формы закрепления (международно-правовой или национально-правовой) упомянутых прав и свобод. В отчете предусматривается обязательность обеспечения конфиденциальности конфиденциальной информации.

Кроме того, в отчете отмечается, что наращивание потенциала — это взаимное усилие, так называемая «улица с двусторонним движением», на которой участники учатся друг у друга и где все стороны извлекают выгоду из общего улучшения глобальной безопасности ИКТ. Упомянута была ценность сотрудничества Юг-Юг, Юг-Север, а также взаимодействия трехстороннего и регионального характера. Отмечалось, что наращивание потенциала должно способствовать преобразованию цифрового разрыва в цифровые возможности. В частности, этот процесс должен быть направлен на содействие подлинному участию развивающихся стран в соответствующих дискуссиях и форумах и повышение устойчивости развивающихся стран в среде ИКТ.

Таким образом, в рамках ООН на различных площадках (межправительственных и экспертных) сформировались достаточно подробно разработанные модели мер по укреплению доверия в ИКТ-среде и наращивание потенциала в отношении использования ИКТ государствами в контексте международной безопасности, которые по понятным причинам не имеют юридического характера. Они представляют собой политико-экспертные

позиции для возможного последующего развития сформированных предложений в актах мягко-правового регулирования (резолюции, носящие рекомендательный характер) или договорно-правовых документах. Наработанный материал может быть использован в научных исследованиях и определении перспектив становления международных нормативных механизмов.

В 2022 г. Национальная Ассоциация международной информационной безопасности (НАМИБ) организовала проведение Научно-исследовательской работы (НИР) на тему: «Проблема применения норм, правил и принципов ответственного поведения государств в ИКТ-среде». Один из пунктов задания НИР предусматривал анализ мер укрепления доверия в ИКТ-среде и их взаимодействие с добровольными, необязательными нормами ответственного поведения государств. Такая постановка исследовательской задачи была оправдана тем, что в процессе исследования добровольных необязательных норм ответственного поведения государств в ИКТ-среде было необходимо определить их место в международной нормативной системе, обеспечивающей функционирование сотрудничества государств в ИКТ-среде, а также взаимодействие с другими элементами указанной системы.

В ходе исследования была проанализирована история формирования концепции «мер доверия» в международных отношениях, начиная с Заключительного акта СБСЕ 1975 г., а также этапы формирования позиции ООН по вопросу возможности применения мер доверия для укрепления сотрудничества в борьбе с разнообразными угрозами в информационной среде. В частности, были исследованы резолюции Генеральной Ассамблеи ООН «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» 53/70 от 4 января 1999 г., резолюция ГА ООН «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности», резолюция 74/29 от 12 декабря 2019 г. и другие аналогичные документы. Кроме того, предметом исследования стали доклады, содержащие положения о системе мер укрепления доверия и транспарентности в ИКТ-среде, подготовленные в рамках сформированных в институциональной системе ООН особых структур (Группа правительственных экспертов ООН в сфере информационно-коммуникационных технологий, Рабочая группа ООН открытого состава по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности).

Результаты проведенной в 2022 году НИР обобщены в итоговом отчете о выполнении научно-исследовательской работы на тему: «Проблема применения норм, правил и принципов ответственного поведения государств в ИКТ-среде». В этом документе было отмечено достижение поставленных в НИР целей по разработке предложений по подходам к применению добровольных и необязательных норм ответственного поведения государств в ИКТ-среде, которые могут быть использованы представителями НАМИБ и заинтересованных федеральных органов государственной власти в процессе участия в деятельности Рабочей группы ООН открытого состава по вопросам безопасности в сфере использования ИКТ и самих ИКТ 2021–2025 гг.

Кратко результаты выполнения работы НИР по вопросу мер укрепления доверия могут быть сведены к следующему. Меры укрепления доверия являются сравнительно новым институтом международной нормативной системы в целом, в том числе регулирующей сферу применения норм, правил и принципов ответственного поведения государств в ИКТ-среде. Меры укрепления доверия представляют собой политический нормативный механизм регулирования отношений в целях обеспечения достаточной степени уверенности в соблюдении субъектами международного договора запрета применения силы и угрозы силой в международных отношениях.

С международно-правовой точки зрения меры доверия могут носить юридически обязательный характер, если они обусловлены международным договором, который определяет их основные параметры[6]. Меры доверия также могут закрепляться в документах «мягкого права» (резолюциях Генеральной Ассамблеи ООН, имеющих нормативный, но юриди-

6 Соглашение между Российской Федерацией, Республикой Казахстан, Киргизской Республикой, Китайской Народной Республикой и Республикой Таджикистан об укреплении мер доверия в военной области в районе границы, заключено в г. Шанхае, 26 апреля 1996 г., вступило в силу 7 мая 1998 г.//http://www.mid/ru/

чески не обязывающий характер, для примера можно привести резолюцию 43/78 (H), резолюцию ГА ООН «Руководящие принципы для мер по укреплению доверия Комиссии по разоружению ООН 1988 г.», которую ГПЭ в своем докладе рекомендовала государствам принимать во внимание[7]. Наконец, меры доверия могут быть сформулированы в политических документах (Заключительный акт Совещание по безопасности и сотрудничеству в Европе)[8].

Наряду с нормативными международными документами, принятыми в ООН, мерам укрепления доверия в ИКТ-среде в настоящее время начинают уделять внимание и межгосударственные региональные организации, которым, как было указано выше, в документах рабочих групп ООН, придается важное значение для продвижения сотрудничества на многостороннем уровне. Так, Организация по безопасности и сотрудничеству в Европе (ОБСЕ), ранее практиковавшая разработку мер доверия в области обычных вооружений, в 2013 и 2016 годах разработала и приняла наборы мер укрепления доверия в ИКТ-среде (например, Решение Постоянного совета ОБСЕ № 1202 от 10 марта 2016 г. о мерах укрепления доверия в рамках ОБСЕ с целью сокращения рисков возникновения конфликтов в результате использования информационных и коммуникационных технологий)[9].

На евразийском пространстве юридически обязательные договоры приняты в Содружестве Независимых Государств (СНГ), Организации Договора о коллективной безопасности (ОДКБ) и Шанхайской организации сотрудничества (ШОС). Каждая из трех перечисленных международных региональных организаций, опираясь на положения учредительных документов о сотрудничестве в сфере поддержания международной информационной безопасности, заключила соответствующие международные договоры, в которых либо в общей форме, либо с конкретной ссылкой на меры доверия, установлены соответствующие обязательства. Соглашение о сотрудничестве государств-участников СНГ в сфере обеспечения информационной безопасности от 20 ноября 2013 г. в преамбуле подчеркивает, что дальнейшее развитие сотрудничества и взаимодействия в сфере обеспечения информационной безопасности является необходимостью и отвечает интересам всех государств-участников. Там же признается необходимость предотвращения возможности использования ИКТ в целях, которые не совместимы с задачами обеспечения стабильности и безопасности государств-участников СНГ и способны оказать негативное воздействие на целостность инфраструктуры государств, нанося ущерб их безопасности как в гражданской, так и в военной сфере.

Соглашение о сотрудничестве государств-членов Организации Договора о коллективной безопасности в области обеспечения информационной безопасности от 30 ноября 2017 г. рассматривает сотрудничество в области обеспечения информационной безопасности одним из основных направлений деятельности ОДКБ. В нем прямо указывается на «развитие мер укрепления доверия в сфере обеспечения информационной безопасности». Соглашение о сотрудничестве между правительствами государств-членов ШОС в области обеспечения международной информационной безопасности от 16 июня 2009 г. также относит к одному из основных направлений деятельности данной международной организации разработку и осуществление совместных мер доверия, способствующих обеспечению международной информационной безопасности. Надо подчеркнуть, что вопросы обеспечения международной информации безопасности постоянно находятся в поле зрения ШОС. В Нью-Делийской декларации Совета глав государств-членов ШОС от 4 июля 2023 г. подчеркивается ключевая роль ООН в сфере противодействия угрозам в информационном пространстве, создания безопасного, справедливого и открытого информационного пространства, построенного на принципах уважения государственного суверенитета и невмешательства во внутренние дела других стран. Государства-члены выступают категорически против милитаризации сферы информационно-коммуникационных технологий. Они поддерживают выработку универсальных правил, принципов и норм ответственного поведения государств в этой об-

7 См.: UN General Assembly resolution 43/78(H) “GUIDELINES FOR CONFIDENCE-BUILDING MEASURES”//documents-dds-ny.un.org.

8 Хельсинкский заключительный акт СБСЕ 1975 г.// http://www.osce.org/ru/resources/csce-osce-key-documents.

9 Текст документа см.: http://www.osce.org.

ласти и продолжат сотрудничать в рамках профильных переговорных механизмов в ООН и на других международных площадках[10].

Следует отметить, что наряду с международными региональными организациями, появляются новые неформальные межгосударственные объединения, примером чего является Совещание по взаимодействию и мерам доверия в Азии (СВМДА), представляющее собой межправительственный форум с самым широким географическим охватом в азиатском регионе, включающим 28 государств. СВМДА рассматривает обширную повестку дня и является наиболее подходящей платформой для консолидации коллективной мудрости всех азиатских стран в интересах мира, сотрудничества, безопасности и развития и для их полной интеграции в глобальную архитектуру безопасности и многосторонних процессов принятия решений глобального значения. В настоящее время отмечается процесс постепенного, поступательного и основанного на консенсусе преобразования СВМДА в полноценную международную региональную организацию. В 2021 г. СВМДА включил новую приоритетную область «Безопасность и использование информационно-коммуникационных технологий» в обновленный каталог мер укрепления доверия по инициативе России и Китая, а в 2022 г. саммит принял совместное заявление лидеров государств-членов СВМДА, в котором подчеркивается стремление его участников сблизить подходы к обеспечению безопасности ИКТ и развивать сотрудничество на основе Устава ООН и принципов международного права, а также активно участвовать в работе соответствующей Рабочей группы открытого состава ООН и в разработке всеобъемлющей международной конвенции под эгидой ООН[11].

Наконец, кроме многосторонних форм регулирования в дополнение к ним и в конкретизацию положений многосторонних международно-правовых и рекомендательных актов, заключаются двусторонние договоры, регулирующие вопросы международной информационной безопасности. В практике Российской Федерации такого рода соглашения заключались как с дружественными государствами (например, Соглашение между Правительством Российской Федерации и Правительством Китайской Народной Республики о сотрудничестве в области обеспечения международной информационной безопасности от 8 мая 2015 г.), так и с развитыми западными державами (например, Соглашение между Правительством Российской Федерации и Правительством Королевства Испания о сотрудничестве в сфере информатизации от 17 мая 1999 г.). Соглашение между Российской Федерацией и КНР придает важное значение роли информационно-коммуникационных технологий в поддержании международного мира, безопасности и стабильности и подчеркивает необходимость разработки и осуществления необходимых совместных мер доверия, способствующих обеспечению международной информационной безопасности. Оно включает ряд конкретных мероприятий по реализации мер доверия между сторонами, таких, например, как создание каналов связи и контактов в целях совместного реагирования на угрозы в сфере международной информационной безопасности. На этом фоне контрастом выглядит Соглашение между Россией и Королевством Испании, возможно по причине более узкого предмета регулирования — информатизации, вопросы которой относятся в основном к социально-экономическим и технологическим вопросам.

Большое внимание привлекла в свое время договоренность между Россией и США, закрепленная в совместном заявлением президентов обеих сторон о новой области сотрудничества в укреплении доверия от 17 июня 2013 года[12]. В этом документе отмечено общее понимание угроз в сфере использования информационно-коммуникационных технологий: военно-политического, криминального и террористического характера. Было объявлено о заключении трех «прорывных» по своей значимости договоренностей, фор-

10 См.: rus.sectsco.org

11См.: Amb. Kairat Sarybay. Current state of affairs in the Conference on Interaction and confidence Building Measures in Asia// moderndyplomacy.eu.

12 В зарубежных источниках эту договоренность называют «соглашением». См.: Накашима Э. США и Россия пописывают соглашение о создании линии связи по кибербезопасности. Иносми (The Washington Post. США). 18 июня 2013//inosmi.ru; или даже одним из самых известных. См.: Promoting international peace and stability by building trust between states in cyberspace: The importance of effective confidence-building measures CYBERSPACE: THE NEW FRONTIER IN GLOBAL CONFLICT, p.7//https://cybertechaccord.org

мирующих комплексную систему мер доверия между Россией и США в информационном пространстве, что предполагало организацию линий связи и обмена информацией о компьютерных инцидентах на трех уровнях: между представителями, курирующими вопросы национальной безопасности (данный канал задействуется в случае возникновения кризисной ситуации, когда необходим прямой доклад президентам); между силовыми ведомствами стран по линии национальных центров по уменьшению ядерной опасности (НЦУЯО) для уведомлений об атаках на объекты критической информационной инфраструктуры; групп экстренной готовности к компьютерным инцидентам (CERT) в целях мониторинга вредоносной активности в сетях[13].

Содержание документа до настоящего времени может рассматриваться как образец разумного и взвешенного примера регулирования мер укрепления доверия в ИКТ-среде. Тем не менее, перемены в международных отношениях, ухудшение отношений между США и Российской Федерации и в целом враждебная позиция США в отношении России фактически нивелировали достигнутый прогресс, о чем ярко свидетельствует принятая в марте 2023 г. Национальная стратегия кибербезопасности США[14].

Таким образом, можно подытожить, что к настоящему времени сложилась многоуровневая структура международного сотрудничества в сфере международной информационной безопасности в целом, включающая комплекс мер по укреплению доверия в ИКТ-среде и мер по наращиванию потенциала в отношении использования ИКТ государствами в контексте международной безопасности. Отдельные элементы этой структуры представлены международно-правовыми актами, имеющими юридически обязательный характер, другие закреплены резолюциями ГА ООН и актами других (например, региональных) организаций, а также содержатся в документах, имеющих значение систематизированных мнений экспертного сообщества.

Вместе с тем, невзирая на большой массив нормативного материала по исследуемым вопросам, следует признать, что на универсальном уровне проблема реализации системы укрепления мер доверия и мер по наращиванию потенциала в отношении использования ИКТ государствами в контексте международной безопасности остается по прежнему актуальной и требующей своего продвижения на более высокий уровень нормативного или даже международно-правового регулирования. Было бы преждевременно порождать ожидания скорого формирования институциональной или правовой нормативной системы, которая бы обеспечила их обнадеживающее функционирование. В документах рабочих групп, ГПЭ и РГОС правильно указывалось, что разработка мер как мер доверия, так и мер по наращиванию потенциала — это длительный процесс, который, логично предположить, по мере своего развития будет сопровождаться не только достижениями, но и новыми вызовами и сложностями, ввиду высокой степени зависимости от политики государств. Следует согласиться с теми исследователями, которые призывают к дальнейшему поиску решения проблем, возникающих на пути разработки юридически обязательных актов по обеспечению безопасности ИКТ-среды, потому что иной альтернативы просто не существует.

В этом смысле следует поддержать посыл, содержащийся в важнейшем выводе проведенной НИР: создание условий для принятия и соблюдения государствами добровольных обязательств будет возможным при решении задачи применения международного права в отношении добровольных необязательных правил ответственного поведения государств в ИКТ-среде. Наиболее эффективным средством достижения этой задачи видится заключение специального международного договора, который предусмотрит такие обязательства как назначение государствами компетентных координаторов и контактных пунктов на политическом и техническом уровнях, обеспечение диалога и консультаций, а также обмена информацией и накопленным положительным опытом. Как, известно, проект такого договора в результате проведения НИР был подготовлен, следовательно, его продвижение на площадке ООН (в том числе, в деятельности

13 См.: Совместное заявление президентов Российской Федерации и Соединенных Штатов Америки о новой области сотрудничества в укреплении доверия//www.mid.ru

14 См.: The National Cybersecurity Strategy. Marth 2023// https://www.whitehouse.gov › uploads › 2023/03

РГОС) и других международных организаций будет способствовать практической реализации достигнутых научных и нормотворческих усилий по формированию системы укрепления мер доверия и мер по наращиванию потенциала в отношении использования ИКТ государствами в контексте международной безопасности.

П.У. Кузнецов
Доктор юридических наук, профессор, заведующий кафедрой информационного права Уральского государственного юридического университета им. В.Ф. Яковлева

ИМПЛЕМЕНТАЦИЯ НОРМ МЕЖДУНАРОДНОГО ПРАВА В РОССИЙСКОМ ПРАВОВОМ ПРОСТРАНСТВЕ

Вначале хотелось бы привести высказанное на Санкт-Петербургском международном юридическом форуме в мае 2019 г. мнение авторитетного юриста, Председателя Конституционного Суда Российской Федерации В.Д. Зорькина о состоянии современной англосаксонской правовой системы, являющейся сегодня пока еще центром притяжения международного права: «В нынешней глобализованной, информационно перенасыщенной и глубочайшим образом взаимосвязанной реальности фактически сделана заявка на полное отрицание тех правовых принципов жизни человечества, которые мы привыкли считать столь же неотъемлемым условием нашего существования, как воздух, которым дышим. Современный кризис права, углубляющийся на наших глазах, имеет свои корни в тех вариантах философствования, которые предъявляет постмодерн (отрицание правовых ценностей — П.У.). В философии постмодерна нет места таким базовым правовым понятиям, как истинность, объективность, справедливость»[1].

И все же, несмотря на сложившуюся неопределенность в области развития права в современную эпоху и правового обеспечения безопасности общемирового киберпространства в частности, многие традиции классического международного права в настоящее время имеют место в практике укрепления мира и сотрудничества между странами в информационной сфере.

Одной из таких традиций является процесс имплементации норм и принципов международного права в российском правовом пространстве. Отметим, что названный процесс в настоящее время складывается противоречиво и неоднозначно. Его актуальность в контексте правового обеспечения международной информационной безопасности (МИБ) частично подчеркнута в известной коллективной монографии экспертов НАМИБ «Международная безопасность в среде информационно-коммуникативных технологий», посвященной проблемам применения норм ответственного поведения государств в ИКТ-среде[2].

Известно, что имплементация (англ. *implementation*) как процесс реализации норм и принципов международного права в национальное (внутригосударственное) правовое пространство возможен в следующих четырех формах:

1) **соблюдение** — пассивная форма реализации норм и принципов международного права. При этом субъект права не совершает никаких активных действий, т.к. соблюдение права предполагает всего лишь *ненарушение* правовых норм (например, соблюдение правил дорожного движения);
2) **исполнение** — активная форма реализации норм и принципов международного права, когда предполагается

1 Зорькин В.Д. Право метамодерна: постановка проблемы / Выступление на международном юридическом форуме. Санк-Петербург. 16 мая 2019 // Сайт Конституционного Суда РФ — 7 декабря 2020.

2 Международная безопасность в среде информационно-коммуникативных технологий / под ред. А.А.Стрельцова, А.Я.Капустина, Т.А.Поляковой, А.С.Маркова, Б.Н.Мирошникова. Коллективная монография. М. НАМИБ. 2023.С.37-63.

реализация *юридических обязанностей*. Исполнение осуществляется в интересах того субъекта, который наделен соответствующим правомочием (субъективным правом). Исполнение осуществляется субъектом сознательно и добровольно согласно его волеизъявлению (например, передача товара или денег по договору купли-продажи и пр.);

3) **использование** — активная форма реализации норм и принципов международного права, которая предполагает воплощение субъектами права своих правомочий, предоставленных им правовыми нормами. Использование права зависит от воли субъекта (обладателя права), оно является его добровольным актом и осуществляется по его желанию (например, свободный поиск информации, обращение в суд с исковым заявлением и пр.);

4) **применение** — активная форма реализации права, которую принято называть особой формой реализации права, т.к. она осуществляется исключительно специальным субъектом — уполномоченным органом публичной власти или должностным лицом. Право реализуется в форме применения только в тех случаях, когда реализация права в других формах не достигла своего результата, т.е. когда не произошло воплощения в реальной жизни законных субъективных прав и юридических обязанностей (на международном уровне применение, как форма имплементации, характерно для деятельности органов юрисдикции ООН)[3].

В литературе по международному праву описаны и другие формы взаимодействия национальной правовой системы и международного права, а также реализации его норм и принципов в российском законодательстве[4].

На протяжении многих лет и даже десятилетий в практике международного права складывались традиции имплементации. Тридцать лет назад в п.4 ст.15 Конституции Российской Федерации был закреплено фундаментальное основание для реализации норм и принципов международного права в отечественной правовой системе: «Общепризнанные принципы и нормы международного права и международные договоры Российской Федерации являются составной частью ее правовой системы. Если международным договором Российской Федерации установлены иные правила, чем предусмотренные законом, то применяются правила международного договора».

В рамках данной статьи нет необходимости подробно комментировать основные характеристики приведенной конституционной нормы, в т.ч. таких терминов, как общепризнанные принципы и нормы международного права, толкование которых в научной литературе дается с разных позиций.

В тексте названной нормы речь идет не просто о реализации отдельных принципов и норм международного права, а о том, что они включены в национальную правовую систему как ее неотъемлемая часть.

Более того, в названной норме зафиксирован приоритет принципов и норм международного права по отношению к национальным правовым принципам и нормам действующего законодательства, т.е. позитивному праву. И не только. Названный приоритет распространяется и на правоприменительную практику и даже на отечественную правовую политику, правопонимание, правосознание законодателя и правовую ментальность в целом.

Заметим, что российская правовая система представляет собой структурно-сложное социальное образование, состоящее не только из нормативного массива и практики его применения, но и правосознания (научного, общественного, индивидуального). Поэтому международное право на уровне его норм и принципов в соответствии с Конституцией Российской Федерации становится составной частью всех названных трех элементов правовой системы.

---

3 Международное право. Учебник для вузов. Ответственные редакторы — проф. Г. В. Игнатенко и проф. О. И. Тиунов. М.: Издательская группа НОРМА–ИНФРА • М, 1999. С. 109–113.

4 Международное право: учебник / Б.М. Ашавский, М.М. Бирюков, В.Д. Бордунов и др.; отв. ред. С.А. Егоров. М.: Статут. 2015; Лукашук И.И. Международное право. Общая часть: учеб. для студентов юрид. фак. и вузов / Изд. 3-е, перераб. и доп. — М.: Волтерс Клувер, 2005. С.139-140; Зимненко Б.Л. Международное право и правовая система Российской Федерации. Общая часть: Курс лекций. М.: Статут, РАП, 2010; Белянская О.В., Пугина О.А. Условия имплементации международно-правовых норм в российское законодательство. // Право и политика. 2005. № 8 и др.

Наука и практика международного права последних десятилетий складывались в соответствии с этим фундаментальным подходом. На его основе были реализованы многие интересы граждан и международных организаций в ущерб национальным интересам. Возникла ситуация противоречия между реализацией отдельных норм и принципов международного права с практикой реализации правовых ценностей (прежде всего идей государственного суверенитета и справедливости как главных правовых ценностей), в связи с чем был нарушен баланс интересов личности, общества и государства в правовом пространстве. Особенно это проявилось в практике Европейского суда по правам человека последних лет — органа наднациональной судебной юрисдикции, который пользовался положением п.4 ст. 15 Конституции Российской Федерации и по факту грубо нарушал правовой суверенитет Российской Федерации. По своей сути этот наднациональный судебный орган в своих решениях формулировал новые правовые ценности и идеи в вопросах, которые затрагивают чувствительные струны национальной идентичности отдельных государств[5].

Одним словом, практика использования, исполнения и применения норм и принципов международного права вошла в противоречие с фундаментальным конституционным основанием процесса имплементации.

Поэтому в ходе конституционной реформы в Конституцию Российской Федерации была внесена норма в ст.79 о том, что «решения международных организаций, принятые на основании положений международных договоров РФ в их истолковании, противоречащих Конституции Российской Федерации, не подлежат исполнению в Российской Федерации».

Названная конституционная поправка существенно изменила безусловно «открытый» характер суверенной национальной правовой системы и скорректировала ее прямую зависимость от норм и принципов международного права.

Отметим, что в настоящее время на наших глазах происходит трансформация международных правовых режимов и ломка традиций классического международного права, заметен в этой сфере явный переход с языка принципов и норм на язык так называемых «правил», которые никем и никогда официально не принимались и которые «пишутся» избирательно только для тех государств, которые не входят в состав коллективного Запада и Североатлантический Альянс. По сути такие официально никем не установленные правила нацелены на установление управляемого хаоса в международных отношениях. Глава Министерства иностранных дел Российской Федерации С.В. Лавров в этом контексте красноречиво заметил: «В целях политико-идеологического прикрытия своей неоколониальной, расистской линии, закрепления собственной гегемонии западные столицы упорно стремятся заменить международное право, которое они ежечасно нарушают, «порядком, основанным на правилах»[6].

Угроза подмены норм и принципов международного права особенно опасна в условиях невозможности применения современных правовых средств регулирования киберпространства. Коллективный Запад сознательно тормозит и активно препятствует принятию проекта Конвенции об обеспечении МИБ. Его ведущие представители «используют современные информационные технологии для достижения собственных геополитических целей, навязывания своей гегемонии, распространения дезинформации, установления цензуры СМИ, манипулирования информацией, использования информационного пространства для подогревания напряжения и разжигания конфликтов»[7].

В этих условиях необходимо более активно использовать потенциал региональных международных организаций (БРИКС, ШОС и др.), в которых наметился реальный консенсус и взаимное понимание наиболее острых проблем современности. Расширяющееся партнерство в рамках названных организа-

5 Зорькин В.Д. Конституционный контроль в контексте современного правового развития // Доклад на Международной конференции «Конституция в эпоху глобальных перемен и задачи конституционного контроля» (СПб, 15 мая 2018 года). Сайт Конституционного Суда Российской Федерации. Обращение 20 сентября 2023 г.

6 Лавров С.В. Выступление на XI Московской конференции по международной безопасности, Москва, 15 августа 2023 года // Официальный сайт НАМИБ. Обращение 20 сентября 2023 г.

7 Крутских А.В. Сборник докладов участников XVI Международного форума «Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационного безопасности» (19–21 сентября 2022 г.). М. 2022.

ций вполне может стать методологическим инструментом не только для разработки и принятия новых механизмов принятия общепринятых принципов и норм международного права. Прежде всего — принципов ответственного поведения в сфере ИКТ.

В целях придания большей устойчивости общепризнанных принципов международного права, установленных Уставом ООН, было бы целесообразно в рамках названных региональных организаций на основе общепринятых фундаментальных руководящих положений разработать принципы ответственного поведения государств в информационной сфере. Причем такие принципы необходимо разработать в качестве самостоятельного акта (международного договора) в расширенной форме имплементации и толкования таких принципов с тем, чтобы государства могли добровольно выбрать и принять на себя обязывающие нормы ответственного поведения.

И еще. Одним из камней преткновения в современной международной практике мирного сосуществования в киберпространстве являются разные правопонимания его терминологии.

В этой связи предлагается разработать два уровня основополагающих и общепринятых понятий международной практики в информационной сфере.

Первый уровень (высший) должен представлять категориальный аппарат (наиболее обобщенные термины и понятия) в общеупотребительном контексте вне зависимости от географического их употребления.

Второй уровень терминологии может быть представлен в форме тезауруса (расширенного словаря) наиболее употребляемых слов и терминов на национальном уровне. Это позволит учесть культурно-цивилизационное многообразие стран, которые могут присоединиться к названному соглашению.

Оформить и предложить к принятию государствами возможно в виде отдельного международного договора с возможностью присоединения всеми странами.

Разработка и принятие общепризнанных принципов и терминов в качестве международных договоров позволит значительно приблизиться к установлению истинного международно-правового режима МИБ и его архитектуры, а также наиболее адекватной их реализации на национальном уровне.

Кроме того, такие промежуточные акты международного права могут быть моделью разработки других источников правового обеспечения глобальной безопасности и придания ей большей устойчивости.

Т.А. Полякова
Главный научный сотрудник, и.о. заведующего сектором информационного права и международной информационной безопасности Института государства и права РАН, доктор юридических наук, профессор, Заслуженный юрист Российской Федерации

ПРИОРИТЕТЫ НАЦИОНАЛЬНОЙ ПРАВОВОЙ ПОЛИТИКИ В СФЕРЕ ФОРМИРОВАНИЯ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В рамках своего выступления полагаю целесообразным коснуться вопросов национальной правовой политики Российской Федерации, направленной на формирование международной информационной безопасности. Полагаю, что тема международной информационной безопасности в глобальной ИКТ-среде в условиях формирования многополярного мира напрямую связана и с правовой тематикой, проблемами правового характера, этому должны быть посвящены многие выступления, касающиеся развития системы.

Значение формирования системы международной информационной безопасности приобретает в современных условиях изменения миропорядка, перехода к многополярности, обострения геополитической обстановки в мире, а также и в информационном пространстве, не только возрастает, но становится одной из ключевых тем государственной национальной политики Российской Федерации и во всем мире, привлекает к себе все большее внимание. В связи с этим особенно хочется отметить возрастающую актуальность и выразить признательность организаторам Национальной Ассоциации международной информационной безопасности за выбор площадки и организацию такого масштабного мероприятия, каким является XVII Международный Форум «Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности». Представляется неслучайным и выбор темы в этом году, поскольку предложенные к обсуждению вопросы связаны с международной безопасностью в глобальной ИКТ-среде в условиях формирования многополярного мира. Такой грандиозный форум, проходящий уже в 17 раз и состоявшийся, несмотря на различные санкции, сложности и ограничения возможностей очного взаимодействия, привлек пристальное внимание руководителей и представителей многих международных организаций, включая РГОС ООН. Кроме того, программа данного форума свидетельствует не только о его достаточно высоком международном уровне, но и глубоко междисциплинарном подходе по своей сути и содержанию. Это подтверждается, на наш взгляд, не только широким составом участников, но и 6 круглыми столами с весьма насыщенной и разнообразной программой, отражающей различные блоки вопросов, связанных с проблемами международной информационной безопасности. При этом обращает внимание, значительное количество участников. Несомненный интерес вызывают подходы как российских, так и зарубежных участников, представляющих различные организации. Такой яркий, высокопрофессиональный состав безусловно является отличительной особенностью данного Форума.

Правовое обеспечение международной информационной безопасности, это составляющая государственной политики. Глобальный характер большинства информационных угроз обуславливает потребность развития международного сотрудничества в сфере международной информационной безопасности. Российская Федерация является после-

довательным сторонником консолидации усилий государств по обеспечению МИБ, продвижению правовых инициатив в этой области, которые являются важной составляющей российской политики в рассматриваемой сфере более четверти века.

С одной стороны, политика выражается в продвижении российских инициатив, но также требует взвешенных подходов и к развитию национального законодательства с учетом национальных интересов в области информационной безопасности, на основе научного обоснования, осмысления вопросов, связанных с формированием международно-правового режима регулирования сферы использования ИКТ.

Представляя Институт государства и права Российской академии наук, и как юрист, специализирующийся в области информационного права и международной информационной безопасности, полагаю важным отметить, что это одна из приоритетных тем, сложность которой измеряется сочетанием международного и национального права. Это стало особенно очевидно в связи с участием в составе российских экспертов в научно-исследовательской работе по изучению проблем применения норм ответственного поведения государств в ИКТ-среде. Подготовленные по результатам исследований реферат и монография включают и правовые вопросы, в том числе о состоянии национального правового регулирования, определенных пробелов. Думаю, что сегодня необходимо сконцентрировать внимание и на приоритетах национальной правовой политики, направленной на формирование системы МИБ.

Одним из приоритетов российской государственной политики в рассматриваемой сфере в правовом и организационном плане является, несомненно, продвижение проекта универсальной конвенции по МИБ, о которой довольно подробно сообщалось и в рамках пленарного заседания и во многих выступлениях. Это, несомненно, важный проект, за судьбой которого на площадке ООН необходимо не только наблюдать, но и активно продвигать, убеждать, обосновывая свои позиции.

Особая роль в Основах государственной политики в области МИБ отводится развитию механизмов ее правового обеспечения, включая:

- содействие принятию странами-участницами ООН Конвенции об обеспечении международной информационной безопасности;
- содействие выработке новых принципов и норм международного права, регламентирующих поведение государств в глобальном информационном пространстве;
- заключение и реализация международно-правовых и иных договоренностей между Россией и иностранными государствами о сотрудничестве в сфере МИБ.

В качестве приоритета также необходимо рассматривать противодействие правовыми средствами в рамках информационного противоборства деструктивному информационно-психологическому воздействию на индивидуальное и общественное сознание, объекты критической информационной инфраструктуры.

Безусловным правовым приоритетом российской государственной политики является правовое обеспечение государственного суверенитета, цифрового и технологического суверенитета Российской Федерации.

Приоритетным направлением российской государственной политики является противодействие правонарушениям и развитие системы борьбы с преступлениями в информационной сфере, доля которых в общей структуре преступности уже составляет более четверти. При этом сегодня наиболее массовыми видами киберпреступлений в России являются мошенничества и кражи денежных средств со счетов граждан и организаций. С целью противодействия информационной преступности с 2021 года в рамках Специального комитета ООН ведется деятельность по подготовке всеобъемлющей международной конвенции в данной области — проект Конвенции ООН о противодействии использованию информационно-коммуникационных технологий в преступных целях A/AC.291/22.

Одним из ключевых приоритетов является формирование унифицированных правовых подходов к пониманию международной информационной безопасности в документах стратегического планирования.

Развитие понятия международной информационной безопасности, на наш взгляд, за-

служивает особого внимания. Так, в Основах государственной политики Российской Федерации в области международной информационной безопасности под международной информационной безопасностью понимается «такое состояние глобального информационного пространства, при котором на основе общепризнанных принципов и норм международного права и на условиях равноправного партнерства обеспечивается поддержание международного мира, безопасности и стабильности» (п. 6).

Как отмечают эксперты, «предложенный и продвигаемый Российской Федерацией термин МИБ подразумевает наличие не только технических, но и политико-идеологических угроз в данной области», в отличие от западной концепции кибербезопасности, где в основном обращено внимание на технологическое измерение информационных угроз. В России в основополагающих документах стратегического планирования в области национальной безопасности информационная безопасность рассматривается комплексно, как состояние защищенности от широкого круга информационных угроз, включая угрозы технического и психологического характера. Такой подход характерен для Стратегии национальной безопасности Российской Федерации 2021 года.

В качестве основной цели государственной политики Российской Федерации в области МИБ определено «содействие установлению международно-правового режима, при котором создаются условия для предотвращения (урегулирования) межгосударственных конфликтов в глобальном информационном пространстве, а также для формирования с учетом национальных интересов Российской Федерации системы обеспечения международной информационной безопасности» (п. 9 Основ государственной политики в области МИБ)[1]. Для достижения указанной цели необходимо развитие всестороннего международного сотрудничества на глобальном, региональном, многостороннем и двустороннем уровнях, связанного с формированием системы обеспечения МИБ. В целях развития системы политико-правового обеспечения МИБ в указанном документе предусмотрено участие Республики Беларусь в международных организациях, профильных международных договорах, двусторонних отношениях с иными государствами, в других формах межгосударственного сотрудничества, поддержка и продвижение соответствующих инициатив, отвечающих национальным интересам Республики Беларусь в информационной сфере. Российскую Федерацию и Республику Беларусь объединяет общность подходов в рассматриваемой сфере. В Концепции информационной безопасности Союзного государства, утвержденной постановлением Высшего Государственного Совета Союзного государства от 22 февраля 2023 г. № 1, подчеркнута нацеленность государств-участников на развитие равноправного стратегического партнерства в области обеспечения международной информационной безопасности[2].

Содействие принятию государствами-членами ООН Конвенции об обеспечении международной информационной безопасности по-прежнему остается одной из приоритетных задач государственной политики России. В Концепции внешней политики Российской Федерации отмечается стремление узкой группы государств подменить международно-правовую систему концепцией «миропорядка, основанного на правилах» (навязывание правил, стандартов и норм, при выработке которых не было обеспечено равноправное участие всех заинтересованных государств). Это «в значительной мере осложняет выработку коллективных ответов на транснациональные вызовы и угрозы, включая использование информационно-коммуникационных технологий в противоправных целях»[3].

Бесспорно, потребует дальнейших исследований вопрос о поведении государств в ИКТ-среде, касающийся добровольных и необязательных норм ответственного поведения государств в ИКТ-среде. Эта тема продолжает обсуждаться в целях сближения различных позиций в отношении норм, закре-

1 Указ Президента Российской Федерации от 12 апреля 2021 г. № 213 «Об утверждении Основ государственной политики Российской Федерации в области международной информационной безопасности» // СЗ РФ. 2021. № 16. Ст. 2746.

2 Концепция информационной безопасности Союзного государства (утв. постановлением Высшего Государственного Совета Союзного государства от 22 февраля 2023 г. № 1). Официально не опубликована.

3 Концепция внешней политики России (утв. Указом Президента РФ от 31 марта 2023 г. № 229). П. 9.

пленных в докладах ГПЭ А/70/174 от 22 июля 2015 г.[4] (далее — Доклад ГПЭ 2015) и А/76/135 от 14 июля 2021 г.[5] (далее — Доклад ГПЭ 2021) и рекомендованных для рассмотрения государствами-участниками Генеральной Ассамблеей ООН на 75-й сессии. По сути, в условиях отсутствия юридически обязательных соглашений, указанные нормы стали неким промежуточным вариантом «мягкого регулирования», нацеленного на закрепление необходимых международных правил обеспечения безопасности ИКТ-среды.

Приоритетом государственной политики является развитие международно-правового регулирования международной информационной безопасности в региональных форматах.

В этой связи на современном этапе очевидна целесообразность усиления региональных и двусторонних направлений международного сотрудничества. В Концепции внешней политики Российской Федерации в числе задач внешней политики указаны «развитие взаимовыгодного и равноправного сотрудничества с конструктивно настроенными иностранными государствами и их объединениями, раскрытие и укрепление потенциала многосторонних региональных объединений и интеграционных структур с участием России» (п. 17). К таким объединениям относятся: БРИКС, ШОС, СНГ, ЕАЭС, ОДКБ, РИК (Россия, Индия, Китай) (п. 19). Это тоже задача национальной правовой политики.

Учитывая проведение специальной военной операции на Украине и усиление противостояния с Западом, важно отметить следующие направления сотрудничества России и Республики Беларусь в сфере информационной безопасности:

- выработка и реализация согласованных мер информационного противодействия идеологической агрессии коллективного Запада;
- обеспечение координации деятельности ключевых государственных информационных агентств России и Беларуси и реализация совместных информационных проектов;
- сближение организационно-правовых механизмов ограничения доступа к противоправной информации в сети «Интернет»;
- усиление координации деятельности компетентных органов по линии выявления и реагирования на компьютерные атаки;
- взаимное продвижение на рынок государств-участников Союзного государства программно-аппаратных средств отечественного производства;
- обмен опытом проведения мероприятий по повышению медиаграмотности и культуры информационной безопасности граждан государств-участников Союзного государства.

Таким образом, для объединения усилий государств по обеспечению информационной безопасности в современных условиях необходима разработка и реализация национальной политики государства на основе анализа развития его законодательства для синхронизации и сплочения усилий на международной арене с целью развития системы обеспечения МИБ.

4 Доклад Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности А/70/174 от 22 июля 2015 г.

5 Доклад Группы правительственных экспертов по поощрению ответственного поведения государств в киберпространстве в контексте международной безопасности А/76/135 от 14 июля 2021 г.

С.В. Коротков
Генерал-майор (в отставке), кандидат военных наук, начальник экспертного отдела Национальной Ассоциации международной информационной безопасности

О ПРОБЛЕМАТИКЕ СОБЛЮДЕНИЯ НОРМ ОТВЕТСТВЕННОГО ПОВЕДЕНИЯ ГОСУДАРСТВ ПРИ ИСПОЛЬЗОВАНИИ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ В КОНТЕКСТЕ ОБЕСПЕЧЕНИЯ МЕЖДУНАРОДНОЙ БЕЗОПАСНОСТИ

Из позиции России на 78-й сессии Генеральной Ассамблеи ООН: «Выступаем за сохранение центральной роли ООН…в глобальном переговорном процессе по международной информационной безопасности (МИБ). Важно не допустить учреждения навязываемых западными странами непрозрачных и подконтрольных им механизмов. Отстаивать строго межгосударственный характер принятия универсальных решений по МИБ.

Приоритетным направлением деятельности должно стать придание правилам, нормам и принципам ответственного поведения в информационном пространстве юридически обязательной силы»[1].

Оценка факторов, влияющих на формирование системы обеспечения международной информационной безопасности

В настоящее время предпринимаемые усилия по продвижению в ООН «западными» и некоторыми другими государствами инициативы по подготовке «Программы действий по поощрению ответственного поведения государств в сфере использования информационно-коммуникационных технологий в контексте международной безопасности» имеют объемное военно-политическое и гуманитарное измерение.

По замыслу авторов Программы действий и активно поддерживающих ее «стран Запада», данный формат институционального диалога по вопросам безопасности в сфере использования ИКТ должен прийти на смену созданной по инициативе России Рабочей группы ООН открытого состава по безопасности в сфере использования ИКТ и самих ИКТ 2021–2025 (РГОС) после завершения действия ее мандата в 2025 году.

Объективно, несмотря на значительную поддержку данной инициативы в рамках принятия на 77-й сессии ГА ООН резолюции A/RES/77/37 («За» проголосовали 156 стран), по своей сути она является одним из элементов реализации концепции доминирования Запада, что не предполагает соблюдения каких-либо обязательных норм.

Важно отметить, что это происходит в обстановке, когда серьезное давление оказывается на ООН и другие многосторонние институты, предназначение которых в качестве площадок для согласования интересов ведущих держав, искусственно обесценивается. Испытанию на прочность подвергается международно-правовая система: узкая группа государств стремится подменить ее концепцией «миропорядка, основанного на правилах» (навязывание правил, стандартов и норм, при выработке которых не было обеспечено равноправное участие всех заинтересованных государств). Осложняется выработка коллективных ответов на транснациональные вызовы и угрозы, в том числе на угрозы использования информационно-коммуникационных технологий в противоправных целях.

1 https://mid.ru/ru/foreign_policy/un/1900137/?

Повышается роль фактора силы в международных отношениях, в ряде стратегически важных регионов расширяется конфликтное пространство[2].

Показательным примером является «гибридная война» нового типа на Украине, которую поддерживают «западные» государства. В рамках этой «войны» осуществляются акты злонамеренного и вредоносного использования ИКТ, ведется агрессивная пропаганда в форме дезинформационных информационных кампаний, которые еще ни разу не стали предметом обсуждения Совета Безопасности ООН. Причем более половины из 50 стран т.н. «коалиции Рамштайн»[3] имеют непосредственное отношение к злонамеренной и вредоносной деятельности против России.

К числу факторов, характеризующих обстановку в области международной информационной безопасности, следует отнести также следующие:

- отсутствие перспективы заключения соглашений о предотвращении милитаризации киберсферы (ИКТ-сферы) и космического пространства;
- неопределенность перспектив решения проблемы запрета не только на вывод оружия в космос, но и на разработку, испытания и развертывание противоспутникового оружия в воздухе, на земле и на море;
- криминализация глобальной ИКТ-сферы, ее взаимосвязь с террористическими, экстремистскими и неонацистскими организациями;
- неопределенность принципов НАТО использования военной силы в соответствии со ст.5 Вашингтонского договора в контексте ответных действий на кибератаки;
- возрастание геополитической конфронтации и турбулентности в киберсфере;
- отсутствие кризисного урегулирования конфликтных ситуаций в ИКТ-среде между крупнейшими субъектами международного права;
- интенсивное развитие систем управления на основе внедрения новых ИКТ и искусственного интеллекта;
- участие негосударственных «кибербойцов» (хакеров) в кибератаках.

Дальнейшие попытки реализации «западными» государствами концепции «миропорядка, основанного на правилах», чревато разрушением международно-правовой системы и другими опасными последствиями для человечества.

Актуальные проблемы формирования системы международной информационной безопасности и возможности их обсуждения в рамках Программы действий.

Наиболее отработанным на уровне ООН направлением продвижения положений обновленной концепции Конвенции ООН о международной информационной безопасности является обсуждение вопросов применения норм ответственного поведения государств в ИКТ-среде.

Результаты анализа показывают, что к числу наиболее актуальных проблем придания нормам ответственного поведения государств в ИКТ-среде относятся:

- закрепление границ зон ответственности государств в ИКТ-среде;
- разрешение международных спорных ситуаций, связанных с инцидентами в ИКТ-среде;
- имплементация норм ответственного поведения государств в ИКТ-среде в национальное законодательство.

Как показал проведенный анализ, несмотря на то, что основные положения предлагаемого мандата Программы действий, как международной площадки обсуждения проблем применения норм ответственного поведения государств в ИКТ-среде, во многом повторяют мандат Рабочей группы ООН открытого состава, но имеют и существенные отличия.

В частности, предполагается, что участниками реализации Программы действий будут приняты консенсусом итоговые документы, носящие рекомендательный характер. Так, предусматривается создание глобального межправительственного **реестра контактных пунктов**, запуск **глобального портала по сотрудничеству**, воплощение идеи **ведения реестра угроз**.

2 Концепция внешней политики Российской Федерации от 31 марта 2023 г.

3 https://www.m24.ru/news/politika/29032023/563458

В этих условиях можно с уверенностью прогнозировать, что итоговые **документы Программы действий будут использоваться «западными» странами в русле продвигаемой США концепции** «порядка, основанного на правилах» — для навязывания выгодных им «правил» толкования норм ответственного поведения государств в ИКТ-среде.

Реализация таких итоговых документов Программы действий приведет к установлению «красных линий», разделяющих мировое сообщество на государства с «ответственным» («коллективный Запад») и «безответственным» поведением в информационном пространстве («авторитарные режимы» и не примкнувшие к «цивилизованному миру» развивающиеся страны — т.н «государства не-Запада»).

В перспективе можно ожидать, что на площадке РГОС ключевой темой станет дискуссия относительно формата регулярного институционального диалога по вопросам безопасности в сфере использования ИКТ и самих ИКТ. Страны Запада продолжат продвигать в этих целях Программу действий, Россия и ее единомышленники — продление мандата РГОС.

В связи с изложенным усилия российской дипломатии должны быть сосредоточены на разъяснении не только недостатков Программы действий, но, прежде всего, на ее применимости только в увязке с принятием Конвенции ООН об обеспечении международной информационной безопасности или другого аналогичного по содержанию международно-правового договора об обеспечении мира в глобальном информационном пространстве.

А.С. Марков
Доктор технических наук, президент ГК «Эшелон»

ПРОБЛЕМНЫЕ ВОПРОСЫ МЕЖДУНАРОДНО-ПРАВОВОГО РЕЖИМА РЕГУЛИРОВАНИЯ БЕЗОПАСНОСТИ ПРОГРАММНЫХ РЕСУРСОВ С ОТКРЫТЫМ КОДОМ

Актуальность

27 сентября мир отметил 40 лет парадигме открытого программного обеспечения (ОПО, free open source software, FOSS). Сегодня как никогда актуально оценить важность данной парадигмы для каждого государства и международных взаимоотношений. Например, как ОПО влияет на мир и безопасность, какие международные риски есть при использовании ОПО, настало ли время международного регулирования безопасности ОПО.

Нормы, правила и принципы ответственного поведения государств

Отметим Нормы, правила и принципы ответственного поведения государств в части безопасного использования программного обеспечения, а именно [1–6]:

1. Норма i): государства должны принимать разумные меры для обеспечения целостности каналов поставки, чтобы конечные пользователи могли быть уверены в безопасности продуктов ИКТ. Государства должны стремиться предупреждать распространение злонамеренных программных и технических средств в сфере ИКТ и использование скрытых вредоносных функций.
2. Норма j): государства должны способствовать ответственному представлению информации и факторах уязвимости в сфере ИКТ и делиться соответствующей информацией о существующих методах борьбы с такими факторами уязвимости, чтобы ограничить, а по возможности и устранить возможные угрозы для ИКТ и зависящей от ИКТ инфраструктуры.

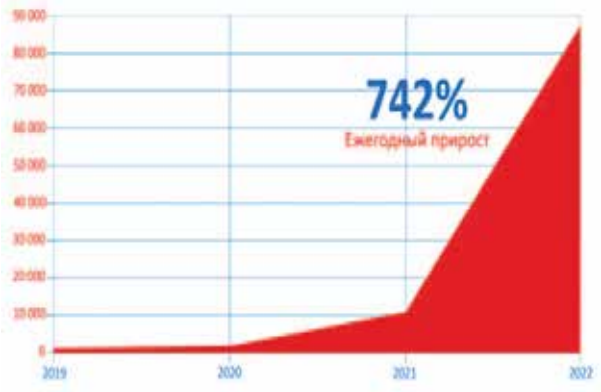
Анализ проблематики безопасности ОПО в контексте указанных Норм позволяет сделать следующие выводы:

1. Именно ОПО создает проблему безопасности цепей поставки;

2. Именно ОПО является главным источником уязвимостей ПО КИИ.

К примеру, можно привести статистику:

- 6/7 уязвимостей в ОПО связаны с зависимостями от компонентов ОПО (то есть от поставщиков библиотек, сред разработки и пр.);
- последние несколько лет наблюдается экспоненциальный рост собственно зависимостей от других компонентов ПО (компонентов третьих сторон);
- 70–97% современных программных средств представляет ОПО;
- в прошлом году зафиксировано, что каждая 5-я уязвимость имеет преднамеренный характер;
- наблюдается взрывной рост уязвимостей в ОПО с 2019 г. (рис. 1).



Источник: Sonatype

Рис. 1. Рост уязвимостей в открытом программном обеспечении

Определение открытого программного обеспечения в контексте международной информационной безопасности

Современные стандарты определяют ОПО как программное обеспечение с доступным для использования исходным кодом в соответствии с некоторой «свободной» лицензией. Следует отметить технический фактор информационной безопасности, а именно наличие исходного кода, что создает основу для доверия (в случае инцидента и при сертификации исходный код можно проанализировать на предмет закладок, недекларированных возможностей и пр.).

На взгляд автора, указанное выше определение не позволяет полно охарактеризовать ОПО с точки зрения международной информационной безопасности по причине отсутствия упоминания зрелости комьюнити, создающего и поддерживающего ОПО. Указанное комьюнити может характеризоваться разным уровнем поддержки процедур безопасности, этики свободного программного обеспечения, аффилированности от государств. Таким образом можно сделать замечание, что уровень комьюнити определяет и уровень международной программной безопасности.

На рис. 2 представлено разделение комьюнити по используемым национальным языкам. Очевидно, что русскоязычное комьюнити позволяет нашей стране оставаться в пятерке лидеров.

Источник: www.jetbrains.com

Рис. 2. Ведущие комьюнити открытого программного обеспечения

Парадигма ОПО 2.0

В [7] сделан вывод, что в 2021–2023 гг. в мире произошло изменение парадигмы ОПО. В качестве подтверждения можно отметить следующее:

1. Наблюдается абсолютная зависимость современных информационных технологий от ОПО;
2. Инициировано государственное регулирование ОПО со стороны ряда стран;
3. Налицо кризис доверия к безопасности ОПО в части устойчивости и безопасности.

Так, согласно данным НПО «Эшелон», в период 2019–2022 гг. в рамках проверки 860 проектов 97% программных средств защиты информации и 74% специального ПО имели в своем составе компоненты ОПО, а 2/3 программного кода современных защищенных операционных систем уже состоят из компонентов ОПО [7].

Наиболее наглядным процесс государственного регулирования виден на примере США. В таблице 1 приведены ряд законодательных и нормативно-правовых актов США за 2021–2022 гг. Наиболее примечателен законопроект Securing Open Source Software Act, предполагающий внесение ОПО в структуру КИИ США.

Что касается кризиса ОПО, то целесообразно отметить ряд следующих моментов (рис. 3):

- современное ОПО, несмотря на усилия программистов, имеет значительное количество уязвимых компонентов,
- ряд уязвимостей из-за особенностей ОПО имеют чрезвычайные и масштабные последствия;
- наблюдается взрывной рост атак, направленных на открытый исходный код в публичных репозиториях и атак на цепочку поставок.

Следует указать на прецеденты нарушения этики ОПО, например, использование протестного ПО и блокировку учетных записей против России. Риторика западных стран не выдерживает критику, к примеру, наличие ОПО в России и Китае — угроза национальной кибербезопасности США [8]. Можно привести совсем уже дикие истории, например, блокировка сайта российского научного журнала «Вопросы кибербезопасности» — cyberrus.com.

Таблица 1.

Год	Название
	Указы президента США
2021	Executive Order on Improving the Nation's Cybersecurity, EO 14028.
	Концептуальные документы
2022	Moving the U.S. Government Toward Zero Trust Cybersecurity Principles. *Executive Office of The President. OMB.*
	Федеральные законы
2021	DHS Software Supply Chain Risk Management Act
2022	Securing Open Source Act
2021	Supply Chain Security Training Act
	НПА органов исполнительной власти
2022	Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure. SEC
2022	Enhancing the Security of the Software Supply Chain through Secure Software Development Practices. *OMB*
2021	SBOM Proof of Concept. V.2.0. *NTIA*
2022	Securing the Software Supply Chain: Recommended Practices Guide for Developers. *NSA, CISA, ODNI*
	Нормативные документы и специальные публикации
2022	Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations. NIST SP 800-161r1. *NIST*
2021	Defending Against Software Supply Chain Attacks. *NIST, CISA*
2021	Guidelines on Minimum Standards for Developer Verification of Software. NISTIR 8397. *NIST*
2022	Secure Software Development Framework. V.1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities. NIST SP 800-218. *NIST*
2022	Software Supply Chain Security Guidance Under Executive Order (EO) 14028. *NIST*
2021	Software Supply Chain Security Guidance. *NIST*

Рис. 3. Распределение ошибок в ОПО

Выводы

Проведенный анализ новой парадигмы ОПО 2.0 позволил сделать ряд выводов, например:

ОПО — это объективная реальность, очевиден рост зависимости ИТ-технологий (ИИ — не исключение) многих стан от ОПО. ОПО рассматривается некоторыми странами как новый потенциальный сегмент КИИ, а также объект госрегулирования (несмотря на «свободную» декларацию).

ОПО претендует и на новую виртуальную сферу взаимодействия мирового сообщества (США, Китай, Индия, Россия и др.). Соответственно, ОПО ставит новые вызовы, угрозы и нарративы в ИКТ-сфере.

С одной стороны, ОПО представляет потенциальную платформу к доверию между странами (по причине наличия исходного кода).

С другой стороны, с применением ОПО и технологические риски растут (и масштабность последствий) и киберриски растут (как и непрогнозируемость необъявленных кибервойн).

Можно предположить, перспективность международного регулирования безопасности ОПО в целях стратегической стабильности.

Литература

1. Международная информационная безопасность: теория и практика / Крутских А.В., Бирюков А.В., Бойко С.М., Волкова С.Г., Зиновьева Е.С., Зинченко А.В., Матюхин Д.В., Смирнов А.И. Учебник для вузов: в 3-х томах / Под общ. ред. А.В. Крутских. — М.: МГИМО, 2021. — Том 1 (2-е изд., доп.) — 384 с.
2. Международная безопасность в среде информационно-коммуникационных технологий. Коллективная монография по проблеме применения норм ответственного поведения государств в ИКТ-среде / Стрельцов А.А. и др.; Предисловие В.П.Шерстюка; под ред. А.А.Стрельцова и др. М.: НАМИБ, 2023, 132 с.

3. Применение норм ответственного поведения государств в ИКТ-среде и международное сотрудничество / Стрельцов А.А. и др.; Предисловие В.Шерстюк — М.: НАМИБ, 2022. — 32 с.
4. Проблемные вопросы повышения достоверности идентификации ресурсов критически важной инфраструктуры / Марков А.С. — В сборнике: Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности. Сборник докладов участников XVI международного форума. — М.: Национальная Ассоциация международной информационной безопасности. 2022. С. 86–91.
5. Ромашкина Н.П., Марков А.С., Стефанович Д.В. Международная безопасность, стратегическая стабильность и информационные технологии / отв. ред. А.В. Загорский, Н.П. Ромашкина. — М.: ИМЭМО РАН, 2020. С. 98.
6. Romashkina N.P., Markov A.S., Stefanovich D.V. Information Technologies and International Security. — Moscow : IMEMO, 2023. — 111 p.
7. Марков А.С. Важная веха в безопасности открытого программного обеспечения. // Вопросы кибербезопасности. 2023, № 1(53), с. 2–12.
8. Aitel D. and etc. Russian Open Source Code. In: Russia's Cyber Operations: A Threat to American National Security. Margin Research, 2022, pp. 83–96.

Н.П. Ромашкина
Кандидат политических наук,
Руководитель подразделения проблем информационной безопасности (ЦМБ) ИМЭМО РАН

ПРИМЕНЕНИЕ НОРМ И ПРИНЦИПОВ МЕЖДУНАРОДНОГО ПРАВА В ИКТ-СРЕДЕ КОСМИЧЕСКОГО ПРОСТРАНСТВА

Современный этап характеризуется новыми важными особенностями, которые максимально обострились в период Специальной военной операции России и являются обоснованием необходимости дополнительных действий в сфере норм и принципов международного права.

1. Первой из таких важных характеристик является повсеместное лавинообразное распространение и существенный рост числа искусственных спутников Земли (ИСЗ)[1]. Причем такое ускоренное распространение ИСЗ, которое представлено на рисунке 1, произошло не столько за 40 лет XX века, а именно в первые десятилетия XI века.

Это говорит о возрастании роли и значимости ИСЗ на современном этапе военно-политических международных отношений. Количественные и качественные характеристики спутниковой группировки являются одним из показателей престижа государства в мире, его влияния и потенциала. Кроме того, растет роль ИСЗ в глобальном информационном пространстве, позволяющем стране обеспечивать безопасное взаимодействие с другими государствами и организациями, а также удовлетворять свои потребности при сохранении баланса национальных и международных интересов[2].

Отмечу, что задача создания глобального единого информационного пространства, включающего в себя космический эшелон, приобретает новое звучание в период кризиса. Это обосновано тем, что инфраструктура сбора, изучения и обработки больших массивов данных, в которой уникальную роль играют ИСЗ, во время конфликтов и военных действий жизненно важна для обеспечения военных операций, экономического анализа и прогнозирования, а также процесса принятия решений.

Учитывая, что цифровая трансформация все больше проникает в космос, можно констатировать, что космический уровень уже сегодня выглядит как быстрореагирующая ИКТ-сеть с масштабными перспективами дальнейшего развития.

Обладая уникальными возможностями получения, хранения и передачи информации, спутники с программно-определяемыми полезными нагрузками и функциями становятся все более гибкими и адаптивными. При этом новые технологии стирают традиционные границы между космическими и наземными сетями, спутниковая наземная инфраструктура адаптируется, переходя от аппаратно-ориентированных архитектур к программно-управляемым системам.

2. Второй важнейшей характеристикой текущего этапа стала существенная диспро-

1 Искусственный спутник Земли (ИСЗ) — космический летательный аппарат (КА), совершающий свободный полёт по геоцентрическим орбитам вокруг Земли (не менее одного оборота) и выводит на орбиту ракетой-носителем. В соответствии с международной договоренностью космический аппарат называется спутником, если он совершил не менее одного оборота вокруг Земли. При несоблюдении этого условия он считается ракетным зондом, проводившим измерения вдоль баллистической траектории, и не регистрируется как спутник. Источник: Искусственные спутники Земли. Сайт Министерство Обороны Российской Федерации. // https://encyclopedia.mil.ru/encyclopedia/dictionary/details.htm?id=5270@morfDictionary.

2 Ромашкина Н.П. Космос как часть глобального информационного пространства в период военных действий. // Вопросы кибербезопасности. 2022. № 6(52). С. 100–111, DOI:10.21681/2311-3456-2022-6-100-111.

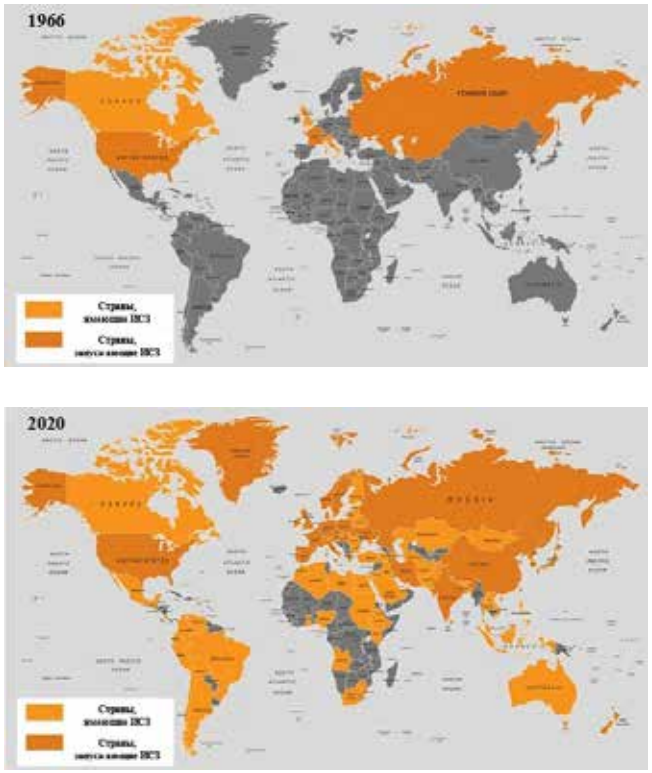


Рисунок 1. Увеличение количества стран, обладающих ИСЗ, с 1966 г по 2020 г[3].

порция в обладании странами искусственными спутниками Земли.

Так, за период с 2008 по 2020 гг. глобальная спутниковая индустрия почти удвоилась и достигла $271 млрд. Только за первое полугодие 2023 г. на орбиты было выведено более 700 ИСЗ.

При этом по данным от 1 января 2023 г. на различных орбитах находится 6718 ИСЗ, среди которых 4529 ИСЗ, т.е. 67%, принадлежит США (было 63% в середине 2022 г.), КНР принадлежит 590 ИСЗ, т.е. около 9% (было 10% в середине 2022 г.), России — 174 ИСЗ, т.е. менее 3%, и 1425, т.е. 21% — всем другим странам (см. рисунок 2). Хочу обратить внимание, что в число этих «других стран» входит большое количество государств — союзников и партнеров США. В июне 2022 г. Подкомитет по стратегическим силам Палаты представителей Конгресса США принял решение о расширении применения частных спутников для ведения разведки, в том числе на Украине, для предоставления этой информации Вооруженным Силам Украины (ВСУ). В проект оборонного бюджета США на 2023 финансовый год были внесены соответствующие поправки[4].

На рисунке 2 также представлено функциональное разделение общего количества спутников США по классификации Соединенных Штатов: 26 гражданских ИСЗ, 3996 коммерческих, 260 правительственных и 247 военных ИСЗ[5]. Обратите внимание, что именно в число коммерческих ИСЗ, которые составляют более 88%, входит масштабная группировка *Starlink* американской компании *SpaceX*, которая сегодня активно используется ВСУ. Сейчас эта группировка ИСЗ насчитывает более 4 тысяч единиц, а планируется разместить на орбите 12 тысяч космических аппаратов[6]. Несколько тысяч терминалов *Starlink*, установленных на территории Украины, позволяют ВСУ управлять беспилотниками, получать разведданные, поддерживать связь и т.д.

3. Сегодня ИСЗ решают все больше задач, в зависимости от которых их подразделяют на научно-исследовательские и прикладные. Неуклонный рост значимости прикладных спутников, используемых в военных целях, стал еще одной тенденцией последних лет.

Наиболее важную роль в период военных действий играют спутники связи, навигационные, дистанционного зондирования Земли (ДЗЗ), а также спутники системы предупреждения о ракетном нападении (СПРН) (см. рисунок 3).

Во время конфликта, во время военных операций ИСЗ служат для обеспечения боевых действий вооруженных сил и боевого применения различных средств вооруженной борьбы:

- наблюдение за наземными, воздушными и космическими объектами, выявление угроз на земле, в космосе и из космоса;
- стратегическая и оперативная космическая разведка с целью получения сведений о противнике, выявление новых целей;

3 UCS Satellite Database. Union of Concerned Scientists (UCS). // https://www.ucsusa.org/resources/satellite-database.

4 H.R. 7900—FY23 NATIONAL DEFENSE AUTHORIZATION BILL SUBCOMMITTEE ON STRATEGIC FORCES. https://armedservices.house.gov/_cache/files/6/6/669844f3-0199-4016-a154-16301f07b96e/45DB9E09D47A3B155E8441C76D8630D3.fy23-ndaa-strategic-forces-subcommittee-mark.pdf.

5 UCS Satellite Database. Union of Concerned Scientists (UCS). // https://www.ucsusa.org/resources/satellite-database.

6 «Законная цель для удара». Какие страны умеют сбивать спутники. 31.10.2022. // https://rtvi.com/stories/zakonnaya-czel-dlya-udara-kakie-strany-umeyut-sbivat-sputniki/.

Рисунок 2. ИСЗ на орбитах Земли[7].

Рисунок 3. Задачи ИСЗ двойного и военного назначения[9].

- обеспечение лиц, принимающих решения, достоверной информацией (в том числе фотоснимками отдельных территорий для получения документальной информации) об активности противника на этапе глубокой подготовки к боевым действиям, о перемещении войск и вооружений, о раннем обнаружении пусков баллистических ракет;
- определение местоположения радиолокационных станций (РЛС);
- предупреждение о ракетном нападении;
- контроль результатов ракетно-ядерных ударов;
- навигационное обеспечение боевого применения подводных лодок, надводных кораблей, самолетов, подвижных ракетных комплексов и других подвижных систем вооружения;
- геодезическое и метеорологическое обеспечение боевых действий войск, круглосуточная и непрерывная передача данных о текущих и прогнозируемых погодных и климатических условиях;
- обеспечение оперативного управления войсками с помощью космической связи, а также управление оружием с космических командных пунктов;
- проведение профилактических и ремонтных работ в космосе;
- ведение боевых действий в космосе и из космоса (по терминологии западных стран, «ведение космической войны»)[8].

При этом быстродействие современных систем обработки и передачи данных, полученных со спутников, позволяет в кратчайшие сроки выявить цель, опознать и создать условия для ее уничтожения.

Ключевую роль для выполнения военных и разведывательных целей играет дистанционное зондирование (ДЗ), лидерами в разработке и использовании которых являются США. Так, одна из составляющих группировки спутников ДЗЗ — программа «Система наблюдения Земли» (*Earth Observing System, EOS*) Национального управления по аэронавтике и исследованию космического пространства США (*National Aeronautics and Space Administration, NASA*), которая исторически напрямую связана с МО США, состоит из значительной группировки скоординированных полярно-орбитальных спутников. EOS призвана выполнять научно-исследовательские и прикладные функции, а данные, получаемые со спутников, активно используются и в военных операциях. Анализ группировки NASA дает представление о масштабных возможностях действующих и перспективных ИСЗ США, которые активно используются в военно-политических целях.

США являются лидерами и в разработке спутников связи, являющихся важнейшим элементом информационно-телекоммуникационной инфраструктуры МО и ВС по управлению группировками войск (сил) в глобальном масштабе, который постоянно совершенствуется

7 Рисунок построен автором на основе: UCS Satellite Database. Union of Concerned Scientists (UCS). // https://www.ucsusa.org/resources/satellite-database.

8 Искусственные спутники земли (ИСЗ) // https://encyclopedia.mil.ru/encyclopedia/dictionary/details.htm?id=13199@morfDictionary Ромашкина Н. П., Стефанович Д.В. Стратегические риски и проблемы кибербезопасности // Вопросы кибербезопасности. 2020. №. 5(39). С. 77–86, DOI: 10.21681/2311–3456-2020-05-77-86.

9 Рисунок построен автором.

в целях повышения пропускной способности, безопасности и защищенности. Ресурсы всех ИСЗ связи между пользователями распределяет Комитет начальников штабов США.

В период военных действий ключевые задачи возлагаются на рекогносцировочные или разведывательные спутники (неофициально — спутники-шпионы) — ИСЗ (спутники связи, навигации, ДЗЗ и другие виды), запускаемые для предоставления разведывательной информации о военной деятельности иностранных государств, развернутые для военных и/или разведывательных целей[10].

В сфере военного использования космоса США смогли добиться технологического превосходства над многими странами мира и в своих доктринальных документах декларируют цель сохранения доминирования и гегемонии в космическом пространстве, что создает глобальные угрозы. Кроме того, США, их союзники и партнеры проводят интеграцию спутниковых систем в единую информационно-телекоммуникационную сеть — основу применения разведывательно-ударных систем и высокоточного оружия в будущих войнах, основанных на комплексном использовании космических средств разведки, связи, боевого управления, навигации, метеообеспечения и др.

4. Еще одна опасная тенденция текущего этапа: открытая демонстрация со стороны стран НАТО использования их спутниковой группировки в военных действиях на Украине в пользу ВСУ. Это напрямую связано с важной для России проблемы неправомерного использования ИСЗ в период военных действий, когда космические информационные технологии — спутники стран НАТО и их партнёров — применяются во враждебных военно-политических целях. Речь идет о передаче со спутников, в том числе, военного назначения, разведывательной информации формально нейтральными государствами для поддержки военных действий одной из сторон военного конфликта для уничтожения военнослужащих и военной техники другой стороны. Использование дронов, которые стали одними из значимых средств ведения текущих военных действий и управляются с использованием информации с навигационных спутников НАТО, также добавляет проблем России.

При этом США и страны НАТО открыто заявляют на самых разных уровнях[11], включая президента США, что они обеспечивают армию Украины разведывательной информацией, в частности снимками высокого разрешения со своих ИСЗ. Это данные о расположении военных объектов, военной техники и военных подразделений российской армии в любую погоду и любое время суток.

МО Российской Федерации и МИД Российской Федерации подтверждают эту информацию. Так, по заявлениям Министра обороны Российской Федерации С.К. Шойгу, «Работает практически вся натовская спутниковая группировка. По нашим оценкам, больше 70 военных и свыше 200 гражданских спутников работают на то, чтобы разведывать месторасположение наших подразделений»[12].

В связи с этим возникает множество вопросов, в частности:

Какие юридические обоснования подобных действий существуют в международном праве?

Можно ли это рассматривать как участие в военных действиях, следовательно, в качестве военного вмешательства?

Можно ли это расценивать как применение силы или угрозу применения силы в соответствии с Уставом ООН?

Таким образом, неправомерное использование ИСЗ в период военных действий наряду с другими вызовами ставит целый ряд глобальных проблем:

1. превращение космического пространства в сферу военно-политических действий в нарушение существующего международного права;

10 Определение дано автором на основе источников: Reconnaissance satellite. // https://infogalactic.com/info/Reconnaissance_satellite. Reconnaissance satellite. // https://www.infoplease.com/encyclopedia/science/space/exploration/reconnaissance-satellite.

11 Напр., см: Постпред США при ООН подтвердила передачу разведданных Украине. 8 мая 2022. // https://www.rbc.ru/rbcfreenews/627803429a7947335ec5768c

12 А. Комолов. Шойгу: почти вся спутниковая группировка НАТО работает против российской армии. 21.09.2022. // https://rg.ru/2022/09/21/shojgu-pochti-vsia-sputnikovaia-gruppirovka-nato-rabotaet-protiv-rossijskoj-armii.html. Выступление заместителя руководителя российской делегации К.В. Воронцова в ходе тематической дискуссии по разделу «Космос (разоруженческие аспекты)» в Первом комитете 77-й сессии ГА ООН. 26 октября 2022. // https://russiaun.ru/ru/news/261022_v.

2. рост вероятности киберугроз в отношении ИСЗ, в том числе военного назначения, самой опасной среди которых является кибервмешательство в работу ИСЗ СПРН, что повышает риск ошибочного запуска баллистических ракет;

3. разработка систем вооружений для применения силы или угрозы силой в космосе, из космоса или в отношении космоса;

4. повышение угрозы гонки космических и противоспутниковых вооружений, в том числе кибероружия;

5. рост вероятности сокращения так называемой лестницы эскалации конфликта в случае массированного вредоносного применения киберсредств на одной или нескольких ступенях лестницы, следовательно, снижение уровня и кризисной, и стратегической стабильности, что может привести к таким тяжёлым последствиям, которые не выгодны ни одной стране в мире.

Западные эксперты заявляют, что «все, что не запрещено — разрешено». Следовательно, международная нормативно-правовая база в космической сфере на данном этапе не отвечает угрозам, связанным с теми характеристиками современной системы, которые я обозначила, и не содержит никаких ограничений на деструктивную деятельность с использованием космического пространства.

Учитывая, что такая ситуация несет угрозы милитаризации космоса, снижения уровня стратегической стабильности логично инициировать международную деятельность для изменения ситуации[13]. Для повышения стабильности в глобальном информационном пространстве, в том числе на космическом уровне, с целью минимизации угроз для России, а также снижению вероятности эскалации конфликта целесообразно:

- введение проблематики использования спутников как важнейшей части глобального информационного пространства в международные обсуждения по МИБ;
- совершенствование механизмов обеспечения информационной безопасности критически важных объектов государственной инфраструктуры, в том числе космических, от которых зависит обороноспособность страны;
- расширение количественного и качественного потенциала формирований ВС Российской Федерации, обеспечивающих информационную безопасность;
- расширение количественного и качественного потенциала спутниковой группировки Российской Федерации;
- создание условий для отражения нападения противника с применением космических аппаратов, недопущения завоевания превосходства в стратегической космической зоне, комплекс мероприятий в околоземном космическом пространстве и на территории России;
- расширение сотрудничества и взаимодействия в рамках ОДКБ и ШОС по обеспечению кибербезопасности, в частности в сфере применения норм и принципов международного права в ИКТ-среде космического пространства[14].

Более подробно об этих и других проблемах информационной безопасности вы можете прочитать в публикациях нашего подразделения проблем информационной безопасности ЦМБ ИМЭМО РАН. Вот одна из последних наших монографий[15].

Спасибо за внимание!

13 Ромашкина Н.П. Международно-правовой режим контроля над кибероружием в будущем миропорядке: угрозы и перспективы // Дипломатическая служба. 2023. № 2. С. 150-161. DOI 10.33920/vne-01-2302-07.

14 Ромашкина Н.П., Марков А.С., Стефанович Д.В. Международная безопасность, стратегическая стабильность и информационные технологии / отв. ред. А.В. Загорский, Н.П. Ромашкина. — М.: ИМЭМО РАН, 2020. — 98 с. DOI: 10.20542/978-5-9535-0581-9.

15 Ромашкина Н.П., Марков А.С., Стефанович Д.В. Information Technologies and International Security : [electronic resource]. — Moscow : IMEMO, 2023. — 111 p. — ISBN 978-5-9535-0613-7. — DOI 10.20542/978-5-9535-0613-7. — URL: https://www.imemo.ru/publications/info/information-technologies-and-international-security.

А.К. Жарова
Доктор юридических наук, старший научный сотрудник сектора уголовного права, уголовного процесса и криминологии Института государства и права Российской академии наук

ПРАВОВОЕ ОБЕСПЕЧЕНИЕ АТРИБУЦИИ КОМПЬЮТЕРНЫХ АТАК

Использование информационных и коммуникационных технологий (ИКТ) для злонамеренной деятельности в отношении информационной инфраструктуры других государств нарушает принципы международного права, в частности, принцип невмешательства во внутренние и внешние дела других государств.

Международное право, в том числе установленное в Уставе Организации Объединенных Наций, подтверждает суверенитет каждого государства и принцип невмешательства в его внутренние дела. Этот принцип является фундаментальным в международных отношениях, и обязывает государства воздерживаться от действий, которые могут нарушить суверенитет другого государства. В ИКТ-сфере нарушение суверенитета реализуется посредством компьютерных атак[1] и других форм киберагрессии.

Многие международные документы запрещают использование ИКТ в целях кибервмешательства во внутренние дела государства, в том числе в целях кибершпионажа против других государств. Принципы ответственного поведения государства в киберпространстве являются одним из примеров таких международных стандартов. Международное сотрудничество и согласованные действия государств важны для поддержания мира и стабильности в киберпространстве.

Однако одной из ключевых сложностей регулирования отношений в ИТК-среде является отсутствие территориальных границ в киберпространстве, что делает традиционные методы мирного разрешения споров менее эффективными.

Для проведения компьютерных атак может использоваться инфраструктура разных государств, что создает сложности в определении источника компьютерной атаки[2], а также ответственного лица за эти действия.

Для решения данных проблем мировое сообщество разрабатывает международные нормы, регулирующие поведение государств в киберпространстве. Например, Рабочая группа открытого состава по обеспечению международной информационной безопасности работает над созданием рекомендаций. Такое сотрудничество должно обеспечивать обмен информацией о киберугрозах и совместные усилия по расследованию инцидентов. В то же время в пока отсутствуют универсальные международные договоры, регулирующие отношения между государствами в области использования ИКТ. Определенные надежды на принятие первого такого документа возникают в связи с работой Специального комитета ООН по разработке всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях.

Принятие и ратификация международных договоров в области борьбы с преступ-

1 Жарова А.К. Обеспечение защиты государства от компьютерных атак в ИКТ-сфере / А.К. Жарова // Труды Института государства и права Российской академии наук. — 2022. — Т. 17, № 4. — С. 100–125. — DOI 10.35427/2073-4522-2022-17-4-zharova. — EDN ZDFJDA.

2 Методический документ. Методика оценки угроз безопасности информации (утв. ФСТЭК России 05.02.2021) (Документ опубликован не был) // СПС «КонсультантПлюс».

ностью в ИКТ-сфере играют важную роль в установлении прав и обязанностей государств для сотрудничества в предупреждении, пресечении и расследовании вредоносных деяний в ИКТ. Например, Конвенция Совета Европы о преступности в сфере компьютерной информации и Конвенция Лиги арабских государств о борьбе с преступлениями в сфере информационных технологий служат хорошими иллюстрациями таких договоров.

Конвенция о преступности в сфере компьютерной информации 2001 г., разработана Советом Европы, представляет собой многосторонний договор, который направлен на борьбу с киберпреступностью. Она устанавливает нормы для уголовной ответственности в случае совершения киберпреступлений, а также включает меры по сотрудничеству между государствами в расследовании и пресечении таких деяний. Эта конвенция также открыта для участия странам, которые не являются членами Совета Европы.

Конвенция Лиги арабских государств о борьбе с преступлениями в сфере информационных технологий принята Лигой арабских государств, также охватывает борьбу с киберпреступностью, и устанавливает нормы и принципы борьбы с преступлениями в области ИКТ. Она способствует укреплению сотрудничества между арабскими государствами в этой области.

Подобные международные соглашения помогают государствам разрабатывать общие стандарты для борьбы с киберпреступностью, обеспечивать совместное расследование компьютерных атак и обмен информацией о киберугрозах, а также усиливают сотрудничество в вопросах кибербезопасности, в целях снижения риска проведения компьютерных атак и повышения международной кибербезопасности.

Особенно такое сотрудничество важно в связи с тем, что ИКТ-сфера создает взаимную зависимость государств от ошибок, уязвимостей, программных закладок, которые возможны в информационных технологиях[3], поэтому невозможно создать абсолютную технологическую защиту в ИКТ-сфере. Не существует такой технологии, которая была бы абсолютно устойчива к внешним атакам. Существующие уязвимости информационных технологий могут быть использованы злоумышленниками для атак и нарушений безопасности[4]. Принимая во внимание, что основой ИКТ-сферы являются интернет-технологии и ее невозможно разделить на территории, принадлежащие государствам, проблема определения источника компьютерной атаки и его атрибуция требует от государства поиска новых подходов к ее решению[5].

С одной стороны, главной силой обеспечения безопасности должны выступать суверенные государства, а не отдельные индивиды,

3 Жарова А.К. Технологии фильтрации контента в целях предотвращения преступлений, совершенных с использованием интернета / А.К. Жарова // Российский судья. — 2023. — № 6. — С. 49-54. — DOI 10.18572/1812-3791-2023-6-49-54. — EDN EYFTZJ.

4 Жарова А.К. Уголовно-правовая охрана частной жизни человека через призму обеспечения безопасности биометрических персональных данных / А.К. Жарова // Право и информация: вопросы теории и практики : сборник материалов XII международной научно-практической конференции, Санкт-Петербург, 11 ноября 2022 года / Президентская библиотека имени Б.Н. Ельцина. — Санкт-Петербург: Президентская библиотека имени Б.Н. Ельцина, 2023. — С. 37–43. — EDN MFVHCF.

5 Федеральный закон от 1 июля 2021 г. № 236-ФЗ «О деятельности иностранных лиц в информационно-телекоммуникационной сети «Интернет» на территории Российской Федерации»// СЗ РФ 2021. № 27 (Ч. I). Ст. 5064.

но в ИКТ-сфере ситуация складывается иным образом. Технологическая составляющая ИКТ-сферы позволяет физическим и юридическим лицам оказывать существенное влияние на ИКТ-отношения. Мы знаем достаточно примеров влияния ИТ-гигантов на регулирование интернет-отношений. Хакеры (как отдельные лица), так и организованное их сообщество также могут нанести существенный вред и осуществить компьютерную атаку на ИКТ[6].

Определение источника компьютерной атаки — одна из самых сложных и важных задач в обеспечении кибербезопасности. Киберпреступники активно используют различные методы для сокрытия своей личности и местоположения, делая их выявление и преследование сложными задачами для правоохранительных органов и специалистов по кибербезопасности.

Инструментами в борьбе с этой проблемой являются, например, лог-файлы, а также мониторинг сетевой активности и анализ данных, которые позволяют анализировать сетевой трафик и выявлять необычное поведение и, тем самым, предупреждать о возможных атаках. Эти инструменты могут быть улучшены использованием искусственного интеллекта, который может помочь справиться с анализом неструктурированных и больших объемов данных, что, в свою очередь, позволит выявить сетевые аномальные активности, которые могли бы остаться незамеченными человеком.

Еще одним инструментом является сетевая сегментация. Разделение сети на отдельные сегменты с ограниченным доступом может помочь предотвратить распространение атаки внутри системы.

Для межгосударственного взаимодействия требуется наладить сотрудничество и информационный обмен. Правительства, компании и организации должны активно сотрудничать и обмениваться информацией о киберугрозах и компьютерных атаках, поскольку время реагирования на инциденты и постоянное обновление знаний и методов защиты являются неотъемлемыми частями стратегии обеспечения кибербезопасности[7].

Для обеспечения информационной безопасности государства видят один путь — это создание условий подчинения своему закону всех лиц, которые разрабатывают и используют информационные технологии на его территории.

Таким образом, одним из методов обеспечения информационной безопасности и принуждения к выполнению требований национального законодательства является привяз-

6 Международная безопасность в среде информационно-коммуникационных технологий: Коллективная монография по проблеме применения норм ответственного поведения государств в ИКТ-среде / А. А. Стрельцов, А. Я. Капустин [и др.] ; Национальная Ассоциация международной информационной безопасности. — Москва : НАМИБ, 2023. — 132 с. — EDN FBKNHG.

7 Правовое регулирование сети Интернет в Республике Беларусь URL: https://kgatk.by/elektronnie-obrazovatelnie-resyrsi/dostup-k-eor/pravovoe-regulirovanie-seti-internet-v-rb/ (дата обращения 09.03.2022).

ка информационных технологий к территории своего государства.

Поскольку невозможно снизить уровень взаимосвязанности современных обществ, лучшим вариантом является усовершенствование механизмов сдерживания и способов защиты. Государствам необходимо разработать и согласовать перечень требований и технического описания информации, полученной от других государств в случае произошедшей компьютерной атаки.

Анализ обеспечения информационной безопасности должен включать оценку рисков безопасности информационных технологий (ИТ) и соответствия требований безопасности ИТ, связанных с функциональными границами информационной системы, которые должна иметь информационная система в ИКТ-сфере.

Этих данных должно быть достаточно для того, чтобы соответствующие органы государственной власти могли определить территорию, с которой произошла компьютерная атака.

Государствам также необходимо обсуждать вопросы о применимости системы норм и принципов в целях обеспечения информационной безопасности, а также выявления ответственных лиц в связи с произошедшими компьютерными атаками и киберинцидентами.

Список литературы

1. Методический документ. Методика оценки угроз безопасности информации (утв. ФСТЭК России 05.02.2021) (Документ опубликован не был) // СПС «КонсультантПлюс».
2. Жарова А.К. О соотношении персональных данных с ip-адресом. российский и зарубежный опыт // Вестник УрФО. Безопасность в информационной сфере. 2016. № 1 (19). С. 61–67.
3. Федеральный закон от 1 июля 2021 г. № 236-ФЗ «О деятельности иностранных лиц в информационно-телекоммуникационной сети «Интернет» на территории Российской Федерации»// СЗ РФ 2021. № 27 (Ч. I). Ст. 5064.
4. Правовое регулирование сети Интернет в Республике Беларусь URL: https://kgatk.by/elektronnie-obrazovatelnie-resyrsi/dostup-k-eor/pravovoe-regulirovanie-seti-internet-v-rb/ (дата обращения 09.10.2023).
5. Жарова А.К. Технологии фильтрации контента в целях предотвращения преступлений, совершенных с использованием интернета / А. К. Жарова // Российский судья. — 2023. — № 6. — С. 49–54. — DOI 10.18572/1812-3791-2023-6-49-54. — EDN EYFTZJ.
6. Жарова А.К. Уголовно-правовая охрана частной жизни человека через призму обеспечения безопасности биометрических персональных данных / А.К. Жарова // Право и информация: вопросы теории и практики: сборник материалов XII международной научно-практической конференции, Санкт-Петербург, 11 ноября 2022 года

/ Президентская библиотека имени Б.Н. Ельцина. — Санкт-Петербург: Президентская библиотека имени Б.Н. Ельцина, 2023. — С. 37–43. — EDN MFVHCF.
7. Международная безопасность в среде информационно-коммуникационных технологий: Коллективная монография по проблеме применения норм ответственного поведения государств в ИКТ-среде / А.А. Стрельцов, А.Я. Капустин [и др.] ; Национальная Ассоциация международной информационной безопасности. — Москва: НАМИБ, 2023. — 132 с. — EDN FBKNHG.
8. Жарова А.К. Обеспечение защиты государства от компьютерных атак в ИКТ-сфере / А.К. Жарова // Труды Института государства и права Российской академии наук. — 2022. — Т. 17, № 4. — С. 100–125. — DOI 10.35427/2073-4522-2022-17-4-zharova. — EDN ZDFJDA.

А.А. Морозов
Кандидат юридических наук, Докторант кафедры компьютерного права и информационной безопасности ФШГА МГУ им. М.В. Ломоносова

ОСОБЕННОСТИ ПРИМЕНЕНИЯ НОРМ МЕЖДУНАРОДНОГО ПРАВА К СФЕРЕ ИСПОЛЬЗОВАНИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И ПРОСТРАНСТВА В КОНТЕКСТЕ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

12 апреля 2021 года Президент России утвердил Основы государственной политики Российской Федерации в области международной информационной безопасности.

В соответствии с ними система обеспечения международной информационной безопасности представляет собой совокупность международных и национальных институтов, регулирующих деятельность в глобальном информационном пространстве в целях предотвращения (либо минимизации) угроз МИБ.

Высокая скорость развития сферы информационно-коммуникационных технологий (далее — ИКТ) ставит перед государствами вопрос о правовом регулировании данной области, в том числе в контексте международного сотрудничества.

Основной особенностью ИКТ является то, что такие технологии могут иметь двойное назначение, и данная проблема пока что не имеет правового решения. То есть, одно и тоже устройство может быть запрограммировано как для выполнения своих прямых функций, так и для оказания вредоносного воздействия. Любая компьютерная система, таким образом, может стать инструментом нанесения вреда информационной инфраструктуре. Этим пользуются злоумышленники, в число которых входят и хакерские группировки, работающие в интересах государств.

Таким образом, пользуясь особенным характером ИКТ, можно осуществлять вредоносное воздействие «под чужим флагом». Эта тактика, использующаяся и в обычном пространстве, в информационном пространстве становится основной. Это происходит по ряду причин, из которых можно выделить следующие.

1. В области обеспечения международной информационной безопасности одним из источников угроз является проблема трансграничного характера ИКТ.

Ряд указанных технологий позволяют вести деятельность, включая противоправную, на территории одних государств посредством информационной инфраструктуры других государств, при этом являясь гражданином третьей страны.

2. Другой пример. Технологии облачных вычислений способствуют трансграничному использованию остальных ИКТ. Стратегия развития информационного общества в Российской Федерации на 2017–2030 годы определяет облачные вычисления как информационно-технологическую модель обеспечения повсеместного и удобного доступа с использованием сети «Интернет» к общему набору конфигурируемых вычислительных ресурсов («облаку»), устройствам хранения данных, приложениям и сервисам, которые могут быть оперативно предоставлены и освобождены от нагрузки с минимальными эксплуатационными затратами или практически без участия провайдера.

Из данного определения следует, что сама суть облачных технологий состоит в простоте доступа к вычислительным ресурсам, что затрудняет контроль над доступом к ним как провайдеров, так и правоохранительных органов.

В данной ситуации органы государственной власти сталкиваются с проблемой, свя-

занной с блокировкой противоправного контента в сети Интернет. При использовании технологий распределенных вычислений сложно заблокировать только нарушителей, не затронув при этом невиновных лиц, имея в виду инфраструктуру, им принадлежащую. Нетрудно представить, что при попытке применять нормы гуманитарного права «по аналогии» к информационной среде, сразу же появится проблема смешения так называемых «гражданских» и «военных» объектов в информационном пространстве, которую методом аналогий права решить не получится.

3. Другой проблемой регулирования информационного пространства является его анонимность.

В информационном пространстве, в отличие от реального, уровень анонимности его участников более высок за счет использования технологий сокрытия точного адреса, например, подмены IP-адресов с помощью «виртуальной частной сети», то есть VPN.

Правовые меры государства не решают проблему доступа полностью, в связи с тем, что относятся к национальному законодательству страны. Ничто не мешает злоумышленникам пользоваться сетями и программным обеспечением на территориях других государств. Таким образом, проблема анонимности в сети имеет тесную связь с проблемой трансграничного характера ИКТ.

4. Еще одной проблемой является распространенность ИКТ среди населения всех стран земного шара, имеющих устойчивый доступ в Интернет. Благодаря упомянутым ранее аспектам трансграничности ИКТ и анонимности глобальной сети связи данные технологии доступны для освоения широким слоям населения. Это, конечно, способствует быстрому развитию таких технологий, так как каждый пользователь сети может принять участие в работе над их совершенствованием.

Однако, в итоге, в информационном пространстве складывается ситуация, когда обладатель информации, включая физические, юридические лица, государства и квазигосударственные образования могут быть источниками вредоносной активности, причем за счет анонимности сети и трансграничности ИКТ маскировать свою деятельность, например, выдавая деятельность отдельных хакерских групп за активность стран или случайный сбой.

Поскольку эффективно бороться с угрозами трансграничного характера возможно только совместными усилиями государств, Российская Федерация ведет работу по созданию системы международной информационной безопасности в соответствии с Доктриной информационной безопасности Российской Федерации.

Этому препятствует неурегулированность данной сферы на международном уровне. Такую проблему нельзя решить путем применения существующих международных норм по аналогии к информационной сфере. Ряд причин уже были названы выше — особые свойства информационного пространства и ИКТ.

Для иллюстрации проблемы приведу следующий пример. Нормы международного гуманитарного права основаны на правилах, принимаемых практически всеми членами мирового сообщества.

Например, в 1975 году между СССР и США было подписано межправительственное Соглашение о предотвращении инцидентов в открытом море и в воздушном пространстве над ним.

Данный документ указывает, что его Стороны примут меры по неукоснительному соблюдению командирами кораблей духа и буквы Правил для предупреждения столкновений судов в море (ППСС). Также обе Стороны признают, что основой свободы плавания (операций) в открытом море являются принципы, признанные международным правом, изложенные в Женевской конвенции об открытом море 1958 года.

То есть, указанное Соглашение основывается на двух других, признающихся мировым сообществом, документах обязательного характера. Таким образом, для регулирования частных вопросов обеспечения безопасности в открытом море уже был создан прочный фундамент в виде международных договоров общего характера.

В области регулирования ИКТ на данный момент ничего похожего не существует. Даже сами принципы ответственного поведения государств в информационном пространстве, на которых такие договоры могут быть построены, вызывают оживленную дискуссию участников мирового сообщества, подтверждением чему является последняя сессия Рабочей группы ООН открытого состава (РГОС)

по вопросам безопасности в сфере использования ИКТ.

В связи с этим попытка применять нормы какой-либо сферы международного права к информационной среде «по аналогии» натолкнется на проблемы, которые данное право не способно решить в связи с уникальностью ИКТ-среды. Таким образом, подход «правовых аналогий» не применим для ИКТ и информационного пространства, иначе как для политических спекуляций.

Подводя итог сказанному, можно сделать следующие выводы.

Прямое применение отраслевых норм права (включая гуманитарное) к регулированию информационной сферы невозможно в связи с уникальностью свойств ИКТ и информационного пространства.

Необходимо разработать новые нормы, принятые всем международным сообществом, для регулирования информационных технологий и пространства и борьбы с вредоносным воздействием с применением ИКТ.

Для выполнения данной задачи следует вести правовую работу одновременно по нескольким направлениям международной информационной безопасности (компьютерные инциденты, информационная преступность, деанонимизация и так далее).

В некоторых направлениях такая работа уже ведется, в некоторых — на уровне необязательных к исполнению документов и рекомендаций.

Главная же цель данных мероприятий — создание взаимоувязанной, общеобязательной системы международного информационного права в целях обеспечения информационной безопасности государств.

Это может быть достигнуто, в том числе, созданием модельного законодательства в области обеспечения МИБ, которое смогут использовать заинтересованные государства, что позволит сблизить правовые подходы в регулировании данной сферы.

С.С. Гулямов
Доктор юридических наук, профессор, Заведующий кафедрой Киберправо Ташкентского государственного юридического университета

ГЛОБАЛЬНОЕ КИБЕРМИРОТВОРЧЕСТВО: НОВЫЙ ИНСТИТУТ ДЛЯ НОВОЙ ЭРЫ МЕЖДУНАРОДНОЙ БЕЗОПАСНОСТИ

Абстракт. Развитие киберпространства создало новые вызовы международной безопасности. Традиционные подходы оказались недостаточными для реагирования на трансграничные киберугрозы. В этой связи предлагается концепция международного кибермиротворчества — развертывание уполномоченных субъектов в киберпространстве для мониторинга, предотвращения и разрешения киберконфликтов.

В данной статье анализируются цели, формы, модели и механизмы кибермиротворчества. Рассматриваются принципы законности, гуманности и подотчетности кибермиротворческих операций. Обосновывается необходимость международной Конвенции по кибермиротворчеству и гармонизации национального регулирования.

Делается вывод о перспективах институционализации кибермиротворчества как инструмента обеспечения международного мира и безопасности в условиях новых глобальных вызовов.

Ключевые слова: кибермиротворчество, разрешение киберконфликтов, международная безопасность, международное право, киберпространство

Введение

Развитие информационно-коммуникационных технологий привело к появлению киберпространства как новой сферы человеческой деятельности. В то же время использование кибервозможностей в политических и военных целях создало потенциальные угрозы международному миру и безопасности.

Государства во все большей степени разрабатывают доктрины кибервойны и инструменты для наступательных операций в киберпространстве. Негосударственные субъекты также используют киберпространство для продвижения деструктивных повесток. В этих условиях растут риски опасных киберконфликтов между государствами и негосударственными образованиями (Gulyamov et al., 2021). Предотвращение киберконфликтов и поддержание мира и стабильности в киберпространстве становится актуальной задачей.

В то время как традиционные механизмы дипломатии, правоохранительной деятельности, разведывательного сотрудничества и военного сдерживания остаются актуальными, их неадекватность в решении новых киберугроз все более признается (Карасев, 2019). Нематериальность, мгновенность и трудности атрибуции злонамеренных кибероперациий ограничивают традиционные возможности реагирования. Более того, взаимосвязанность киберпространства требует совместных трансграничных решений для управления рисками, выходящими за рамки национальных границ. Это подчеркивает неотложную необходимость разработки инновационных механизмов управления, адаптированных к уникальным характеристикам киберпространства.

Кибермиротворчество возникло как один из таких новых подходов для поддержания международного мира и стабильности в киберпространстве (Gulyamov, 2023). Оно подразумевает развертывание уполномоченных субъектов в киберпространстве с целями мониторинга поведения, деэскалации напряженности, сдерживания агрессии и обеспечения защиты. Хотя это все еще развивающаяся концепция, кибермиротворчество предлагает гибкие, быстрые и экономически эффективные механизмы, адаптированные к киберпространству, которые укрепляют кооперативную безопасность. Однако практическое применение возможностей кибермиротворчества государствами и негосударственными субъектами опережает связанные правовые разработки. Ключевые аспекты, включая мандаты, системы надзора и модальности сотрудничества, остаются недостаточно определенными, что препятствует эффективности и универсальному участию.

Это подчеркивает необходимость всестороннего правового исследования кибермиротворчества для формирования прочной теоретической базы и практических рекомендаций. Однако в существующих исследованиях сохраняются значительные пробелы, поскольку большинство работ ограничены технически-

ми, стратегическими или этическими вопросами кибермиротворчества (Шевцов, 2020). Отсутствует глубокий анализ правовых вопросов, имеющих первостепенное значение для эффективной политики и управления. Данное исследование нацелено на заполнение этого пробела путем разработки системной теории и комплексных правовых основ кибермиротворчества, соответствующих международному праву.

Цели и формы

Основными целями кибермиротворчества являются предотвращение и разрешение киберконфликтов, деэскалация напряженности, сдерживание киберагрессии и обеспечение защиты в киберпространстве.

Кибермиротворчество может принимать различные формы, включая:

- Мониторинг поведения государств и негосударственных субъектов в киберпространстве для раннего предупреждения киберугроз.
- Меры по укреплению доверия путем обмена информацией, прозрачности и предсказуемости действий.
- Наращивание потенциала государств для обеспечения кибербезопасности и предотвращения киберпреступности.
- Деятельность по обеспечению соблюдения норм ответственного поведения государств и негосударственных игроков в киберпространстве.
- Защита объектов критической информационной инфраструктуры и обеспечение кибербезопасности гражданских лиц.

Таким образом, кибермиротворчество охватывает широкий спектр превентивных, стабилизирующих, защитных и принудительных мер, реализуемых санкционированными субъектами в киберпространстве в интересах безопасности и мира.

Модели и механизмы

Для предотвращения киберконфликтов могут использоваться такие модели кибермиротворчества, как:

- Системы раннего предупреждения на основе мониторинга киберугроз и обмена разведданными для своевременного реагирования (Лазарев, 2021).
- Продвижение норм ответственного государственного поведения в киберпространстве через международные соглашения.
- Проведение совместных киберучений и тренировок для отработки взаимодействия и доверия между ключевыми игроками.

Для разрешения возникших киберконфликтов могут применяться следующие механизмы кибермиротворчества:

- Международное посредничество и добрые услуги для деэскалации и переговоров (Савельев, 2017).
- Создание международных органов для арбитража и расследования киберинцидентов (Яковлева, 2020).
- Введение целевых киберсанкций против злоумышленников при поддержке международного сообщества (Новикова, 2019).
- Проведение ограниченных кибермиротворческих операций по обеспечению критической инфраструктуры и защите гражданских объектов.

Таким образом, кибермиротворчество обладает широким инструментарием для упреждающего предотвращения и оперативного разрешения киберконфликтов между различными субъектами.

Ключевые принципы

Проведение кибермиротворческих операций должно основываться на следующих ключевых принципах:

- Законность использования киберсил в миротворческих целях на основе мандатов международных организаций или согласия конфликтующих сторон.
- Соразмерность кибермиротворческих действий с точки зрения интенсивности, масштаба и длительности для избегания чрезмерного ущерба.
- Гуманность при проведении кибероперациий, исключающая гражданские жертвы и ненужные страдания.
- Беспристрастность и нейтральность кибермиротворцев, не принимающих чью-либо сторону в конфликте.
- Подотчетность за любые нарушения, совершенные кибермиротворческим контингентом с применением мер ответственности.

Эти принципы обеспечивают законное, этичное и эффективное проведение операций кибермиротворчества в соответствии с нормами международного права. Их соблюдение критически важно для легитимации кибермиротворчества и обеспечения участия государств (Орлов, 2018).

Правовой статус и регулирование

Кибермиротворцы должны обладать определенным правовым статусом согласно международному праву (Загорский, 2020). Этот статус включает конкретные права, обязанности, привилегии и иммунитеты кибермиротворческих сил.

Для установления стандартизированных основ правового регулирования кибермиротворчества необходима разработка специальной Международной конвенции о кибермиротворчестве. Такая конвенция должна закрепить ключевые принципы и процедуры проведения кибермиротворческих операций и определить правовые рамки для взаимодействия государств в этой сфере. Принятие подобной конвенции будет важным шагом к институционализации кибермиротворчества как легитимного инструмента обеспечения мира.

Национальное законодательство

Для обеспечения участия государств в глобальных и региональных инициативах по кибермиротворчеству необходимо принятие ими соответствующего национального законодательства.

Такое законодательство должно устанавливать правовые рамки и процедуры для развертывания национальных кибермиротворческих контингентов, определять полномочия государственных органов в этой сфере, а также механизмы ответственности за нарушения. Гармонизация национального регулирования кибермиротворчества между странами будет способствовать эффективному международному сотрудничеству.

Заключение

Кибермиротворчество укрепляет кооперативную безопасность, адаптированную к киберпространству. Однако для институционализации кибермиротворчества как легитимного инструмента управления киберконфликтами необходимы комплексные правовые основы на международном и национальном уровнях. Такая нормативно-правовая база позволит раскрыть весь потенциал кибермиротворчества для поддержания стабильности в глобальном киберпространстве.

К рекомендациям следует отнести следующие пункты:

- Разработать универсальную Конвенцию о кибермиротворчестве, устанавливающую общие принципы и стандарты.
- Подготовить типовые законы и региональные соглашения для гармонизации национального регулирования кибермиротворчества.
- Выработать в государствах национальную политику, доктрины и потенциал, позволяющие эффективно участвовать в кибермиротворческой деятельности на благо международной безопасности.

Список литературы

1. Карасев А.Т. (2019). Международная информационная безопасность: проблемы и решения. Международная жизнь, 8, 51–62.
2. Ачилов О.И. (2020). Киберпреступность как угроза национальной безопасности. Вестник МГУ. Серия 18. Социология и политология, 3, 95-105.
3. Вехов В.В. (2019). Кибертерроризм и проблемы борьбы с ним. Вестник Санкт-Петербургского университета МВД России, 3(79), 169-178.
4. Орлов А.П. (2018). Стратегическая стабильность и информационно-коммуникационные технологии. Проблемы национальной стратегии, 5(44), 70–85.
5. Загорский А.А. (2020). Международная безопасность, стратегическая стабильность и информационные технологии, 2, 15-29.
6. Яковлева А.В. (2020). Кибербезопасность и ее правовое регулирование (зарубежный и российский опыт).
7. Новикова Е.С. (2019). Кибердипломатия как новое направление современной дипломатии. Вестник МГИМО-Университета, 12(3), 60-75.
8. Шевцов В.С. (2020). Информационное противоборство в глобализирующемся мире: актуальность, дифференци-

ация понятий, угрозы политической стабильности.
9. Gulyamov Said Saidakhrarovich. 2023-10-03. International Cyber Peacekeeping: Concept and Legal Regulation. Monograph. 472 p. ISBN 978-620-6-77988-9. LAP LAMBERT Academic Publishing
10. Gulyamov S.S. (2024). Legal Frameworks for the Integration of Artificial Intelligence. 6th International Conference on Nanotechnologies and Biomedical Engineering. ICNBME 2023. IFMBE Proceedings, vol 92. Springer.
11. S.S. Gulyamov, A. A. Rodionov, I.R. Rustambekov and A. N. Yakubov, "The Growing Significance of Cyber Law Professionals in Higher Education: Effective Learning Strategies and Innovative Approaches," 2023 3rd International Conference on Technology Enhanced Learning in Higher Education (TELE), Lipetsk, Russian Federation, 2023, pp. 117–119, doi: 10.1109/TELE58910.2023.10184186.

А.К. Дубень
Кандидат юридических наук, научный сотрудник Института государства и права Российской академии наук

МЕЖДУНАРОДНОЕ СОТРУДНИЧЕСТВО ГОСУДАРСТВ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Вопросы правового обеспечения информационной безопасности приобретают особую актуальность при формировании правовой доктрины и законодательства во многих государствах, отстаивающих свои национальные интересы и заинтересованных в поддержании мира, международной и национальной безопасности.

Сегодня по-прежнему актуален вывод профессора В.А. Копылова относительно места и роли информационной безопасности. По его мнению, информационное пространство не имеет как географических границ, так и часовых поясов[1]. Информационное право, как одна их ведущих отраслей российского права определяет динамику правоотношений, вместе с тем данные отношения, как правило, имеют межгосударственный характер, в котором существуют определенные обязательства в области информационных прав и свобод по таким вопросам, как трансграничная передача данных, использование сетевого пространства, современных цифровых технологий и иных, имеющих значение в аспекте охраны общепризнанных ценностей.

Вопросам правового обеспечения информационной безопасности сегодня уделено особое внимание в свете современных геополитических процессов и их влияния на все сферы жизнедеятельности. Обращает внимание, что одной из задач современного общества является поиск универсальных решений по вопросам информационной безопасности. Одну из ключевых ролей в этом вопросе играет Россия, выступающая инициатором международных конвенций по защите информации и обеспечению международной информационной безопасности. К примеру, 7 декабря 2022 г. 77-я сессия Генеральной Ассамблеи ООН приняла представленную Россией и дружественными ей государствами резолюцию по международной информационной безопасности и поддержала деятельность Рабочей группы открытого состава ООН по вопросам безопасности в сфере использования информационно-коммуникационных технологий (ИКТ) 2021–2025[2].

Ввиду этого система международной информационной безопасности строится на системе взаимосвязанных международных норм, сформированных на основе международного и межрегионального сотрудничества. Вместе с тем одним из перспективных направлений в данной теме является создание международно-правовой базы и формирование понятийного аппарата.

Сегодня на межрегиональном уровне сотрудничество в области обеспечения международной информационной безопасности активизируется и ключевое значение приобретает деятельность межгосударственных организаций. К примеру, в рамках работы ОДКБ государства-члены этой организации подчеркивают, что информационная безопасность каждого государства формирует общую

1 Копылов В.А. Информационное право: Учебник. 2-е изд., перераб. и доп. М.: Юристъ, 2005. С. 21.

2 Интервью заместителя Министра иностранных дел Российской Федерации О.В. Сыромолотова МИА «Россия сегодня» в связи с принятием 7 декабря 2022 г. предложенной Россией резолюции ГА ООН по обеспечению международной информационной безопасности // Официальный сайт МИД России. URL: https://www.mid.ru/ru/foreign_policy/news/1842982/ (дата обращения: 10.09.2023).

безопасность и непосредственно влияет на состояние коллективной безопасности. В совместном заявлении министров иностранных дел государств-членов ОДКБ в 2022 г. отмечено, что государства-члены ОДКБ исходят из необходимости активизации политического взаимодействия[3] в рамках вступившего в силу Соглашения о сотрудничестве в области обеспечения информационной безопасности 2017 г[4]. Соглашение направлено на формирование практических механизмов совместного реагирования на вызовы, угрозы и риски информационной безопасности.

Признавая важность эффективного использования информационных технологий для усиления противодействия новым вызовам и угрозам информационной безопасности, нельзя не отметить, что в 2013 г. участниками Содружества Независимых Государств подписано Соглашение в области обеспечения информационной безопасности[5], по результатам которого современные международные программы в сфере кибербезопасности содержат базовые положения, выработанные и закрепленные в соглашениях СНГ. Кроме того, на постоянной основе проводятся межведомственные консультации государств-участников СНГ по проблематике обеспечения международной информационной безопасности, к примеру, в декабре 2022 г. обсуждалась выработка совместных позиций государств СНГ и их продвижение на международных площадках, а также определены правовые подходы к регулированию международной информационной безопасности с учетом трансграничного обмена данными в рамках реагирования на угрозы и инциденты в условиях новых вызовов и рисков . Обращает внимание, что вопросам международной информационной безопасности особое внимание уделено в ШОС. В рамках исполнения Плана взаимодействия государств-членов ШОС[6]по вопросам обеспечения международной информационной безопасности на 2022–2023 гг. группы экспертов ШОС осуществляют работу по рассмотрению и принятию совместных решений в сфере обеспечения информационной безопасности, включая взаимодействие на профильных многосторонних площадках международных организаций[7].

В свою очередь, Союзное государство в целях снижения уязвимости информационной безопасности от политических и экономических санкций оперативно принимает меры по регулированию информационной безопасности, в частности 22 февраля 2023 г. постановлением Высшего Государственного Совета Союзного Государства утверждена Концепция информационной безопасности Союзного государства. Документ является итогом тесного взаимодействия аппаратов советов безопасности, внешнеполитических ведомств и иных компетентных органов двух стран в сфере совместного противодействия современным информационным вызовам и угрозам на основе прочного правового фундамента.

В целях обеспечения кибербезопасности и защиты информации от внешних угроз в настоящее время подписано более 20 двусторонних соглашений о сотрудничестве в области обеспечения международной информационной безопасности[8]. В совокупности данные со-

3 Совместное заявление министров иностранных дел государств-членов Организации Договора о коллективной безопасности об активизации сотрудничества в области обеспечения международной информационной безопасности // Официальный сайт МИД России. URL: https://www.mid.ru/ru/foreign_policy/news/1840115/ (дата обращения: 10.09.2023).

4 Соглашение о сотрудничестве государств-членов Организации Договора о коллективной безопасности в области обеспечения информационной безопасности от 30 ноября 2017 г. (вступило в силу для Российской Федерации 17 апреля 2019 г.) // Официальный интернет-портал правовой информации. URL: http://publication.pravo.gov.ru/Document/View/0001201904260001 (дата обращения: 10.09.2023).

5 Соглашение о сотрудничестве государств-участников Содружества Независимых Государств в области обеспечения информационной безопасности // Бюллетень международных договоров. 2015. № 10. С. 7–13.

6 Страны СНГ активизируют сотрудничество в области информационной безопасности // Официальный сайт Парламентского Собрания Союза Беларуси и России. URL: https://belrus.ru/info/strany-sng-aktiviziruyut-sotrudnichestvo-v-oblasti-informacionnoj-bezopasnosti/ (дата обращения: 10.09.2023).

7 Сообщение для СМИ об итогах заседания Группы экспертов ШОС по международной информационной безопасности (Ташкент, 13 июля 2022 г.) // Официальный сайт Шанхайской организации сотрудничества. URL: http://rus.sectsco.org/news/20220719/855125.html (дата обращения: 10.09.2023).

8 См., например: распоряжение Правительства Российской Федерации от 23 марта 2022 г. № 587-р «О подписании Соглашения между Правительством Российской Федерации и Правительством Азербайджанской Республики о сотрудничестве в области обеспечения международной информационной безопасности» // СЗ РФ. 2022. № 13. Ст. 2153; распоряжение Правительства Российской Федерации от 4 июля 2017 г. № 1424-р «О подписании Соглашения между Правительством Российской Федерации и Правительством Южно-Африканской Республики о сотрудничестве в области обеспечения международной информационной безопасности» // Официальный интернет-портал правовой информации. URL: www.pravo.gov.ru, 06.07.2017; распоряжение

глашения направлены на выработку совместных мер по развитию норм права, обеспечивающих информационную безопасность, защиту критически важных информационных объектов и предотвращение угрозы кибербезопасности. В свою очередь, стороны принимают участие в выработке стандартов кибербезопасности на основе внутреннего законодательства, при этом двусторонние соглашения определяют не только правовое обеспечение информационной безопасности, но и унификацию норм права при создании, эксплуатации и развитии интегрированной информационной системы, т.е. устанавливают техническое взаимодействие по порядку обеспечения кибербезопасности[9]. Из этого следует, что международное сотрудничество в рамках исследуемого вопроса основано на принципе социальной ответственности и взаимодействие осуществляется в целях восполнения выявляемых пробелов в нормативном регулировании киберсреды.

Анализ базовых положений межгосударственных соглашений позволил определить, что общая цель состоит в формулировании единых правил поведения в информационном пространстве в целях обеспечения информационной безопасности в условиях новых вызовов и угроз посредством международного сотрудничества между всеми соответствующими заинтересованными сторонами.

Таким образом, в целях развития системы информационной безопасности и понятийного аппарата, а также согласованных моделей целесообразно дальнейшее развитие межгосударственного сотрудничества на основе сближения евразийской и евро-атлантической систем международной информационной безопасности с учетом общепризнанных принципов и норм международного права, при котором особое внимание должно быть уделено вопросам безопасности личности и общества в информационной сфере, включая противодействие нежелательному информационно-психологическому воздействию.

Правительства Российской Федерации от 13 мая 2010 г. № 721-р «О подписании Соглашения между Правительством Российской Федерации и Правительством Федеративной Республики Бразилия о сотрудничестве в области обеспечения международной информационной и коммуникационной безопасности» // СЗ РФ. 2010. № 21. Ст. 2628; Соглашение между Правительством Российской Федерации и Правительством Китайской Народной Республики о сотрудничестве в области обеспечения международной информационной безопасности (заключено в г. Москве 8 мая 2015 г.) // Бюллетень международных договоров. 2016. № 11. С. 82–88; Соглашение между Правительством Российской Федерации и Правительством Республики Беларусь о сотрудничестве в области обеспечения международной информационной безопасности (заключено 25 декабря 2013 г.) // Бюллетень международных договоров. 2015. № 7. С. 16–23 и т.д.

9 См., например: Рекомендация Коллегии Евразийской экономической комиссии от 3 февраля 2015 г. №2 «О перечне стандартов и рекомендаций в области информационно-телекоммуникационных технологий и информационной безопасности, применяемых при создании, эксплуатации и развитии интегрированной информационной системы внешней и взаимной торговли» // Официальный сайт Евразийского экономического союза. URL: http://www.eaeunion.org/, 04.02.2015.

Джон К. Мэллори
Научный сотрудник Массачусетского технологического института

ПОСЛЕДНИЕ ИЗМЕНЕНИЯ В РАМКАХ КРУГЛОГО СТОЛА ПО ВОЕННОЙ КИБЕРСТАБИЛЬНОСТИ

Overview

- Roundtables and seminars
- Approach
  - Cyber Threat Reduction Objectives
  - Multi-level cyber conflict
  - Key Mechanisms Destabilizing International Security Architectures
  - Four Modes Cyber Risk Reduction
  - Devising Norms for Conflict Containment
  - Common Aversion Hierarchy
- Catalytic Actors
  - Risk from Catalytic Actors
  - Risk of Catalytic Escalation by Conflict Phase
  - Prevention of 3rd Party Catalytic Attacks
  - Incident Response
  - Declaratory Policies to Deter 3rd-Party CI Attacks
  - Norms To Counter 3rd Party Catalytic Attacks
- Conclusions

Roundtable on Military Cyber Stability 2 John C. Mallery

Roundtable on Military Cyber Stability (RMCS)

Mission: The mission of this roundtable is to scope out a plan for a multinational research program for military cyber stability centered around series of track 1.5 conferences. The research effort develops interdisciplinary and cross-cultural analytical frameworks to understand military cyber stability and evaluate practical cyber stability steps for international security architectures. To this end, the roundtable assembles leading academics, think tankers, and government practitioners from the United States, China, Russia, and other countries to contribute their expertise, experience, and perspectives to help reduce cyber risks to international peace and security.

- ***Roundtables: 6 since 2016***
- ***Seminars: 21 since 2020***
- ***Workshops: 1 since 2019***
- ***Position Papers: 40***
- ***Experts: 23 core, 100 occasional***

Roundtables and Workshops

- *1st Roundtable on Military Cyber Stability*
  Computer Science & Artificial Intelligence Laboratory, Massachusetts Institute of Technology, Cambridge, MA, USA, December 13-14, 2016
- *2nd Roundtable on Military Cyber Stability*
  Shanghai Institutes for International Studies, Shanghai, and China Institute for International Strategic Studies, Beijing, PRC, August 21-25, 2017
- *3rd Roundtable on Military Cyber Stability*
  Center for International and Strategic Studies, Washington, DC, USA, July 17-19, 2018
- *4th Roundtable on Military Cyber Stability*
  Conseil Supérieur de la Formation pour Recherche Stratégique École Militaire, Paris, France, November 27-28, 2018
- *1st Workshop on Military Cyber Stability*
  Cyber Policy Institute, Helsinki, Finland, June 18-19, 2019
- *5th Roundtable on Military Cyber Stability*
  Shanghai Institutes for International Studies, Shanghai, PRC, September 9-10, 2019
- *6th Roundtable on Military Cyber Stability*
  Centre for Humanitarian Dialogue, Geneva, Switzerland, June 15-16, 2023.

Military Cyber Stability Seminar

- During the pandemic, RMCS moved online with the *Seminar on Military Cyber Stability*
- 21 2-hour Seminars were held between September 14, 2020, and May 30, 2023
- Simultaneous translation between Chinese, English, and Russian was introduced in April 2021
  - 15 seminars enjoyed simultaneous translation
- Summaries written in Chinese, Russian, and English and circulated to RMCS experts

MCS Seminars 1

2020-09-14 Joseph S. Nye, *The Broad Context of Military Cyber Stability*

2020-11-02 Nigel Inkster, *Managing Technology Decoupling*

2021-02-22 John C. Mallery, *Prevention and Management Cyber Incidents: A Framework Inspired by the 1972 Incidents At Sea Agreement*

2021-03-08 Lu Chuanying, *Competition Without Catastrophe: A New China-US Cybersecurity Agenda*

2021-03-22 Benjamin Bahney, *The Delicate Balance of Survivability: Using Deterrence Theory to Explain How Imperfect Left of Launch and Damage Limitation Capabilities Impact Crisis Bargaining*

2021-04-12 Natalia P. Romashkina, *Threats in Cyberspace: What the Russian Federation and the United States Can and Should Agree on*

2021-04-19 Lyu Jinghua, *Enhancing Strategic Stability in Cyberspace*

2021-05-03 Xu Manshu, *China-US Cyber Crisis Management*

2021-05-17 Robert Axelrod, *Vengeance and Cyber Conflict*

2021-11-22 *Developments in Cyber Norms & Confidence Building Measures and Their Relevance to Military Cyber Stability*

MCS Seminars 2

2022-01-24 *Recent Artificial Intelligence Challenge Cases for Military Cyber Stability*

2021-11-08 *Cyber Norms and Confidence Building Measures for Biosecurity*

2022-02-28 *Building & Security Measures Among Cyber and Nuclear Weapons States in Times of Crisis*

2022-04-11 *Strategic and Military Competition Under Globalized Interdependence Crisis*

2022-05-10 *International Law and Military Cyber Stability: Thresholds and Actors Roles*

2022-09-26 *Space Competition and Strategic Stability: International Law, Cyber Norms, and Arms Control*

2022-11-07 *Wartime Cyber Restraint: International Law, Norms, and Confidence Building Measures*

2022-12-20 *Space Governance for Military Cyber Stability: Challenge Cases*

2023-04-03 *Confidence Building Measures to Attenuate Insecurity Dilemmas and Enhance Stability*

2023-04-24 *Protection of Cyber Critical Infrastructure During Wartime*

2023-05-30 *3rd-Party Catalytic Actors: Risks and Mitigations*

Cyber Threat Reduction Objectives For Escalatory Models Of Cyber Conflict And Cooperation

- Bilateral confidence building and security measures (CBSMs):
  - Avoid accidental or unintended escalation of conflict
  - Accurately interpret signals
  - Identify indices of intent and capability
  - Establish pre-crisis management mechanisms and institutions
  - Rapidly advance intra- and inter-state *learning* on cyber dynamics
- Multilateral CBMs:
  - Reduce sources of instability in international security systems
  - Reduce numbers of cyber-empowered malicious actors
  - Provide institutions for management of cyber conflict
- Approach:
  - Articulate functionally-grounded norms to reduce cyber risks
  - Address cyber risks above and below "use of force" thresholds
  - Develop challenge cases to illustrate the risk scenarios and motivate proposed norms for threat mitigation
  - Develop shared models, analytical frameworks and perceptions of cybered conflict and cooperation
    - Understand broadly cyber impact on escalation and de-escalation
    - Generate data to confirm models and drive their development
    - Identify actor-specific perspectives and preferences
- Precedents for developing management processes
  - Nuclear weapons
  - Biological weapons

Focus on the Critical Infrastructure Layer (6) in Dimensions of Multi-level Cyber-physical Conflict, Competition, and Cooperation

Dimension	No	Layers	Below LOAC	Description
Ideation	9	socio-cultural	Yes	Ideation, value systems, cultural dynamics, [illegible]
	8	cultural	Yes	[illegible] systems; legal systems; international governance; human rights; [illegible] control
Policing	7	Criminality	Yes	International law enforcement cooperation, domestic law enforcement, criminal investigations, anti-crime efforts.
Security	5	Intelligence	Yes	Espionage, counter-intelligence, cyber defense, counter-terrorism, counter-influence.
	5	[illegible]	Yes	Inter-state cooperation & competition; balance of power; [illegible] land, sea, air, space and cyber; [illegible] information operations. Defense industrial base.
Economics	4	Critical Infrastructure	No (at scale)	Finance, telecom, energy.
	3	Economic	Yes	Systemic stability, exchange rates, finance, trade, portfolio & direct investment, globalization.
	2	Technology	Yes	[illegible] and practices in communications, computation and cryptography.
	1	Science & Engineering	Yes	Research and development, especially ICT.

Ideological Stability

Military Stability

Economic Stability

Key Mechanisms Destabilizing International Security Architectures

- Erosion of confidence in military deterrence
  - Strong advantage to offense over defense in cyber
  - Cyber resilience deficits for conventional forces
  - Fragility of critical infrastructures, especially finance
- Structural security dilemmas
  - Vast advantages for offense over defense
  - Marginal cost of additional unit of offense radically lower than additional unit of defense
  - Pre-emption strategies due to offense advantage
- Insecurity dilemmas
  - Cyber risk drives states to increase security
  - But, counterparties become more insecure and increase their effort
  - Arms races result
  - All parties become more insecure
- Reduced crisis stability
  - Momentum-driven cyber conflict
  - Short decision times
  - Retaliatory pressure due to requirements of proportionality in cross-sector and cross-domain deterrence
  - Catalytic attacks on key infrastructure by 3rd parties
- Escalating conflict below threshold of armed attack (LOAC)
  - Cyber espionage – theft of intellectual property
  - Strategic influence operations
  - Mining critical infrastructure

States take maladaptive decisions – rational actor assumption fails, predictability low

- Ideology or propaganda blowback produces detachment from reality (political psychosis)
- Group think (Janis), toxic leadership into bad policy
- Bureaucratic politics optimizes local power but produces irrational macro-outcomes
- Internal political logic maintains leadership power but produces maladaptive foreign policy
- Information overload impedes ability to identify an adaptive strategy

Four Modes Cyber Risk Reduction

- **State Restraint:** Normative constraints on interstate conflict
  - **Confidence and security building measures (CSBMs)**
    - Transparency measures
    - Cooperative measures
    - Stability measures
  - Cyber norms
  - **International law**
  - Cooperative risk reduction measures
- **Cyber Security and Resilience** (Deterrence by Denial)
  - National
    - National security systems, Critical infrastructure, Enterprise defense, Consumer privacy
  - International shared ICT
    - Finance and commerce, Internet, ICT capital goods
- **Deterrence** (by punishment) of potential adversaries
  - Declaratory policy
  - Tailored response
  - Attribution
- **Persistent Engagement** (Deterrence by Denial and Disruption)
  - Enterprise cyber defense (Defend)
  - Espionage to support cyber defense (Defend Forward)
  - Disruption of adversary operations (Contest)

Devising Norms for Conflict Containment

- Situation
  - Shared international critical infrastructures and those of non-belligerents are at risk of disruption from cyber operations across these conflict phases:
    - Struggle for position
    - Crisis
    - Armed conflict
    - Post conflict struggle for position
- Objective
  - Devise cyber norms and confidence building measures (CBMs) to:
    - Contain conflict and maintain escalation control
    - Avoid adverse impacts on non-belligerents and the world economy
    - Protect civilians within belligerent states
    - De-escalate conflict
- Approach
  - Design norms and CBMs to be self-enforcing based on common aversions and symmetric goals

Common Aversion Hierarchy

Threshold	Common Aversion
1.	Strategic Nuclear War
2.	Limited Nuclear War
3.	Conventional War among Major Powers
4.	Destruction of Non-Belligerent Critical Infrastructure
5.	Attacks on Civilian Populations
6.	Proxy War with Major Power
7.	Local Conventional War between a Lesser and Major Power
8.	Cyber Attacks on National Critical Infrastructures During Crises
9.	Information Attacks During Crises

- Cyber norms and CBMs can be engineered for enforcement by the stage.
- Exceeding a threshold in the aversion hierarchy eliminates it as an enforcement mechanism.

Risk from Catalytic Actors

- **Threat:** Proliferation of advanced cyber attack capabilities
  - Availability of tools, techniques, and procedures (TTP)
  - Diffusion of expertise
  - Black markets for cyber tools, data, expertise
    - Large-scale cyber crime
  - Gray markets for cyber weapons
    - Diversion to catalytic actors
  - Availability of CI vulnerability data and defense techniques
- **Vulnerability:** Difficulty coordinating incident response creates a joint vulnerability of hostile states to 3rd-party catalytic attacks
  - **Attribution Problem:** Inability to exchange situational awareness necessary to identify the 3rd party and exculpate the counterparty
- **Force Multiplier:** Mining of adversary critical infrastructures creates the risk that 3rd parties will hijack implants of a primary party

Risk of Catalytic Escalation by Conflict Phase

- Peacetime
  - No major disputes and no perception of threat
  - No intelligence struggle
  - Business as usual
- Struggle for Position
  - Range of major disputes
  - Gray-zone
    - Intelligence struggle
    - Aggressive cyber operations
    - Battlespace preparation
    - Provocative operations
  - Strategic competition short of armed conflict
    - Defense modernization – arms races
    - Technological and economic competition
- Crisis – tipping point
  - Diplomatic
  - Economic sanctions
  - Militarized
- Armed Conflict
  - Proxy
  - Low intensity
  - Regional
  - Strategic
- Post-Conflict Struggle for Position
  - Return to struggle for position
- Settlement
  - Major disputes resolved
  - Return to peacetime

Extreme
High
Moderate
Moderate

Prevention of 3rd Party Catalytic Attacks

- Deterrence by denial:
  - Increase assurance of CI
  - Increase resilience of CI
  - Improve cyber defense of CI
- Shape interactions
  - Control proliferation of cyber tools, data, expertise
  - Use threat intelligence to disrupt (pre-empt) 3rd-party attacks
  - Jointly deter 3rd-party attacks

Incident Response

- Communications channels to report and discuss "anomalous" cyber operations
  - Directory of counterparts by function
    - Government
    - Critical infrastructure operators
    - Other IT industry
- Mechanisms to share situational awareness necessary for accurate attribution
  - Establish a hot line to address incidents
  - CERT to CERT real-time sharing
  - Frameworks for exchange of forensic data
  - Criteria for assessing probability of 3rd activity
    - Assumes a framework for attribution
    - Trusted party for attribution may help
      - Example: UN attribution council
- Joint response plans
  - Procedures to guide and coordinate response
  - Exercises to test and debug response procedures

Declaratory Policies to Deter 3rd-Party CI Attacks

- Requirements
  - Credibility of joint attribution
    - Mechanisms to share situational awareness necessary for accurate attribution
  - Schedule of punitive responses
    - Agreement on joint punitive responses
  - Joint commitment to response
    - Establishment of credibility despite hostile relations
- Efficacy
  - Likely to deter rogue states and uncontrolled proxies
  - Unlikely to deter ideological actors like hacktivists, insurgents, and terrorists
- Difficulty
  - Coordinating such a declaratory policy is not easy
  - Yet, as the risks are perceived to risk, motivation to coordinate will increase

Norms To Counter 3rd Party Catalytic Attacks

- Technical
  - Increase assurance, resilience, and cyber defense
  - Develop mechanisms to exchange situational awareness
    - Forensic data
    - Attribution criteria
- Operational
  - Do not preposition attack-ware in adversary critical infrastructure
  - Develop communications channels for response
  - Acquire and share threat intelligence on risky actors
  - Develop joint plans for preparation before and response after a CI attack
- Policy
  - Control proliferation of cyber tools, data, expertise
  - Restrain proxies or 3rd parties associated with state cyber operations
  - Prevent non-state actors from launching CI attacks from national territory
  - Adhere to UNGGE norms not to attack CI
    - Adhere to IHL proscription of unnecessary harm to civilians
  - Develop joint declaratory policies to deter risky actors

Conclusions

- The RMCS process is one of the few dialogues on military cyber between the US, Russia, and China
  - The dialogue cuts across cultures, histories, ideologies, doctrines, disciplines, and political systems
- The intellectual synergy across the RMCS experts:
  - Enriches exploration of cyber and information risks
  - Helps generate mitigation strategies
- Governments receive readouts to inform their thinking
  - Early warning mechanism outside routine bureaucratic cognition
- States may take steps to avoid or manage mechanisms of instability
- Continuing research and dialogue will be required to effectively manage high complexity of the international system and military interactions:
  - Pervasive cyber systems
  - Digitized mass cognition
  - Widespread introduction of artificial intelligence

Dimensions of Conflict Containment

- Geographic scope
- Military domains
  - Land
  - Sea
  - Air
  - Space
  - Cyberspace
- Societal dimension
  - Economic
  - Civilian
- Intensity
  - Level of disruption
    - Consequences
    - Time to restoration
  - Civilian Hardship
    - Health consequences
    - Fatalities

Cyber Risk Reduction

Risk = f	(Threat		Vulnerability		Consequences)	
Attacker	Intent	Capabilities	Inherent	Introduced	Fixable	Fatal
Defender	Deter	Disrupt	Defend	Detect	Restore	Discard
Strategy*	Shape Interactions		Increase Assurance		Increase Resilience	
Deterrence*	Punishment		Denial		Denial/Entanglement	
Norms*	Stability Measures		Architectural Change		Duty to Assist	

DSB Layered approach for managing cyber risk:

- When property exercised, defensive strategies can defend against Tier 1 and 2 threats
- Defending against known vulnerabilities is an insufficient strategy against Tier 3-4 threats
- Since it will be impossible to fully defend our systems against Tier 5-6 threats, deterrence must be an element of an overall risk reduction strategy
- Additional measures are required, such as consequence management

* Mallery addition

Source: Defense Science Board, *Resilient Military Systems and The Advanced Cyber Threat*, January 2013: 6.

Strategic Modes of Critical Infrastructure Protection

No.	Modes	Concept	Escalatory Potential	Protection Outside Cyber
	Deterrence			
1.	Punishment	Retaliation to dissuade counterparty from CI attack	Cross-Domain	Yes
2.	Denial	Security & resilience benefits	No	Yes
3.	Entanglement	Economic & social benefits	No	Yes
4.	Taboo	Reputational & soft power benefits	No	Yes
	Persistent Engagement			
5.	Maintenance of Access	Targets cyber offense	Low	Yes
6.	Threat Intelligence	Tracks offensive tradecraft	Low	Yes
7.	Defense Informed by Threat	Neutralizes adversary offensive capabilities	No	Yes
8.	Offense Suppression	Disrupts adversary offensive capabilities	Moderate	Yes

The Challenge Case Methodology

Case-based approach describes a mechanism in a scenario that leads to a cyber problem

- Phenomenological description enables analysis from multiple perspectives
- Brings out divergences in perspectives for discussion
- Motivates cyber norms, CSBMs or other means to mitigate the cyber problem

	Template for Challenge Cases	
1.	Title	Telegraphic title conveys the nature of the case
2.	Scope	The actors or systems affected by the challenge
3.	Description	A scenario summary that lays out the mechanisms leading to undesirable outcomes
4.	Consequences	The impact and dangers if the challenge case is not addressed
5.	Norm	Proposed principles or steps to mitigate risk
6.	Forum	Institutional context for addressing the challenge
7.	Barriers	Blocks that impede realizing the solution
8.	Enablers	Elements necessary to realize the solution
9.	Technical Feasibility	Technological basis for the proposed norm
10.	Political Feasibility	Alignment of interests among solution actors

Challenge Cases 1

1. Crisis Stability - Changsha, 2011
2. Cybered Signaling - Changsha, 2011
3. Cross-domain Responses - Changsha, 2011
4. Proportionality Judgments - Changsha, 2011
5. Principle Of Distinction - Changsha, 2011
6. Cyber Insecurity Dilemmas - Changsha, 2011
7. Structural Cyber Security Dilemmas - Changsha, 2011
8. Information Warfare in the Digital Noosphere - Changsha, 2011
9. Misattribution of Actions By Uncontrolled Actors - Changsha, 2011
10. Low Intensity Cyber Conflict - Changsha, 2011
11. Cybered Economic Conflict - Changsha, 2011
12. Revelatory Surprise - Changsha, 2011, Garmisch, 2018 revised
13. Measuring The Intensity of Actions or Campaigns from Hostility to Altruism - Changsha, 2011, revised 2018
14. International Attribution Council Increase General Deterrence in the World System - Palo Alto, 2013
15. Destabilization of Nuclear Force Balances - Garmisch, 2013, revised 2018
16. Catalytic Actor Attacks Telecom Core During Major Power Crisis - Garmisch, 2013, revised 2018
17. Pathological Deterrence Dynamic - Garmisch, 2018
18. Miscalibration of the Threshold for Armed Attack - Paris 2018
19. Momentum-driven Nuclear War Based on Fear of Cyber First-mover Advantage - Helsinki, 2019
20. Inadvertent Cyber Attacks on NC4/SR - Helsinki, 2019
21. Left-of-Launch Attacks on Missile Systems - Helsinki, 2019
22. Artificial Intelligence and Instability - Helsinki, 2019

Challenge Cases 2

23. Cyber Incident Prevention & Management - Moscow, 2020
24. Cyber Dynamics Leading to Uncontained Escalation Above LOAC Thresholds - Helsinki, 2019
25. Major Damage to 3rd Parties via Uncontained Cyber Impacts on International Critical Infrastructures - Helsinki, 2019
26. Erroneous Early Warning in ISR Systems - MCS Seminar, January 2022
27. Cognitive Pathologies Arising from AI Decision Support - MCS Seminar, January 2022
28. Critical Infrastructure Safety Systems - MCS Seminar, January 2022
29. Uncontrolled Propagation of Destructive Narratives (AI Gain of Function) - MCS Seminar, January 2022
30. Preventing the Robespierre Scenario - How Virtue Signaling Campaigns can be exploited and weaponized - MCS Seminar, January 2022
31. Autonomous Cyber Operations - MCS Seminar, January 2022
32. Shadows of Killer Robots: The Case of the "Algorithmic" Assassination in Tehran - MCS Seminar, January 2022
33. The Phantom Straw Threatening Great Power Relations - Standalone AI Systems That Lack "Brake" - MCS Seminar, January 2022
34. Trust and Non-Interference in Human Target Recognition Systems - MCS Seminar, January 2022
35. AI-enabled Cyber Attack Spoofs or Takes Down Strategic Early Warning Systems - MCS Seminar, January 2022
36. AI Application on Nuclear Weapons and Nuclear Deterrence - MCS Seminar, January 2022
37. Threats of Deep Fake Technology in Political Sphere - MCS Seminar, January 2022
38. AI Arms Race & Arms Proliferation - MCS Seminar, January 2022
39. Catalytic Actor Destabilization of Politico-Military Crisis - MCS Seminar, February 2022
40. Secondary Party Escalation Spiral in a Multiparty Politico-Military Crisis - MCS Seminar, February 2022
41. Maintaining Communications Channels to Control Escalation - MCS Seminar, November 2022
42. CNA Operations Should Rule From Undeniable C&C Infrastructure - MCS Seminar, November 2022
43. Transparent Prepositioning For Signaling and Deterrence - MCS Seminar, November 2022
44. Military Use of AI and its Application in The Nuclear Field - MCS Seminar, April 2023

КРУГЛЫЙ СТОЛ № 3
АКТУАЛЬНЫЕ ПРОБЛЕМЫ СОХРАНЕНИЯ ТРАДИЦИОННЫХ ДУХОВНО-НРАВСТВЕННЫХ ЦЕННОСТЕЙ В ГЛОБАЛЬНОМ ИНФОРМАЦИОННОМ ПРОСТРАНСТВЕ

Ведущий:

Прокопенко И.С., автор и ведущий программы «Военная тайна» на телеканале «РЕН ТВ», семикратный лауреат премии ТЭФИ, документалист, журналист, писатель

А.Н. Митин
Доктор экономических наук, профессор, зав. кафедрой социально-гуманитарных дисциплин УрГЮУ им. В.Ф. Яковлева

ТРАДИЦИОННЫЕ ДУХОВНО-НРАВСТВЕННЫЕ ЦЕННОСТИ В КОНТЕКСТЕ ЗАЩИТЫ РОССИЙСКОЙ ГОСУДАРСТВЕННОСТИ

Государственность в трудах И.Л. Бачило определяется как единый политико-правовой механизм, в котором отражаются субъективные возможности этноса[1]. В исследованиях других авторов, государственность, с одной стороны, представляется как комплекс элементов, структур, институтов публичной власти, а также институтов неполитического характера, а с другой, трактуется как свойство, качество, состояние общества на конкретном историческом этапе его функционирования[2].

Исходя из наработанных в науке понятий, государственность сегодня рассматривается как самоорганизация общества, выражающая навыки и решения, традиции и нормы, образования и институты, в которых накапливаются (сосредотачиваются, объединяются) способы управления общими делами, поддержания порядка и безопасности воспроизводства сообщества и урегулирования вопросов, возникающих с другими образованиями.

В состоянии реализации государственность — это качество, порядок, безопасность, образование, институты, обычаи и правовые нормы, а по форме, государственность — это страхование общества от случайностей. Государственность рассматривается как ключевой элемент организации и функционирования страны. Она включает в себя не только наличие территории, города и правительства, но и суверенитет, международное признание и способность принятия решений внутри своих границ.

Причины потери государственности могут быть различными, что в конечном итоге приводит к потере независимости страны. Государство, переживающее потерю государственности, обычно ожидает распад или поглощение другими странами с последующей ассимиляцией населения.

Любое государство обладает набором своих ценностей, которые всегда направлены на личность, на жителей страны, на поддержание их жизнедеятельности, прав и свобод. По существу, это набор желаемых характеристик, которые наиболее важны для осуществления государственной деятельности. Они доступны в информационном пространстве и требуют защиты как в национальном, так и в международном формате.

Т. Парсонс утверждает, что ценности остаются объяснением действий индивида, то есть обоснованием его стремлений поступков и предпочтений[3], что справедливо и применимо не только к отдельным личностям, но и к государствам. Предлагаемые государством ценности, выполняют две функции: во-первых, мотивационную, при реализации политического курса и приведении его в соответствии с желаемым идеалом, во-вторых, легитимационную, для оправдания, объяснения принимаемых управленческих решений стремлением достижения желаемого идеала.

Как отмечает Н. Патрушев, интерес к вопросу о том, какие ценности нужны, возникает, как правило, когда перед обществом

1 Бачило И.Л. Факторы, влияющие на государственность//Государство и право. 1993. №7 с. 27.

2 Морозова Л.А. Современная российская государственность//Проблемы теории и практики. М.1998 с.16.

3 Парсонс Т. О структуре социального действия. М.: Академический проект, 2000. С. 458–563.

встает вопрос о выборе путей дальнейшего развития[4], об укреплении государственности. В первую очередь речь идет о духовно-нравственных ценностях, нравственных ориентирах, находящихся в основе мировоззрения.

Именно такая ситуация сложилась для России, что потребовало впервые в новейшей истории страны принять качественное мировоззренческое решение: впредь оценивать уровень государственности страны из своих ценностей и своих национальных интересов, не забывая при этом своих экономических интересов и геополитических выгод.

Для достижения этих целей потребуется возродить такие почти не востребованные ценностные ориентиры, как Родина, совесть, справедливость, солидарность, патриотизм, служение Отечеству. Сегодня им противостоят: культивирование эгоизма, вседозволенность, безнравственность, отрицание идеалов патриотизма, разрушение красоты воспитания ребенка и крепкой семьи. Они идут не только из-за рубежа, но и формируются внутри общества и представляют реальную угрозу: уменьшение рождаемости, физическое выживание народа как такового, дискредитация функции защиты страны, распад государства и др.

Механизм взаимовлияния, взаимозависимости ценностей и государственности может быть реализован через ценностно — цивилизационный подход, при котором человечество развивалось не по единому пути, поскольку всегда суперэтносы (по Л. Гумилеву), или цивилизации (по Тойнби или Хантингтону), на которые делится человечество, отличали прежде всего ценностями. Государство при таком подходе формирует из состава своего населения профессиональных управленческих работников, которые приобретают необходимые компетенции для реализации многих государственных функций, в том числе идеологических, влияющих на формирование мировоззрения через систему ценностей — целостное восприятие человеком действительности. Даже если в Конституции присутствует запрет на государственную идеологию, невозможно внедрить запрет на самосознание, на собственное мировоззрение. Поэтому любая функция государства остается глубоко идеологичной по существу.

В Российской Федерации ценностно-цивилизационный подход конкретизируется в двух указах Президента Российской Федерации, которые в отличие от законов, что создают нормы, создают смыслы в контексте некоего понимания добра и зла, должного и не должного. Это — указ от 9 ноября 2022 г. №809 «Об утверждении Основ государственной политики по сохранению и укреплению традиционных российских духовно-нравственных ценностей»[5]; Указ от 25 января 2023 г. №35 «О внесении изменений в Основы государственной культурной политики, утвержденные Указом Президента Российской Федерации от 24 декабря 2014 г. №808»[6].

У государственной политики три основные цели: сохранить и укрепить традиционные ценности; обеспечить их передачу от поколения к поколению; сохранить свою культурную и цивилизационную идентичность. Для достижения этих целей государственные политики должны решить комплекс задач. В некотором смысле ценности и культуры становятся более важными, чем оборона и экономика, а ценностное представление о культуре приобрело звучание: «культура — это механизм передачи ценностей от поколения к поколению»[7]. В свою очередь, «воспитание в национальной культуре — это уже идеология»[8], где культура всегда идеологична. Следовательно, осмысление многочисленных процессов и явлений, происходящих в российской государственности, производится с опорой на традиционные ценности и последующие появившиеся смыслы. В этом случае государственность, как самоорганизация общества, и ценности, имеющие вневременной характер, нерасторжимы. Вместе с тем ценности не должны быть самоцелью, поскольку остаются частью каж-

4 Патрушев Н. Нужны ли России универсальные ценности? [Электронный ресурс]. Режим доступа: http://www.scrt.gov.ru/news/allnews/2802/ (Дата обращения 05.03.2023).

5 [Электронный ресурс]. Режим доступа: http://www.garant.ru/products/ipo/prime/doc/405579061 (Дата обращения 17.09.2023).

6 [Электронный ресурс]. Режим доступа: http://www.garant.ru/products/ipo/prime/doc/406130451 (Дата обращения 2.09.2023).

7 Аристархов В. От слов к делу. Защита традиционных ценностей и политика государства. Изборский клуб. [Электронный ресурс]. Режим доступа: https://dzen.ru (дата обращения17.09.2023).

8 Шахназаров К.: Мы воспитали детей в чужой культуре. Изборский клуб. [Электронный ресурс]. Режим доступа: https://dzen.ru (дата обращения17.09.2023).

дого гражданина России, частью его идентичности, они в определенном смысле объединяют материальное и духовное. В процессе реализации государственных политик требуются государственные и отраслевые программы, комплексный анализ и внесение изменений в законодательство. Творческое внедрение новых учебных дисциплин в системах просвещения и высшего образования. Например, в новой учебной дисциплине «Основы российской государственности»», приводя примеры безнравственных западных ценностей, будет ошибкой отрицать, что некоторые из них проявляются в нашей рыночной экономике, а при обсуждении будущего развития страны не будет лишним вести разговор о необходимости объединяющей идеи, которая сродни долгосрочной национальной стратегии. В ней безусловно будут присутствовать ценности интересов России, не подчиненные интересам Запада или любой другой цивилизации.

А.В. Шевченко
Доктор политических наук, профессор, заведующая кафедрой Института права и национальной безопасности РАНХиГС

СЕМАНТИКО-КОГНИТИВНЫЙ ПОДХОД К ИССЛЕДОВАНИЮ ИНФОРМАЦИОННОЙ УСТОЙЧИВОСТИ МЕЖДУНАРОДНОЙ ПОЛИТИЧЕСКОЙ СИСТЕМЫ

На пленарном заседании XVII Международного Форума «Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности» в выступлении представителя Координационного центра доменов RU/.РФ прозвучал актуальный призыв к созданию «новых информационных пространств и программ». Согласимся: снятие проблем доверия и ответственного поведения выходит за рамки технических и технологических решений и не может рассматриваться вне проблемы понимания смыслов международной информационной безопасности. Объектом научного исследования МИБ становятся *геополитические среды*, поскольку принятая в теории международных отношений размерность *«геополитическое пространство»* недостаточна для анализа причинно-следственных связей остроты проблем МИБ.

Средообразующим (формирующим) компонентом является феномен доверия, стремительно теряющий свое исходное значение, в том числе и как категория международного права. Провозглашенные ООН меры доверия, выражающиеся в обмене информацией, наблюдении и проверке, ограничениях военных действий и т.п., не применимы, так как лишены собственно основы отношений, при которых «участник ставит себя в добровольную зависимость от кооперативности поведения контрагента».

Семантическое значение понятия «добровольности» в современных международных отношениях тоже девальвировано. Применив известные модели идеальных типов поведения и эмоционального состояния государств Макса Вебера и Доминика Моизи, не сложно определить, какая страна реагирует на инициативы России в области укрепления МИБ по собственной воле, а какая — под давлением «кооперативного контрагента»[1].

Динамика трансформаций структуры и функций мировой политической системы от однополюсной иерархии — к системно-сетевой организации и к хаотизации и перерождению — определяет функциональные состояния геополитической среды как совокупности принуждений и ограничений, устанавливаемых в отношении системы международных отношений. Выявлена закономерная зависимость устойчивости политической системы от информационной, ментальной и политической идентичности политических акторов: чем полнее учтены и реализованы согласуемые параметры идентификации человека с миром политического, тем устойчивее поведение политической системы[2].

Геополитическая среда, в которую погружаются инициативы обеспечения международной безопасности, формируется в беспорядочном перемешивании дипломатий: «дипломатии страха», «дипломатии надежды», «дипломатии унижения», «дипломатии превосходства».

В этих условиях дипломатическая практика в целях обеспечения безопасности и стабильности международных отношений в пери-

1 Моизи Доминик. Геополитика эмоций. Как культуры страха, унижения и надежды трансформируют мир — М., 2010.

2 Шевченко А.В. Информационная устойчивость политической системы постиндустриального общества — https://new-disser.ru/_avtoreferats/01003307784.pdf.

од хаотизации основополагающих структурных элементов политической системы (организационного, институционального, коммуникативного, культурно-идеологического и др.) призвана формировать *параметры порядка* в виде динамических информационно-коммуникативных комплексов, отражающих философию и идеологию геополитических игроков.

На современном этапе цивилизационные оппоненты России реализуют политическую экспансионистскую концепцию, пришедшую на смену колониальной политики, — так называемого «стратегического соседства», в основу которой положен дуальный (зависящий от целеполагания субъекта геополитики) принцип географической непрерывности.

В целом политика соседства реализует «рациональный подход к организации устойчивых, долгосрочных отношений с соседними государствами (отдельными их группами), позволяющий использовать выгоды соседства и минимизировать его ограничения в качестве средства обеспечения необходимых условий национального роста и развития»[3]. Это особое направление внешнеполитической стратегии государства, которая может формироваться или трансформироваться под влиянием разного рода политических обстоятельств.

Принцип географической непрерывности (континуальности), в отличие от принципа прерывности (дискретности), фундирует концепцию стратегического соседства в ее претензии на территориальную взаимосвязанность и слитность государств, беспредельную делимость географического национального пространства, нелокальность и постепенность в сближении процессов и состояний[4]. Применение принципа географической непрерывности в геополитике и позволяет государству-гегемону распространять сферу своих национальных интересов на территории других государств, ни по каким географическим признакам не являющихся его соседом.

При этом колониальная идеология остается прежней, а технологический арсенал стратегического соседства представляет собой динамические комбинации методов и средств жесткой и мягкой политической экспансии, включающей информационно-коммуникационно и информационно-коммуникативно обеспеченные гуманитарные политики — этнические, образовательные, культурные, медийные и др. — все известные по арсеналу «мягкой силы», но в более завуалированной «добрососедской» помощи.

Одна из стратегических целей «стратегического соседства» — ослабить геополитическое влияние конкурентов или противников, в частности — России и Китая. Например, неприкрытые жесткие формы «стратегического соседства» реализованы через политэкономические и финансовые механизмы Евросоюза по отношению к странам Балтии, спекулятивно используются для манипулирования ресурсами и активами Украины и др. государств бывшего социалистического лагеря.

Концепцию стратегического соседства в ее мягких вариантах принимают и более осторожные геополитические акторы: например, Монголия, выстраивающая свою международную политику с учетом интересов трех соседей: России, Китая и США.

Технологии стратегического соседства активно реализуются в государствах Центральной Азии: обильное финансирование грантов, стажировок для воспитания молодых «прогрессивных лидеров наций», программ, акцентированных на удовлетворение самых острых потребностей (вода, энергия, опустынивание и др.). При этом программы обеспечены такими опциями как, например, внешние адвокации или надзор за деятельностью государственных органов и повышение прозрачности в принятии политических решений.

Особый уклон программы стратегического соседства имеют в стороны неэлитных, широких слоев общества. Так, в Узбекистане завершена реализация пятилетнего плана «Образ для совершенного будущего» с бюджетом почти в 30 млн долл. Разработчики — два госуниверситета Флориды и Миссисипи — создали программу улучшения результатов обучения узбекского языка как родного. В основу положен принцип когнитивного постижения семантики языка.

Единицей измерения показателей массовой информации, заполняющей информационно-коммуникативное пространство, служит

3 Песцов С.К. Регионализм как тактика: политика Индии «Соседство прежде всего» // Россия и АТР. 2023, — №3. С. 9–36.

4 Преображенский В.С. Непрерывность и прерывность в географической оболочке — https://www.activestudy.info/nepreryvnost-i-preryvnost-v-geograficheskoj-obolochke/?ysclid=ln5sc60pwe547607373.

смыслофакт: категория, отражающая результат профессионального осознания, понимания и рефлексии творческого субъекта по поводу сообщения любой информационной природы, т.е. извлечения смысла из явлений реальной действительности. Он образован методом логического совмещения понятий: факт как явление материального и смысл как субъективированная реальность. Смыслофакт фиксирует переход денотативного значения слова к его коннотативному смыслу, отражая в социальном явлении единство формы (факт) и содержания (смысл). Культурная насыщенность смыслофакта определяется разрешающей способностью семантического пространства информационного субъекта[5].

Когнитивные технологии «стратегического соседства» искусно изменяют структуру смыслофакта за счет эффектов семантических сдвигов, визуального упрощения восприятия, примитивизации изложения или откровенной манипуляции культурными традициями объекта воздействия, например, использованием метафор. Установить смысловые «закладки» приема метафоризации и глубже познать сущность и механизмы образно-метафорического мышления, «свойственные носителям определенной этнокультуры, общие закономерности метафорической концептуализации и репрезентации мира, характерные для конкретного исторического периода», позволяет семантико-когнитивный подход[6].

Одна из продуктивных моделей семантико-когнитивного подхода, разработанная Ю. Кравцовой, представляет собой трехкомпонентную структуру, «включающую исходную и новую денотативно-понятийные сферы и семантико-когнитивный формат, который трактуется как понятийно-смысловой элемент, интегрирующий разные сущности, сходные в каком-либо отношении».

Семантико-когнитивный подход к анализу геополитической среды МИБ, зависящей и от политико-дипломатического дискурса, позволяет выявить ментальные особенности и приёмы участников переговорных процессов, особенности англо-саксонских, северо-американских, азиатских, арабских когнитивных моделей и речевых стратегий.

5 Шевченко А.В. Информационная устойчивость политической системы — М., Издательство «Граница», 2005.

6 Кравцова Ю. Семантико-когнитивный подход к исследованию метафоры: методологические основания и перспективы развития // ACTA UNIVERSITATIS LODZIENSIS FOLIA LINGUISTICA ROSSICA № 12, 2016. https://www.semanticscholar.org/paper/Семантико-когнитивный-подход-к-исследованию-и-Кравцова/beba623da0993390be9ac22a4b8a8dfc084d4edb.

В.А. Чумаков
Кандидат политических наук, помощник руководителя ФКУ «Аппарат Общественной палаты России»

Ф.В. Ниточкин
Аспирант МГЮА им. О.Е. Кутафина, ответственный секретарь Координационного совета по общественному контролю за голосованием при Общественной палате Российской Федерации

ДИСТАНЦИОННОЕ ЭЛЕКТРОННОЕ ГОЛОСОВАНИЕ: МЕЖДУ ЛИЧНЫМ УДОБСТВОМ И ОБЩЕСТВЕННОЙ БЕЗОПАСНОСТЬЮ

Аннотация: Развитие дистанционного электронного голосования (ДЭГ) в России идёт впечатляющими темпами. Впервые проведённое в качестве эксперимента в 2019 году на муниципальных выборах в Москве, в 2023 году оно охватило уже 25 субъектов Российской Федерации. Популярность ДЭГ среди избирателей тоже стремительно растёт. Однако сохраняющееся психологическое недоверие к новым информационно-коммуникационным технологиям, помноженное на некоторый правовой нигилизм и избирательный абсентеизм, всё ещё имеющие место в нашей стране, является серьёзной угрозой легитимности выборов. К задачам современной науки о защите информации в этом разрезе относится разработка подходов к нормативному регулированию новых правоотношений, возникших в связи с внедрением ДЭГ. Также важно обеспечение твёрдых правовых гарантий и технологических инструментов соблюдения при проведении ДЭГ основных принципов избирательного процесса, установленных Конституцией Российской Федерации, а именно: всеобщности выборов, тайны голосования, гласности, достоверности волеизъявления.

Ключевые слова: прозрачность выборов, общественное наблюдение, дистанционное электронное голосование (ДЭГ), цифровой сейф-пакет, аудируемость и анонимность ДЭГ, нода блокчейн ДЭГ.

В XXI веке процесс глобальной цифровизации охватил практически все виды человеческой деятельности в экономической, политической, общественной и личной сферах. Развитие цифровых технологий существенно модернизирует взаимоотношения гражданина, общества и государства, меняет конкретные способы их взаимодействия, включая механизмы обратной связи и продвижения гражданских инициатив, формы общественного контроля за властью, а также процедуры легитимации государственных институтов.

Современному активному пользователю новых цифровых решений удобнее не

только покупать и продавать товары (B2P — business-to-people взаимодействие и P2P — person-to-person взаимодействие), но и получать государственные и коммерческие услуги в электронном виде. Подобно этому его общественная активность так же неуклонно перемещается в Интернет. Регистрация актов гражданского состояния, электронные опросы, заявки на гранты, общие собрания собственников жилья, перепись населения, и, наконец, дистанционное электронное голосование (ДЭГ) — все эти процессы цифровизации публично-правовых отношений отвечают на существующий общественный запрос и являются приметами нового времени, составляя, по мнению ряда экспертов [1], фундамент формирующейся электронной демократии.

Вместе с тем, цифровая трансформация традиционных и возникновение новых социальных отношений влечет за собой необходимость их дополнительного правового регулирования [17]. Это безусловно относится и к избирательному законодательству Российской Федерации, в которое с 2021 года включены нормы о ДЭГ. Сложная эпидемиологическая ситуация в период пандемии COVID-19, став естественным катализатором больших организационно-технических изменений, предопределила ускоренное внедрение в России новых электоральных технологий в 2020–2021 годах.

В Единый день голосования (ЕДГ) в качестве эксперимента ДЭГ впервые проводилось на выборах в Мосгордуму в 2019 году, а затем в 2020 году также в Москве на довыборах в муниципалитеты и в ходе общероссийского голосования по вопросу одобрения изменений в Конституцию Российской Федерации. В 2021 году ДЭГ проходило уже в семи, а в 2022 году в восьми регионах России. На выборы в ЕДГ 2023 года было подано 30 заявок от субъектов Российской Федерации, из них ЦИК России одобрила 25. Такой стремительный рост распространенности ДЭГ позволяет говорить о возможности достижения полного охвата им российских избирателей в ближайшем будущем.

Пионером инноваций в сфере пользовательской цифровизации, как это часто бывает, выступила Москва, которая использует собственную платформу ДЭГ на базе портала mos.ru. Абсолютное большинство жителей столицы знают о возможности проголосовать электронно, каждый второй допускает для себя такой формат участия в выборах [6]. Доверие к ДЭГ растет и на федеральном уровне: порядка 76% опрошенных заявляли, что знают, слышали или имеют опыт участия в нем. К процедуре ДЭГ среди россиян сложилось положительное отношение — данные соцопроса показывают, что она востребована в обществе. Интересен и тот факт, что за распространение ДЭГ в регионах также выступает большинство (59%) опрошенных [18].

Среди преимуществ ДЭГ респонденты отмечают: простоту и удобство использования, доступность для различных возрастных групп, а также популярность среди молодежи и впервые голосующих; устранение территориальной привязки к УИК, что позволяет голосовать из любого места; экономию времени в связи с отсутствием необходимости являться на избирательный участок; возможность проголосовать в любое время суток. Упрощение избирательных процедур и легкость организации выборов также являются преимуществами электронного голосования. Таким образом, обратная связь с гражданами свидетельствует о формировании у россиян новой электоральной привычки, которая имеет все возможности стать со временем общепринятой нормой.

В то же время, как у любого технического новшества, у ДЭГ есть свои «луддиты» — люди, не просто не доверяющие инновациям, но и агрессивно навязывающие свою точку зрения остальным. Такой выраженный «неолуддизм» является психологической особенностью, характерной для небольшого числа граждан, негативные аргументы которых неоднократно публично опровергались, но их голос по-прежнему слышен довольно громко, а общественный резонанс, вызываемый «разоблачениями» ДЭГ, является серьезной угрозой для легитимности выборов и наблюдения за ними.

Несмотря на рост популярности ДЭГ, оно по-прежнему незаслуженно критикуется скептиками за якобы непрозрачность процедур, недоступность для общественного контроля и представляется своеобразным «черным ящиком». Высказываются мнения о возможности применять ДЭГ для «накручивания» голосов избирателей, подмены результатов воле-

изъявления граждан, недобросовестного использования в политической борьбе. Активно раздуваются страхи об утрате конституционного права граждан на тайну волеизъявления в условиях объективной уязвимости инфраструктуры ДЭГ перед кибератаками из-за рубежа или административным вмешательством со стороны национальных властей. В случае с ДЭГ критики этого новшества и оппоненты власти умножают недоверие к избирательной системе на недоверие к современным технологиям вообще. Произведением этой «математической» операции, по их расчётам, должен стать кризис легитимности власти.

Надо сказать, что в мире существует весьма разнообразная практика в сфере электронного голосования: от активного использования технических средств голосования и (или) подсчета голосов на участках до дистанционного голосования через сеть Интернет, от полного отрицания возможности ДЭГ (например, в Германии) [3] до его использования большинством избирателей (например, в Эстонии) [16]. В этом смысле российский опыт успешного внедрения ДЭГ весьма показателен, так как демонстрирует его возможности на выборах разного уровня (местного, регионального, федерального) — в стране с многомиллионным населением, при голосовании в различных часовых поясах, в условиях неприкрытого внешнего давления и попыток вмешательства в суверенный избирательный процесс.

Суммируя возможные «страхи» вокруг ДЭГ, можно выделить следующие блоки аргументов разных исследователей против его внедрения:

1. *Нарушение всеобщности избирательного права и углубление неравенства избирателей ввиду социальной и (или) технической недоступности такого голосования для определенных групп граждан* [12]. Однако ДЭГ не подменяет и не заменяет традиционное голосование, а лишь расширяет возможности голосования для определенных групп населения (молодежи, жителей мегаполисов, маломобильных групп граждан и т.п.) [8, 9]. Напротив, вопреки доводам противников ДЭГ, расширение охвата участников голосования за счет использования электронных форматов соответствует конституционному принципу равенства голосования [2].

2. *Нарушение тайны голосования ввиду технической возможности идентификации волеизъявления конкретных граждан* [10]. Однако высказываемая критика не учитывает современные криптографические методы, которые используются, например, в федеральной системе ДЭГ как для обеспечения тайны голосования, так и для возможности проведения независимой верификации результата подсчёта голосов. Тайна голосования достигается в этом случае фактической невозможностью идентифицировать по заполненному бюллетеню заполнившего его избирателя.

3. *Нарушение принципа гласности (открытости) избирательного процесса.* При ДЭГ якобы не обеспечивается принцип гласности [14]. Однако механизмы общественного контроля за ДЭГ, разработанные и апробированные Общественной палатой Российской Федерации в 2021–2023 годах, свидетельствуют об обратном.

4. *Нарушение принципа достоверности волеизъявления граждан.* Утверждается, что система ДЭГ критически уязвима перед DDoS-атаками, вирусными программами и другими формами целенаправленного вмешательства в избирательный процесс [4]. Не отрицая сам факт серьезности киберугроз, необходимо отметить высокий уровень готовности российской системы ДЭГ к таким угрозам. Так, по информации Председателя ЦИК России, в период проведения выборов с 8 по 10 сентября 2023 года зафиксировано около 30 тысяч атак, направленных на систему ДЭГ [13]. Однако к ощутимым сбоям в ее работе эти атаки не привели.

Задача общественного наблюдения за голосованием вообще и ДЭГ в частности заключается в развенчании этих «мифов». Оно стимулирует внимание и интерес, а также рождает доверие к новым информационным технологиям, применяемым в ходе ДЭГ. Общественные наблюдатели активно и непосредственно противостоят случаям фальсификаций, вбросов непроверенной информации и иным попыткам дискредитации выборов, а также обеспечивают надежную защиту избирательных прав граждан от манипуляций со стороны недружественных внешних сил, транспарентность избирательного процесса.

В практической плоскости общественное наблюдение за ДЭГ должно обеспечить гарантии:

- прозрачности процесса электронного голосования, то есть в применяемой системе не должно быть этапов, на которых даже гипотетически могут происходить абсолютно не фиксируемые наблюдателями манипуляции над бюллетенями;
- безусловного соблюдения тайны голосования, понимаемой применительно к ДЭГ как невозможность идентифицировать по заполненному электронному бюллетеню заполнившего его избирателя;
- независимой проверки корректности подведения итогов голосования [7].

Общественное наблюдение за ДЭГ состоит из «трех контуров» или уровней, а именно:

1) экспертный контур, представленный группой наблюдателей, находящихся непосредственно в помещении территориальной избирательной комиссии дистанционного электронного голосования (ТИК ДЭГ) и имеющих доступ к персональным данным избирателей;
2) технический контур, состоящий из группы наблюдателей в Ситуационном центре Общественной палаты Российской Федерации в Москве, у которых есть возможность получать данные непосредственно с ноды блокчейн в системе ДЭГ по защищенному каналу связи;
3) общий контур, включающий наблюдателей, работающих дистанционно в регионах.

Для первых двух контуров общественного наблюдения за ДЭГ требуется участие специалистов-юристов, обладающих специальными познаниями в области IT, блокчейн-технологий и криптографии. Это позволяет им работать с информацией о формировании цепочек блоков информации в распределенной базе данных программно-технического комплекса ДЭГ. Кроме того, у каждого избирателя, голосующего электронно, есть возможность самостоятельно проверить результаты своего голосования. Таким образом, он выступает одновременно в роли и избирателя и наблюдателя.

Применимость ДЭГ должна обеспечиваться, во-первых, принятием и соблюдением участниками электорального процесса набора определённых процедур, которые являются общепризнанными и составляют основу легитимации власти. Во-вторых, возможностью тщательного независимого анализа (аудита) реализующего функции ДЭГ программного обеспечения. И, наконец, в-третьих, использованием современных криптографических алгоритмов, делающих невозможным незаметное искажение защищаемых данных [11].

Как и в традиционной форме, при голосовании с помощью ДЭГ перед организаторами выборов в полной мере встаёт проблема согласования двух принципов организации выборов: обеспечение тайны голосования и подконтрольности процесса учета голосов (подлинность выборов). Для решения этой проблемы в преддверии выборов, проведенных в ЕДГ 2023 года, был разработан Стандарт общественного наблюдения за ДЭГ [15]. Он представляет собой список (так называемый «чек-лист») из более чем 60 пунктов, включающий всё, что необходимо проверить наблюдателю в ходе голосования, чтобы убедиться, что оно соответствовало требованиям прозрачности, аудируемости и анонимности федеральной системы ДЭГ.

Среди ключевых инструментов общественного контроля необходимо отметить технологию цифрового сейф-пакета (пункт 37 Стандарта) — уникальную разработку, используемую Общественной палатой Российской Федерации с 2021 года. Эта система, автоматически и в реальном времени сохраняющая все происходящие в блокчейне ДЭГ события и сверяющая этот архив с состоянием блокчейна после публикации результатов. Цифровой сейф-пакет позволяет убедиться, что ни один бюллетень не был изменён, добавлен или удалён в ночь между фактическим окончанием голосования и подведением его итогов.

Ещё одна техническая новация общественного наблюдения на выборах (пункты 29–31 Стандарта) относится к возможности проверки избирателем своего собственного бюллетеня. Наблюдатель должен убедиться, что такая функция избирателям предоставлена, и в случае, если в его распоряжении имеется информация о транзакции приёма заполненного бюллетеня (например, если наблюдатель сам участвует в ДЭГ в качестве избирателя либо если кто-то из избирателей предоста-

вил ему такую информацию), что эта проверка проходит успешно: бюллетень действительно присутствует в блокчейне ДЭГ и его цифровая подпись не нарушена. Эту проверку можно осуществить как в ходе голосования, так и после его завершения, поэтому она подтверждает, что заполненный избирателем бюллетень был не только сохранён в блокчейне ДЭГ, но и учтён при подведении итогов.

Для наблюдателей, работающих в регионах, а также наблюдателей из числа активных граждан, желающих проверить результаты своего волеизъявления, такой способ самопроверки транзакции является оптимальным, так как не требует специальных навыков. Для этого достаточно сразу после голосования в федеральной системе ДЭГ сохранить «скриншот» или идентификатор транзакции и проверить его через функцию «наблюдение» на сайте stat.vybory.gov.ru.

По итогам ДЭГ в ЕДГ 2023 года эксперты-криптографы, IT-специалисты, а также представители политических партий положительно оценили как прозрачность и надежность самой процедуры ДЭГ, так и эффективность общественного наблюдения за ним [19]. Единственный технических сбой в работе системы случился на выборах в Ненецком автономном округе (НАО) и был вызван человеческим фактором, а именно некорректностью ввода данных в систему ответственными исполнителями, что было своевременно выявлено наблюдателями. При этом электронное голосование в НАО было приостановлено, внесены необходимые коррективы, после чего все избиратели получили возможность переголосовать в этот же день [20]. В целом, количество специалистов, наблюдавших за ДЭГ на выборах 2023 года, увеличилось со 100 до 200 человек. Растет интерес к наблюдению за ДЭГ среди парламентских партий, представители которых могли наблюдать за выборами на выделенной ноде блокчейна в Общественной палате Российской Федерации и в ТИК ДЭГ.

Среди возможных путей развития ДЭГ будет уместным назвать:

- совершенствование технических средств наблюдения, включая организацию непрерывного общедоступного наблюдения за базой данных блокчейна ДЭГ с использованием механизма веб-сайтов — «зеркал», а также возможность предоставления наблюдателям за ДЭГ доступа к контрольным цифрам голосования с детализацией до конкретных избирательных участков;
- пропаганду ДЭГ в молодежной среде, в том числе, выделение в рамках школьного курса по функциональной грамотности часов для обучения процедурам ДЭГ;
- оптимизацию процедуры назначения наблюдателей за ДЭГ, в том числе возможность регистрации наблюдателей и подачи жалоб и предложений по процедуре через Федеральную государственную информационную систему «Единый портал государственных и муниципальных услуг (функций)» (Госуслуги).

Таким образом, можно утверждать, что дистанционное электронное голосование в России состоялось. Проведение ДЭГ в нашей стране в 2020–2023 гг. позволило добиться необходимого баланса между требованиями общественной безопасности информационных технологий и их удобства для пользователей. Как «стартовый этап» цифровой демократии успех ДЭГ может и должен повлиять на суверенную цифровизацию других сфер общественно-государственных отношений в Российской Федерации, включая создание цифровой системы автоматизированного управления национальными проектами, развитие системы социального казначейства, бережливого здравоохранения и других высокотехнологичных социальных инноваций.

Список литературы

1. Борисов И.Б. На пути к электронной демократии. Цифровые технологии в системе демократического воспроизводства властных институтов // Избирательное законодательство и практика, 2019. — № 3. — С. 3–10.
2. Брод А.С., Булгакова А.В. Развитие института общественного наблюдения в условиях цифровизации избирательного процесса. Доклад Ассоциации «Независимый общественный мониторинг», 2023. — URL: https://nom24.ru/info/events/budushchee-za-deg-v-op-rf-predstavili-doklad-nom-ob-instrumentakh-nablyudeniya-za-

e-golosovaniem/ (дата обращения: 29.09.2023).
3. Выборы в мире: электронное голосование / И.Б. Борисов, А.Г. Головин, А.В. Игнатов; под общ. ред. И.Б. Борисова. М.: Российский общественный институт избирательного права, 2020. — 218 с.
4. Головин А.Г. О некоторых аспектах концепции делегирования власти народом в контексте развития технологий дистанционного электронного голосования // Избирательное законодательство и практика, 2021. — № 2. — С. 3–13.
5. Гонтарь С.Г. Электронное голосование — новая возможность участия граждан в формировании органов власти // Государственная власть и местное самоуправление, 2019. — № 4. — С. 29–33.
6. Данные опроса жителей Москвы, посвященного системе дистанционного электронного голосования (ДЭГ): ВЦИОМ, 30 августа 2021 г. — URL: https://wciom.ru/analytical-reviews/analiticheskii-obzor/distancionnoe-ehlektronnoe-golosovanie-v-moskve (дата обращения: 29.09.2023).
7. ЕДГ-2023: ОП РФ и политические партии объединят усилия в наблюдении за выборами, 10 августа 2023 г. — URL: https://oprf.ru/news/edg2023-op-rf-i-politicheskie-partii-obedinyat-usiliya-v-nablyudenii-za-vyborami (дата обращения: 29.09.2023).
8. Колюшин Е.И. Правовые проблемы дистанционного электронного голосования избирателей // Конституционное и муниципальное право, 2020. — № 2. — С. 25–30.
9. Котикова Д.В. Правовое регулирование дистанционного электронного голосования на выборах депутатов Московской городской Думы: проблемы, их решение и перспективы совершенствования // Государственная власть и местное самоуправление, 2020. — № 5. — С. 22–28.
10. Матренина К.Ю. Принцип тайного голосования при использовании современных информационных технологий // Вестник Тюменского государственного университета, 2014. — № 3. — С. 206–211.
11. Ниточкин Ф.В. Проблема легитимности в политико-правовых учениях и избирательное право // Гражданин. Выборы. Власть. 2023. — №2(28). — С. 29–37.
12. Овчинников В.А., Антонов Я.В. Правовая структура электронного голосования в системе электронной демократии // Российская юстиция, 2016. — № 5. — С. 5–8.
13. Памфилова рассказала о хакерских атаках на ресурсы избирательной системы, 10 сентября 2023 г. — URL: https://ria.ru/20230910/vybory-1895409867.html (дата обращения: 29.09.2023).
14. Садекова Г.У., Токарева Е.А. Перспективы развития электронного голосования: совершенствование законодательства в условиях сближения международного и внутригосударственного права // Государственная власть и местное самоуправление, 2011. — № 4. — С. 28–32.
15. Стандарт общественного наблюдения за ДЭГ. — URL: https://files.oprf.ru/storage/documents/standart-deg-21072023.pdf (дата обращения: 29.09.2023).
16. Федоров В.И. Дистанционное электронное голосование и явка избирателей: опыт Эстонии и Москвы // Избирательное законодательство и практика, 2019. — № 4. — С. 37–42.
17. Чумаков В.А., Сейранян Г.А. «Жизнь в онлайн-эпоху: новые вызовы и поиск решений» как тема российского председательства в МАЭССИ в 2021-2023 годах // Новое индустриальное общество второго поколения (НИО.2): проблемы, факторы и перспективы развития в современной геоэкономической реальности (СПЭК-2022) / Под общ. ред. С.Д. Бодрунова. М.: ИНИР им. С.Ю. Витте, 2022. — С. 576–583.
18. «Это генеральная репетиция перед 2024 годом» — мнение экспертов о предстоящем ЕДГ: Независимый общественный монито-

ринг, 27 июля 2023 г. — URL: https://nom24.ru/info/events/eto-generalnaya-repetitsiya-pered-2024-godom-mnenie-ekspertov-o-predstoyashchem-edg/?ysclid=lmitsqnsey338703138 (дата обращения: 29.09.2023).
19. Предложения наблюдателей за ДЭГ проработает специально созданная в ОП РФ группа, 26 сентября 2023 г. — URL: https://oprf.ru/news/predlozheniya-nablyudateley-za-deg-prorabotaet-spetsialno-sozdannaya-v-op-rf-gruppa (дата обращения: 29.09.2023).
20. В Ненецком АО решили проблему с дистанционным голосованием, 09 сентября 2023 г. — URL: https://tass.ru/politika/18692605 (дата обращения: 29.09.2023).

Е.А. Дербин
Профессор кафедры «Информационная безопасность» МГТУ им. Н.Э. Баумана, доктор военных наук

ОБ АКТУАЛЬНОЙ ТРАНСФОРМАЦИИ ДУХОВНЫХ ЦЕННОСТЕЙ В ОБЩЕСТВЕННОМ СОЗНАНИИ И ПУТЯХ ИХ СОХРАНЕНИЯ В УСЛОВИЯХ ГЛОБАЛЬНОГО ИНФОРМАЦИОННОГО ПРОТИВОБОРСТВА И ВОЙН НОВОГО ТИПА

Духовные ценности человека и общества в ускоряющейся глобализации стали определяющим условием дальнейшего развития человеческой цивилизации, а их деградация как результат разрушительных процессов войн нового типа — важнейшим фактором ее упадка.

Ключевые слова: информационная опасность, угрозы информационной безопасности общества и личности, духовные ценности, мировоззрение.

Современное состояние мировой цивилизации характеризуется обострением борьбы неоглобалистов за свое господство в «новом мировом порядке», воздвигаемом ими войнами нового типа и кризисами. При этом одним из основных инструментов (оружием) в этой борьбе становятся технологии перевода общественного сознания из режима созидания и творчества во имя будущего человечества — на основе высоких этических норм — в режим материального потребления в условиях распространения идеологии неолиберализма, трансгуманизма и технологии цифровизации сфер человеческой деятельности и жизни (схема на рисунке 1).

Развитие информационных, сетевых и программных технологий привело к осознанию возможности создания новой мощнейшей системы управления человеческим сознанием, управления государственными, военными, научными, исследовательскими, финансовыми и другими системами завоевания господства в мире. В настоящее время передача потоков информации в системе управления мировыми финансами и информационное воздействие на народонаселение Земли осуществляется посредством сети Интернет.

За последние годы в социальных коммуникациях произошли значительные изменения, связанные с внедрением и развитием трансгуманистических технологий искусственного интеллекта. Данные технологии находят свое применение во всех аспектах человеческой деятельности, в том числе как инструмент вредоносной деформации общественного сознания, где определяющую роль играют ценностные системы человека и социальных групп.

Целью данной статьи является постановка проблемы трансформации духовных ценностей в общественном сознании.

При этом под сущностью ценности далее предполагается: а) положительная или отрицательная значимость объектов окружающего мира для человека, социальных групп и общества в целом, определяемая, в основном, не их свойствами, а вовлеченностью в сферу потребностей и интересов жизнедеятельности; б) критерии и способы оценки этой значимости, выраженные в этических принципах, нормах, идеалах, установках и целях.

Следует отметить, что сравнение цивилизационных этических парадигм Запада и Востока (рисунок 2) позволяет сделать вывод об их диаметральной сущностной и смысловой противоположности и антагонистическом характере.

Президент России В. Путин в своей речи на церемонии подписания договоров о вступлении ЛНР, ДНР, Запорожской и Херсонской областей в состав России заявил, что диктатура западных элит направлена против всех обществ, в том числе и народов даже самих западных стран. Он назвал подобное поведение вызовом всем: «… Такое полное отрицание человека, ниспровер-

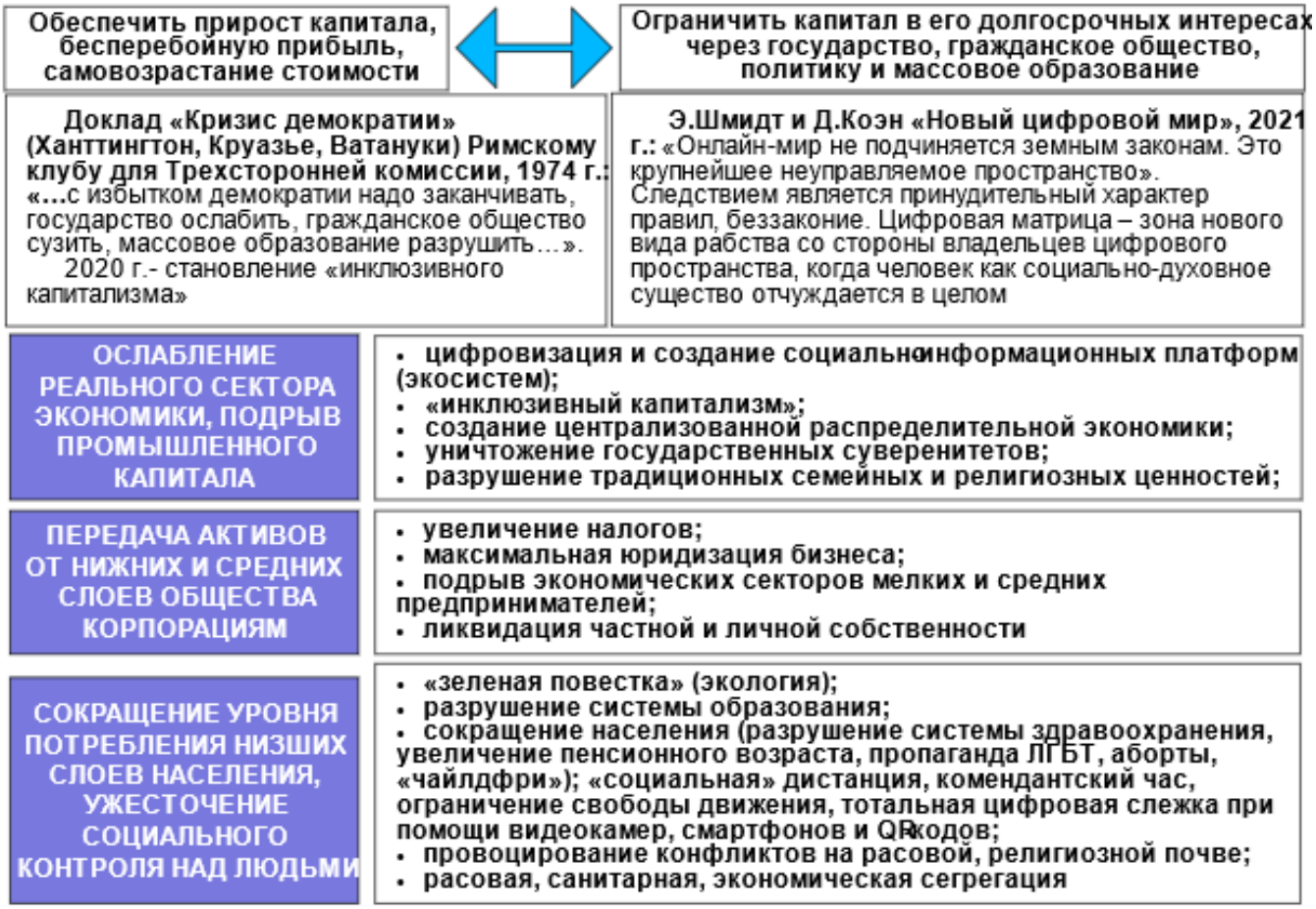


Рисунок 1. Факторы разрушительной трансформации духовных ценностей в условиях расширения глобализационных процессов.

жение веры и традиционных ценностей, подавление свободы приобретают черты религии наоборот — откровенного сатанизма…»[1].

Следует утверждать при этом, что субъекты противоборствующей с Россией системы сатанистских ценностей обладают, прежде всего, мощной функцией контроля над общественным сознанием с эффективными технологиями нейросетей, фактически представляющими оружие воздействия на человека, одновременно предполагающее производственный комплекс совершенного телекоммуникационного оборудования, а также научноисследовательских учреждений, занимающихся разработкой разрушительных идеологий и технологий.

Оценка остроте данной угрозы дана 9 ноября 2022 г. в Указе Президента РФ № 809 «Об утверждении Основ государственной политики по сохранению и укреплению традиционных российских духовнонравственных ценностей» [1].

Действительно, целью продвижения глобализации является построение нового мирового порядка по типу «инклюзивного» капитализма с депопуляцией, установлением режима подавления и ограничения свободы человеческого сообщества в мировом «цифровом» концлагере.

Глобализационная экспансия нового типа как форма покушения на национальную безопасность, в первую очередь, через угрозы информационной безопасности обществу[2], состоит в создании чрезвычайной ситуации через подавление населения низким уровнем

1 https://tvzvezda.ru/news/20229301553-ZBgEP.html

2 Здесь — информационная опасность обществу — потенциальный вред информации в общественном сознании и коллективном бессознательном, способности социальных объектов к развитию, повышению просвещенности и образованности, их возможностям по нейтрализации деструктивного информационного воздействия, когда вероятность и размеры вреда могут превышать допустимый уровень. Вред обществу заключается в таком ущербе, как утрата социальными группами своей идентичности и возможностей (нарушение структурной це-лостности общества — деструкция, дезорганизация; нарушение духовной целостности общества — дисфунк-ция; перепрограммирование общественного сознания в целеполагании, смысловом образовании, ценностях; утрата ресурсов (исторической памяти, опыта, знаний и пр.); нарушение (разрыв) системных связей — дезор-ганизация; потеря способности общества к развитию; распад общества.

Рисунок 2. Цивилизационный антагонистический конфликт этических позиций Запада и Востока.

жизни, страхом экологических, эпидемиологических, климатических и пр. изменений; в деградации национального образования и науки, культуры и здравоохранения; в развращении общественного сознания либеральными идеями и ценностями, чуждыми национальным, в форме создания условий различного рода чрезвычайных ситуаций типа «пандемии» одновременно в нескольких сферах со специфическим своим содержанием и направлениями реализации в каждой из них (схема на рисунке 3):

- в информации коллективного и индивидуального бессознательного и мировоззренческой (индивидуального и коллективного сознания) — подмена цели и смысла жизни человека и человечества: от трансцеденции человека в «Богочеловека», согласно И. Канту, или в «Человека» с большой буквы — к «квалифицированному потребителю», «человеку служебному», к «человеку цифровому» через трансгуманизм и расчеловечивание;
- в информации областей мировоззренческой и профессиональноприкладной деятельности — распространение и закрепление либеральной идеологии; разрушение суверенных государственных экономик и установление реального экономического и политического господства над миром владельцев транснациональных кланов и корпораций; переход от методов военнополитического влияния к санкционному экономическому шантажу и изоляции; применение военной силы переводится в информационную сферу: кибервторжения в системы управления, установление контроля над органами управления всех уровней и видов; глобальное информационнопсихологическое воздействие на общественное сознание с целью разжигания страха, добровольного отказа от контроля за соблюдением норм международного права, прав человека, традиционных национальных норм социальных отношений и приучения покорности насилию;
- в области информации повседневных отношений и быта — к доминированию

Рисунок 3. Объекты трансформации духовных ценностей.

материальных потребностей над духовными и потребительству.

К сущностным признакам духовных ценностей обычно относят следующие:

- духовные ценности выходят за рамки конкретных действий и ситуаций;
- духовные ценности как категория этики, не могут устанавливаться нормативно;
- существует тесная органическая связь с историческими, этноконфессиональными и культурными святынями и ценностями;
- отсутствуют противоположности и противоречия на различных уровнях деятельности обладателя духовных ценностей;
- ценности устойчивы к изменениям в масштабе общественноэкономической формации и жизни поколения;
- ценности соотносятся не с истиной, а с представлениями об идеале;
- ценности непосредственно связаны с целями и смыслами жизни и деятельности;
- духовные ценности непродажны и необменяемы с другими ценностями, предлагаемыми в зависимости от конъюнктуры материальных потребностей;
- ценности служат стандартами или критериями, определяют выбор или оценку действий, установки людей и событий;
- ценности проникают в сознание, когда действия или суждения, с которыми мы сталкиваемся, имеют противоречивый характер для разных ценностей, которыми мы дорожим;
- ценности образуют упорядоченную систему приоритетов, характеризующих личность, и лежат в основе всех действий, которые она выбрала;
- ценности нельзя окончательно опровергнуть или принять и др. [3,4,5]

В любых формах противодействия внедрению чуждых ценностей и в интересах формирования личности гражданина (схема на рисунке 4), следует учитывать, вопервых, положения этики и традиционной бытовой морали, традиции религии (теологии и обыденного верования), основы политического

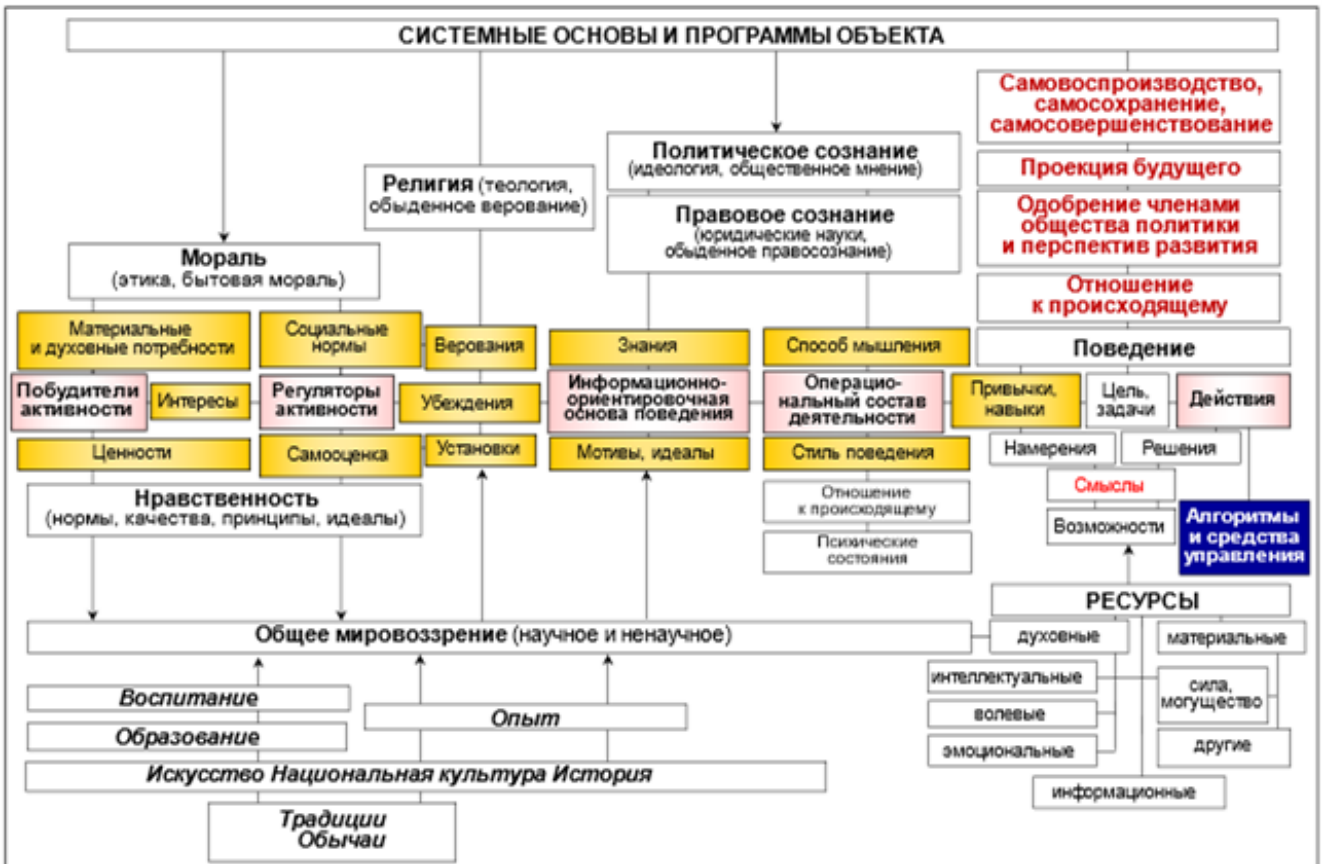


Рисунок 4. Условия формирования духовных ценностей, их трансформации и влияния на поведение социальных объектов.

(идеологии и общественного мнения) и правового сознания (требований юридической науки и обыденного правосознания), а также содержание общего мировоззрения общества (как научного, так и ненаучного), вовторых, условия общественного развития: традиции, обычаи, достижения национальной культуры, искусства, исторический базис, а также воспитание, образование и опыт общественного строительства.

При этом целями формирования гражданского общества, отражаемыми в национальной идее развития России, могут быть самовоспроизводство, самосохранение и самосовершенствование народов России.

Возможная и, как представляется, достаточно подробная классификация ценностей представлена на рисунках 5 и 6 [4,5].

Основные направления деформации духовных ценностей представлены на рисунке 7.

Актуальными приемами и методами деформации индивидуальных духовных ценностей человека в профессиональноотраслевой и бытовой сферах деятельности могут считаться: принуждение к бессмысленной работе, введение взаимоисключающих правил, введение коллективной ответственности, формирование состояния неопределенности (незнания наверняка, каково положение и чего ждать), суровые дисциплинарные меры и обещание доброго отношения, доведение противоречивых новостей, формирование психологического или физического стресса и его искусственное снятие и др.

Структурное изложение условий и факторов деградации духовных ценностей в коллективном сознании представлено в схеме на рисунке 8, а пути нейтрализации опасностей духовным ценностям — в схеме на рисунке 9 [2].

Концентрированным выражением системы традиционных духовных ценностей России может являться ее национальная идея (схема на рисунке 10).

С учетом вышеизложенного, противостоять глобальному разрушительному воздействию на духовные ценности общества России возможно путем работы государства и общества в таких направлениях, как:

1. Мобилизация общественного сознания:
   - признание существования геополитических перманентных враждебных действий со стороны «антицивилизации»;

1. ЦИВИЛИЗАЦИОННЫЕ ЦЕННОСТИ

- жизнь человека, сохранность культур и сфер жизни человека

2. ГЛАВНЫЕ ЦЕННОСТИ ЖИЗНИ ЧЕЛОВЕКА

- любовь (к Богу, к ближнему, к себе, к Родине, к природе);
- самовоспроизведение (продолжение рода);
- здоровье (нравственное, физическое, психическое;)

3. ДУХОВНЫЕ ЦЕННОСТИ

3а) по уровням влияния на государственное и социальное управление

- **традиционные ценности**– нравственные ориентиры, формирующие мировоззрение граждан России, передаваемые из поколение в поколение, лежащие в основе общероссийской гражданской идентичности и единого культурного пространства страны… К традиционным ценностям относятся жизнь, достоинство, права и свободы человека, патриотизм, гражданственность, служение Отечеству и ответственность за его судьбу, высокие нравственные идеалы, крепкая семья, созидательный труд, приоритет духовного над материальным, гуманизм, милосердие, справедливость, коллективизм, взаимопомощь и взаимоуважение, историческая память и преемственность поколений, единство народов России;
- **универсальные** («общечеловеческие») традиционные: социально-политические и нравственные принципы, разделяемые большинством населения мирового сообщества; идеалы, общенародные цели и основные средства их достижения; природные ценности и ценности, которые имеют глобальный характер: проблемы сохранения мира, разоружения , международного экономического порядка и др.: нормы, свобода, любовь, мир, жизнь, справедливость, «золотое правило нравственности», свет, радость;
- **Европейские либеральные** (общность исторической судьбы и наследия народов Запада; право наций на самоопределение; парламентаризм, демократическое устройство государства и общества, особенно прав меньшинств; верховенство права, правовая культура; рыночная экономика, базирующуюся на частной собственности; социальная справедливость; приоритет прав человека, суверенитета личности над государственным, либеральный индивидуализм; светскость общества и культуры, основанную на христианском наследии; толерантность и мультикультурализм, гедонизм и пр.);
- **национальные политические** (национальная безопасность. правовые и пр.)
- **социально-политические** (национально -этнические, религиозные; родовые, семейные, корпоративные, партийные);
- **моральные** (добро и зло, патриотизм, долг, трудолюбие, честь, добросовестность, достоинство, человеколюбие, справедливость, искренность, уважение к старшим);
- **нравственные** (психологические, экзистенциальные и пр.) – гармония, сбалансированность, умиротворение, соответствие; саморегуляция,
- **эстетические** (прекрасное, возвышенное, трагическое, комическое, безобразное); PR-ценности (свобода, комфорт, безопасность, деньги, секс, семья, дружба, вера, результат, стремление к познанию, тайна, статус, профессионализм и пр.)

3б) по уровням обобщения информации и взаимосвязям в общественном сознании и в социальных отношениях

- **мировоззренческие** (религиозные, этнические, конфессиональные, идеологические, культурные и пр.) ;
- **научные** (биомедицинская этика, исторические, этические и пр.)
- **профессиональные** (власть, компетентность; мастерство, корпоративные и пр.);
- **повседневной жизни и бытовыхсоциальных отношений, индивидуальные и коллективно-групповые, межличностные и внутриличностные** (отношения с другими и переживания; рефлексия страданий и пр.)

4. МАТЕРИАЛЬНЫЕ ЦЕННОСТИ

Рисунок 5. Духовные ценности в системе цивилизационных ценностей

1. **Качества человека, характеризующие отношение к Богу**: - благочестивый, почитающий Бога; - веротерпимый, терпимый к чужой вере, признающий ее право на свободное существование и т.д.

2. **Качества, характеризующие отношение к другим людям**: - альтруистичный, готовый бескорыстно действовать на пользу другим, не считаясь со своим личным интересом; - великодушный, обладающий высокими душевными качествами, снисходительный к другим до готовности пожертвовать своими интересами; величие души, соединенное с разумом и т.д.

3. **Качества, характеризующие отношение к добру и злу**: - благородный, чувствующий добро и отвечающий тем же; восприимчивый к добрым делам и словам; - добродетельный, высоконравственный, проявляющий добродетель; - добрый, делающий добро другим, отзывчивый; - милостивый, не помнящий зла, отвечающий добром.

4. **Интеллектуальные качества** : - дальновидный, предусматривающий последствия; - даровитый, обладающий способностями, талантом; - здравомыслящий, обладающий здравым рассуждением и т.д.

5. **Качества, характеризующие отношение к труду**: - активный, деятельный, энергичный; - действенный, активный; - деятельный, энергичный; - добросовестный, честно выполняющий свои обязательства, обязанности; - исполнительный, выполняющий порученное дело и т.д.

6. **Бойцовские качества** : - воинственный, обладающий воинским духом; - доблестный, отважный, мужественный, самоотверженный в работе; - жизнеспособный, способный к выживанию в различных условиях.

7. **Качества, характеризующие отношение к собственности**: - бережливый, бережно относящийся к имуществу, расчетливый, экономный; - бескорыстный, не видящий цели жизни в наживе, в приобретении; - умеренный, довольствующийся немногими благами и т.д.

8. **Качества, отношение к Родине и государству** : - верный, стойкий и неизменный в своих чувствах, отношениях, в исполнении обязанностей, долга; - державный, стремящийся к укреплению государства, державы; - патриотичный, проникнутый любовью к родине.

9. **Волевые качества** : - волевой, преодолевающий препятствия на пути к благу, поставленной цели; - выдержанный, способный следовать правильному суждению, терпеливый в печали; - обязательный, исполняющий порученное, взятое обязательство; - терпеливый, способный перенести различные тяготы во имя долга и веры.

10. **Эмоциональные качества**: - веселый; - воздержанный, обладающий умеренными страстями; - жизнеутверждающий, проникнутый оптимистическим отношением к жизни и т.д.

11. **Качества, характеризующие осознание самого себя**: - гордый, исполненный чувства собственного достоинства, сознающий свое превосходство; - самобытный, не похожий на других, идущий своим путем; - самодовлеющий, достаточно значительный сам по себе.

12. **Качества, характеризующие свободолюбие**: - вольный, свободный, независимый, свободолюбивый; - самостийный, независимый, самостоятельный; - свободолюбивый, стремящийся к независимости во всем, стремящийся жить по- своему; независимый в действиях и мыслях

Шадриков В.Д. «Происхождение человечества».С.53-58

Рисунок 6. Классы духовных качеств человека

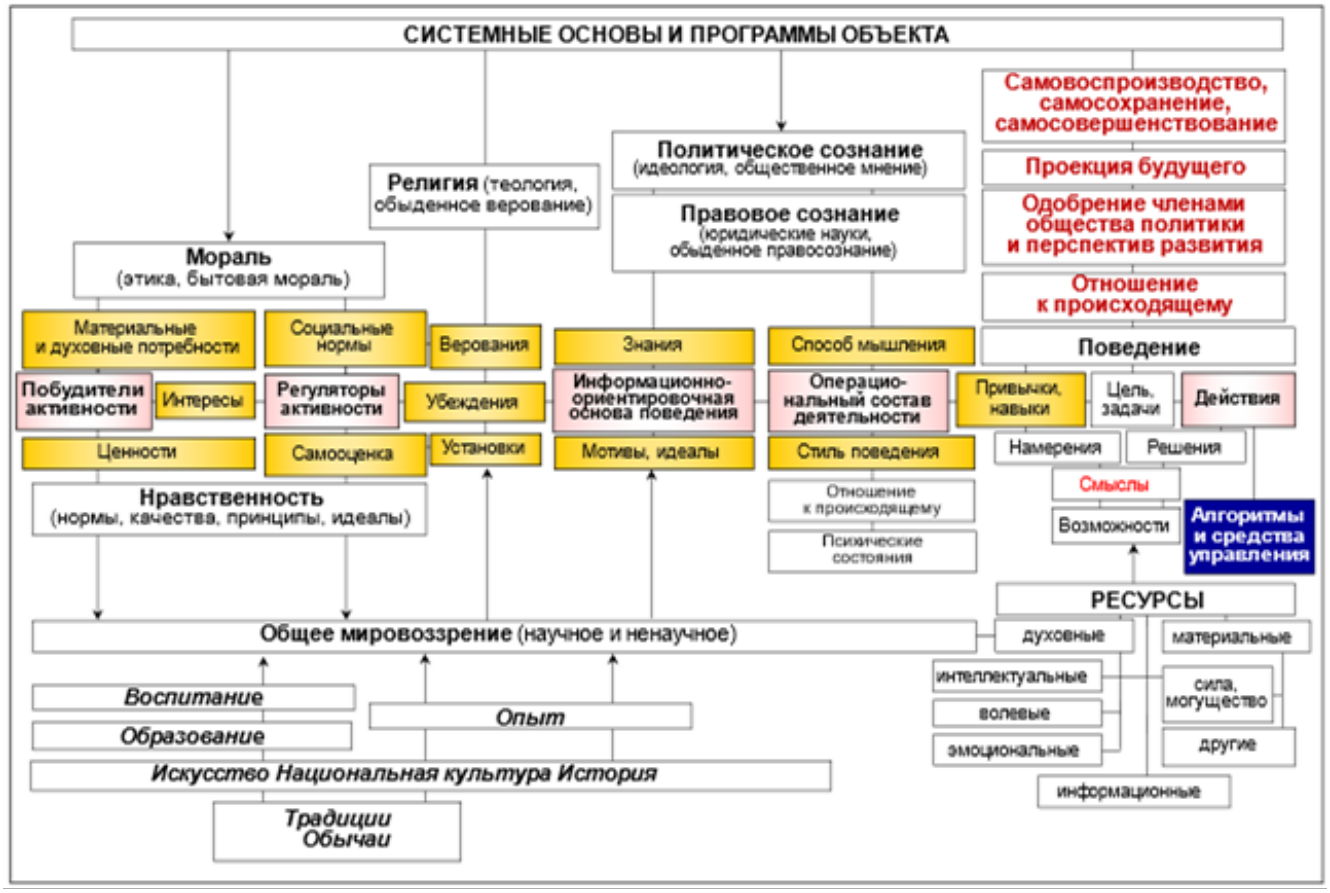


Рисунок 7. Направления деформации духовных ценностей.

- возрождение приоритета и ценности производительного труда, поддержание национальной идеологии;
- предъявление требований к гражданам по исполнению должностных и социальных обязанностей и обязательств согласно праву и этике;
- обеспечение приоритета духовного над материальным;
- следование национальным традициям и поддержание национальной культуры;
- формирование в общественном сознании цельной исторической и культурной картины мира, восстановление подлинного исторического знания, вскрытие и обнародование реальных смыслов ключевых постулатов западной цивилизационной модели и ее идеологической основы с последующим предложением иных смыслов; развитие национальных философских и идеологических школ;
- осознание наличия транснациональной олигархии как субъекта геополитики, выявление ее реальных интересов, реализуемых посредством мировых политических и экономических институтов;
- отказ от представлений о рыночной экономике как о всемогущем социальном регуляторе, в том числе по причине ее моральнонравственной непригодности;
- пересмотр соотношения личностных и надличностных ценностей, интересов, взаимных прав и ответственности государства, бизнеса, общества и личности с целью формирования системы общественных соглашений, принимаемых большинством населения;
- взращивание понятия духовности как базовой ценности общества.

2. Развитие научного знания:

- формирование цельной исторической и культурной картины мира с учетом приоритета духовных ценностей над материальными, восстановление подлинного исторического знания, анализ ошибок и отказ от дезинформации общества;
- восстановление отечественной экономической научной школы;
- возрождение отечественной науки и системы образования;
- проведение отечественных научноприкладных работ по вопросам моделиро-

1. **Качества человека, характеризующие отношение к Богу**: - благочестивый, почитающий Бога; - веротерпимый, терпимый к чужой вере, признающий ее право на свободное существование и т.д.

2. **Качества, характеризующие отношение к другим людям**: - альтруистичный, готовый бескорыстно действовать на пользу другим, не считаясь со своим личным интересом; - великодушный, обладающий высокими душевными качествами, снисходительный к другим до готовности пожертвовать своими интересами; величие души, соединенное с разумом и т.д.

3. **Качества, характеризующие отношение к добру и злу**: - благородный, чувствующий добро и отвечающий тем же; восприимчивый к добрым делам и словам; - добродетельный, высоконравственный, проявляющий добродетель; - добрый, делающий добро другим, отзывчивый; - милостивый, не помнящий зла, отвечающий добром.

4. **Интеллектуальные качества** : - дальновидный, предусматривающий последствия; - даровитый, обладающий способностями, талантом; - здравомыслящий, обладающий здравым рассуждением и т.д.

5. **Качества, характеризующие отношение к труду**: - активный, деятельный, энергичный; - действенный, активный; - деятельный, энергичный; - добросовестный, честно выполняющий свои обязательства, обязанности; - исполнительный, выполняющий порученное дело и т.д.

6. **Бойцовские качества** : - воинственный, обладающий воинским духом; - доблестный, отважный, мужественный, самоотверженный в работе; - жизнеспособный, способный к выживанию в различных условиях.

7. **Качества, характеризующие отношение к собственности**: - бережливый, бережно относящийся к имуществу, расчетливый, экономный; - бескорыстный, не видящий цели жизни в наживе, в приобретении; - умеренный, довольствующийся немногими благами и т.д.

8. **Качества, отношение к Родине и государству** : - верный, стойкий и неизменный в своих чувствах, отношениях, в исполнении обязанностей, долга; - державный, стремящийся к укреплению государства, державы; - патриотичный, проникнутый любовью к родине.

9. **Волевые качества** : - волевой, преодолевающий препятствия на пути к благу, поставленной цели; - выдержанный, способный следовать правильному суждению, терпеливый в печали; - обязательный, исполняющий порученное, взятое обязательство; - терпеливый, способный перенести различные тяготы во имя долга и веры.

10. **Эмоциональные качества**: - веселый; - воздержанный, обладающий умеренными страстями; - жизнеутверждающий, проникнутый оптимистическим отношением к жизни и т.д.

11. **Качества, характеризующие осознание самого себя**: - гордый, исполненный чувства собственного достоинства, сознающий свое превосходство; - самобытный, не похожий на других, идущий своим путем; - самодовлеющий, достаточно значительный сам по себе.

12. **Качества, характеризующие свободолюбие**: - вольный, свободный, независимый, свободолюбивый; - самостийный, независимый, самостоятельный; - свободолюбивый, стремящийся к независимости во всем, стремящийся жить по- своему; независимый в действиях и мыслях

Шадриков В.Д. «Происхождение человечества».С.53-58

Рисунок 9. Пути нейтрализации опасностей духовным ценностям в коллективном сознании

Рисунок 10. Национальная идея как концентрированное выражение системы традиционных духовных ценностей.

вания и прогнозирования этнокультурных взаимодействий и социальнополитических процессов, внедрение их результатов в практическую деятельность органов государственного управления;

- отказ от блокирования и расширение исследований в области нематериального мира, отражаемого аспектами религиозной философии и теософии.

3. Просвещение и образование граждан:

- ревизия содержания вузовских и школьных общественных дисциплин в контексте их роли в формировании системы смыслообразующих ценностных ориентиров, сохранении социокультурного архетипа народа и запуска социальнопсихологических механизмов его самосохранения, следования национальным традициям и поддержания национальной культуры;
- формирование духовного мировоззрения у населения; формирование адекватного понимания рамок применимости научного подхода как способа познания и осмысления действительности, пересмотр стереотипов технократического и антропоцентрического мышления с последующим предложением модели развития, предполагающей сохранение природной среды обитания.

4. Развитие духовности граждан России:

- обращение просвещения и воспитания людей — как молодежи, так и достаточно взрослых людей — к приоритету этическим, духовнонравственным ценностям над утилитарными;
- разъяснение раннехристианских представлений о любви и вере, исключая при этом религиозную, формальную догматику, смешанную с современными тенденциями распространения в массовой культуре пропаганды открытого сатанизма и богоборчества;
- реализация подхода к построению стратегии обеспечения общественной безопасности, связанного с выработкой мер блокирования деятельности деструктивных социальных групп.

5. Совершенствование государственной информационной политики.

Совокупность предлагаемых мер укрепления традиционных духовных ценностей обеспечит создание условий для гармонизации общества, поддержания высокой ответственности Российского государства и его граждан

в деле противостояния «новому мировому порядку» и самосохранения в условиях продвигающейся глобализации в войнах нового типа.

Литература:

1. Указ Президента Российской Федерации 9 ноября 2022 г. № 809 «Об утверждении основ государственной политики по сохранению и укреплению традиционных российских духовно-нравственных ценностей».
2. Анисимов О. С. Культура и духовность в мышлении стратега. — М., 2012, — 745 с.
3. Бочкарев А.И. Девальвация общечеловеческих ценностей в среде двойных стандартов, 2023, https://cyberleninka.ru/article/n/devalvatsiyaobschechelovecheskihtsennosteyvsrededvoynyhstandartov.
4. Бочкарев А.И. Фундаментальные основы этногенеза: учебное пособие для вузов. — М.: Флинта, 2008. — 464 с.
5. Шадриков В.Д. «Происхождение человечества». — М.: 2022, С. 53–58.

В.Б. Титов
Доктор педагогических наук, профессор, Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации (РАНХиГС)

МЕЖДУНАРОДНАЯ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ПРОЦЕССНОЕ УПРАВЛЕНИЕ ОБРАЗОВАНИЕМ

Международная проблема

В конце XX века переход российской национальной экономики к геоэкономической модели развития сопровождался стремлением западной постиндустриальной цивилизации подчинить эксплуатацию российских ресурсов требованиям функционирования транснациональных корпораций. Ими была сформирована надгосударственная воспроизводственная система. Характерной чертой исторического этапа стал переход от управления в интересах государств-наций к управлению в интересах глобальных сетевых структур. Карта мира перекраивалась не по политическим, а по экономическим границам. Борьба развернулась не только за энергетические и сырьевые, но прежде всего за людские и интеллектуальные ресурсы. В России в образовательной сфере был запущен Болонский процесс, позволивший манипулировать понятием «профессиональная мобильность». Он способствовал исходу из стран СНГ высококвалифицированных специалистов в экономикообразующих наукоемких отраслях, таких как атомная и космическая.

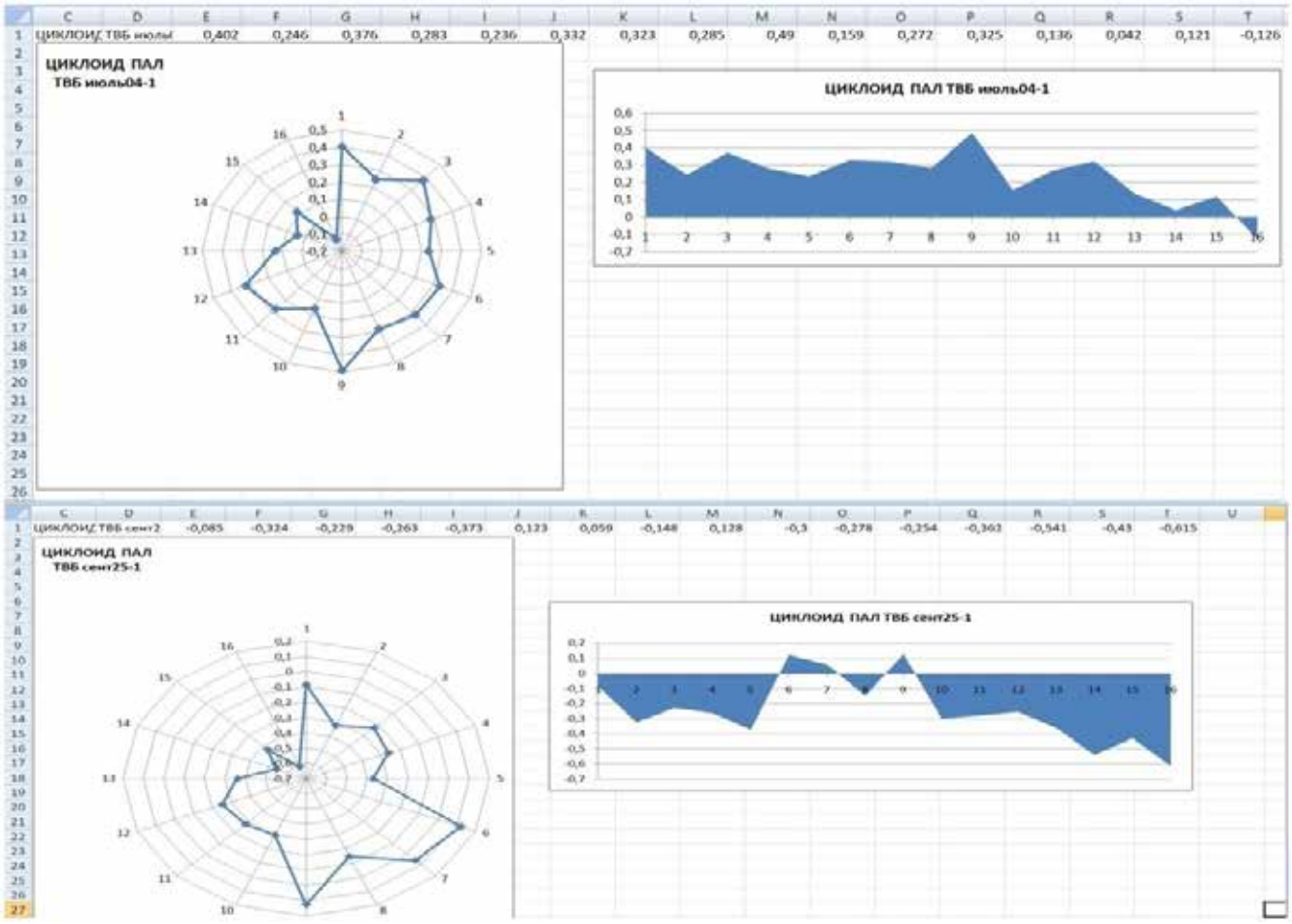
Научная проблема

В сфере образования, как это и принято в программах Международного валютного фонда, активно внедряются и методы проектного управления, и методы процессного управления. Так как проектное управление предполагает реализацию системы международных норм, результатом внедрения проектного управления в образовании стало создание на их основе национальной систем профессиональных стандартов, федеральных государственных образовательных стандартов. Но практика последовательно сменяемых каждые несколько лет ФГОС проявила неготовность научной педагогической общественности работать с понятием «владение» — одним из основных понятий теории обучения и теории воспитания. Это привело к искаженной трактовке уровней обученности и воспитанности, исказило информационные потоки системы образования при процессном управлении.

Будучи результатом соединения навыка и свойств личности обучаемого, «владение», в силу сложности измерения и оценивания, оказалось для большинства сфер деятельности ненаблюдаемым. Поэтому, в результате либо слабой развитости, либо отсутствия психологических и педагогических методов и объективных средств диагностики формируемых компетенций, образовательный процесс в государстве-мишени имеет высокую опасность нерегламентированных воздействий на обучаемых. Для этого сегодня разработан широкий спектр деструктивных педагогических технологий, выдаваемых за новое слово в педагогике. В условиях не ограниченных ни одной из форм ответственности, такие технологии позволяют, помимо снижения качества образования, формировать базы данных о трудовом потенциале и состоянии социума в реальном масштабе времени.

Научная задача

Обосновать потребность в использовании для обеспечения международной информационной безопасности (МИБ) в гуманитарной



1 — интравертированный нестабильный (Ц), 2 — экстравертированный стабильный (Э), 3 — экстравертированный нестабильный (И), 4 — интравертированный стабильный (Ш); 5, 6, 7, 8 — норма, соответственно: Ц, Э, И, Ш; 9, 10, 11, 12 — пограничная аномальная личность (ПАЛ): Ц ПАЛ, Э ПАЛ, И ПАЛ, Ш ПАЛ; 13, 14, 15, 16 — патологическая психологическая конституция (ППК): Ц ППК, Э ППК, И ППК, Ш ППК.

сфере психофизиологически обоснованной методологии шкалирования традиционных, а именно человеческих, ценностей.

Разрабатывается процедура интегральной оценки человека в пространстве состояний. Результат процедуры должен характеризовать обучаемого одновременно и как субъекта деятельности, и как личность, и как индивида. Это формирует в системе образования свойство управляемости педагогическими рисками. При использовании таких методов процессного управления в образовании появится возможность сопоставлять педагогические инновации с традиционными человеческими, национальными и духовными ценностями на основе этики и эстетики, традиции и гармонии.

Модель человека представляется в виде иерархически-сетевой системы стандартных шкал, имеющих единый физиологический смысл адаптации и приспособления. С позиций системного подхода каждой шкале соответствует своя функциональная система. Физиологический смысл шкалы заключается в том, что она количественно отражает степень напряжения функциональной системы организма, оцениваемого на основе показателей «ритм» и «симметрия». Ритм — повторение подобного через равные промежутки времени, симметрия — повторение в пространстве.

Такая целостная система шкал отражает устойчивую, реально существующую структуру связей, свойственную единой системе «организм — среда». Отличительной особенностью показателей шкал является их внутренняя взаимосвязанность и однородность, что позволяет при измерениях оперировать не с абсолютной погрешностью, а с относительной.

Временные структуры, получаемые с использованием динамической акупунктуры (аку-

пунктурографии), характеризуют системные реакции организма (системокванты деятельности), функциональное состояние, адаптоспособность, работоспособность и уровень профессионализма человека, порождающие профессиональную надежность.

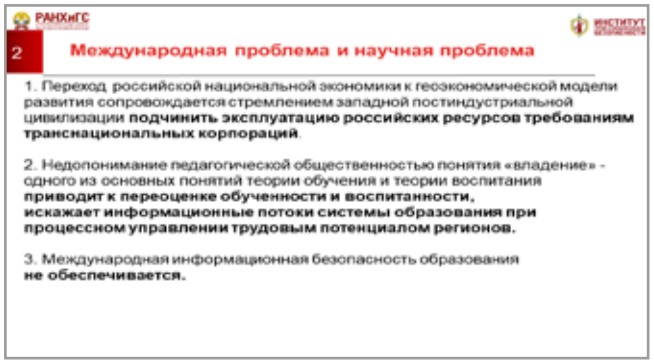
Шкалы, используемые для оценки функционального состояния, адаптоспособности и работоспособности, по способу получения делятся на группы, в зависимости от изучаемой акмеологической иерархии: индивид — личность — субъект деятельности — индивидуальность.

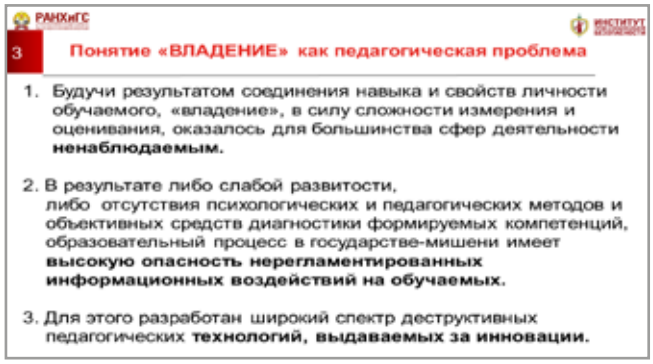
Оценка результата педагогического воздействия предполагает три этапа: 1-й этап — изучение напряженности функциональных систем. Оценка ритма. 2-й этап — сравнительный анализ измерений по БАТ. Оценка симметрии. 3-й этап — изучение системоквантов деятельности, связности системы физиологических процессов организма. Оценка владения как целостной совокупности навыка, опыта и свойств личности.

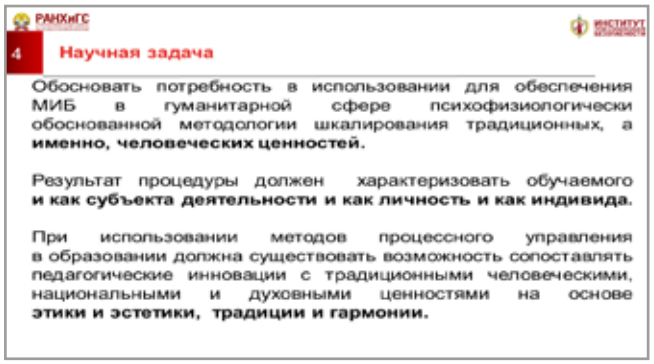
С использованием методов искусственного интеллекта на основе единого психофизиологического показателя адаптации строится пространство из 16 состояний, часть из которых являются запрещенными.

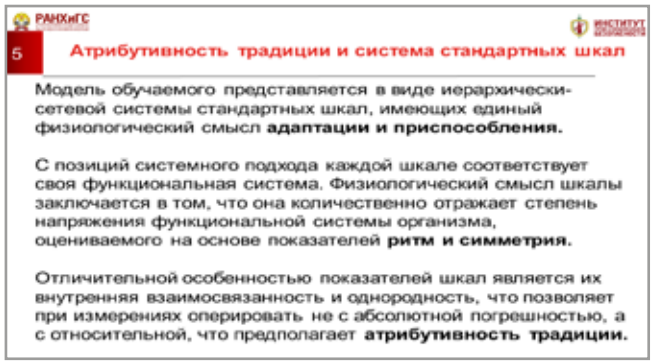
На рисунке представлены примеры вероятностной оценки результата педагогического воздействия по 16 шкалам в терминах клинической психологии.

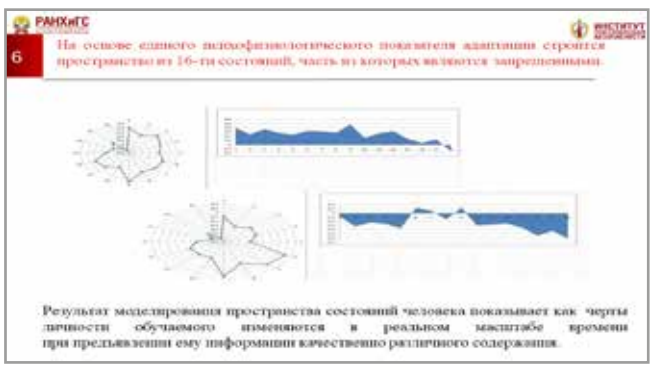
Результат моделирования пространства состояний человека показывает, что черты личности обучаемого изменяются в реальном масштабе времени при предъявлении ему информации качественно различного содержания.

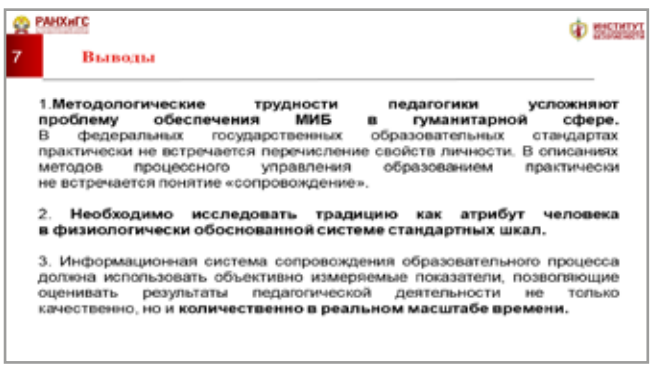












Выводы

1. В федеральных государственных образовательных стандартах практически не встречается перечисление свойств личности. В описаниях методов процессного управления образованием практически не встречается понятие «сопровождение». Эти теоретические трудности усложняют проблему обеспечения МИБ в гуманитарной сфере.
2. Под воздействием объективных обстоятельств сегодня формируется реакция мировой общественности на сформировавшуюся систему наднациональных механизмов управления внутренними политическими и социально-экономическими процессами в национальных государствах. Именно поэтому информационная система сопровождения образовательного процесса должна использовать объективно измеряемые показатели, позволяющие оценивать результаты педагогической деятельности не только качественно, но и количественно.

Е.А. Михайлова
Кандидат политических наук,
член Национальной Ассоциации
международной информационной
безопасности

РЕБРЕНДИНГ ТРАДИЦИОННЫХ ЦЕННОСТЕЙ КАК ЗАЛОГ ПОВЫШЕНИЯ МЕДИЙНОЙ ГРАМОТНОСТИ

На сегодняшний день вопрос сохранения и воспроизводства традиционных ценностей представляет колоссальную важность в связи с ростом факторов, влияющих на усиление сегментации общества, атомизации и даже конфронтации. В рамках фактической войны, ведущейся коллективным Западом против Российской Федерации, представители «европейских демократий» открыто заявляют, что основная задача проводимой в формате пакетов санкционной кампании — мобилизация народа нашей страны на борьбу с действующей властью и теми, кто ее поддерживает.

Одновременно с этим в информационном пространстве ведется полномасштабная когнитивная военная операция: посредством разнообразных методов информационного давления, монополизации дискурса наши противники фактически оправдывают дискриминацию русских по национальному признаку, где бы они ни жили и какую бы позицию ни занимали. Чтобы хоть краешком глаза взглянуть на богатое историко-культурное наследие Запада, откусить кусочек санкционного сыра, заказать картошку фри в «настоящем» Макдональдсе, наиболее подверженные информационному давлению соотечественники готовы терпеть длительные перелеты с пересадками, визовые отказы, сложности с бронированием отелей, очереди на оформление карточки местного банка и ни в коем случае не афишировать свою национальность. Ну и самое главное — не испытывать особого когнитивного диссонанса от такого положения вещей.

Безусловно, наиболее эффективно последствия данной гибридной войны сказываются на молодежи: их национальное самосознание, гражданская позиция, чувство прочной связи с Родиной еще находятся в стадии оформления, а активно навязываемые и потому столь желанные блага «сияющего града на холме» представляют для них гораздо более высокую ценность. Чтобы их получить, надо стыдиться своей связи с Россией, надо терпеть пренебрежение и несправедливость по отношению к себе и согражданам. Высока ли эта цена за новый айфон и красивые фотографии в социальных сетях? Если мы сегодня не сможем объяснить молодежи, от чего именно они отказываются, что именно они предают, то получим целое поколение людей, считающих, что их страна заслужила подобное возмутительное отношение со стороны международного сообщества. Последствия воспроизводства подобной пропозиции — тема для отдельной дискуссии, но, я думаю, никто не будет оспаривать факт ее катастрофичности.

Переходя к вопросу о роли традиционных ценностей в сегодняшней борьбе «за умы и сердца» наших граждан, следует выделить сразу три фундаментальных задачи, которые позволяет решить наличие коллективного разделяемого знания о базовых моральных установках, регулирующих поведение человека в социуме и его соответствующее самопозиционирование.

Во-первых, это позволит укрепить связь молодой аудитории с представителями старшего поколения, в том числе, находящегося у власти. Данная банальная, на первый взгляд, задача сегодня приобретает особую актуальность в связи с развитием средств массовой коммуникации и технологий искусственного

интеллекта. На сегодняшний день политический дискурс представляет собой не единое информационное пространство, а конгломерат самоизолированных поддискурсов, каждый из которых развивается по своим законам и в рамках своей политической реальности. Это стало возможным, благодаря способности индивида влиять на те инфоповоды, которые попадают в фокус его внимания: интересы каждого пользователя отслеживаются и анализируются с помощью искусственного интеллекта, после чего алгоритмы поисковой выдачи или предложенных постов в социальных сетях выдают пользователю только ту информацию, которая будет встречена с интересом и одобрением. Таким образом, если нет базового разделяемого знания о ценностях, которые государство защищает, осуществляя свою политическую волю, не будет ни понимания, ни поддержки проводимой политики среди «резидентов» самоизолированных поддискурсов: нужная информация просто не будет до них доходить.

Вторая задача, которую позволяет решить успешная трансляция и воспроизводство традиционных ценностей — это формирование и укрепление национальной гордости и самосознания. Только тот, кто гордится своей историей и предками, кто видит перед собой дорогу к более счастливому будущему и свою роль в его приближении, может эффективно противостоять злонамеренным попыткам унизить его гражданское и национальное достоинство, оправдать несправедливое отношение, репрессии, а там и до открытой агрессии недалеко.

Наконец, третьей задачей, прямо вытекающей из второй, является повышение уровня медийной грамотности у населения, под которой, по определению д.п.н. А.А. Казакова, следует понимать «…умение человека находить в материалах массмедиа интересующую его информацию, критически ее осмысливать и проверять достоверность, а также — при наличии соответствующей необходимости — самому создавать элементарные медийные сообщения»[1]. В эпоху засилья фейков и дипфейков, а также бурного развития технологий, стремящихся наводнить информационное пространство только той точкой зрения, которая выгодна их владельцам, единственным эффективным механизмом сопротивления манипулятивному воздействию является «медийная самозащита». Как бы ни старались официальные структуры вести превентивную работу по регулированию и блокировке контента, на современном этапе развития технологий этого недостаточно для обеспечения должной безопасности граждан.

Только крепкая убежденность индивида в собственных позициях, основанных на традиционных ценностях, а также в совпадении этих позиций с точкой зрения и политикой государственных акторов позволит распознать «фальшивые ноты» манипулятивных инфоповодов. Та же убежденность позволяет фильтровать инфопоток и с особым подозрением относиться к тем месседжам, которые содержат сильную эмоциональную окрашенность и побуждают нас действовать под влиянием этих эмоций.

Как можно заметить, сформулированные задачи имеют стратегическую важность для обеспечения эффективного взаимодействия власти и общества, а также для противодействия внешним угрозам. Таким образом, основной целью государства должна являться максимизация усилий по формированию коллективного представления о разделяемых традиционных ценностях, в том числе — у наиболее «сложных» сегментов целевой аудитории, к которым, в первую очередь, относится молодежь. Данная сфера стратегических политических коммуникаций не может позволить себе подходить к решению поставленных задач с пассивных позиций в духе «кому надо, тот поймет» и распространять знание о провозглашаемых ценностях с односторонних, вещательных позиций.

Вместо этого необходимо проявлять инициативу, прорываться в непривычные дискурсы, использовать нетрадиционный сленг, чтобы донести свою позицию до каждого реципиента, независимо от его сферы интересов, уровня образования и материального достатка. Одновременно с этим, государству необходимо интенсифицировать усилия по «вирусному» распространению и воспроизводству знания о традиционных ценностях. Они должны находить свое воплощение в образовательных программах, культурных продук-

1 Казаков А.А. Способы противодействия политическим манипуляциям в СМИ // Изв. Сарат. ун-та Нов. сер. Сер. Социология. Политология. 2018. №1. С. 87. URL: https://cyberleninka.ru/article/n/sposoby-protivodeystviya-politicheskim-manipulyatsiyam-v-smi.

тах, а также ретранслироваться в семейных и дружеских ячейках. Если родители не понимают, о защите каких ценностей идет речь и почему это имеет критическую важность, они не смогут объяснить это своим детям.

Безусловно, сформулированные рекомендации носят крайне масштабный характер, поставленных целей нельзя достигнуть в краткосрочной перспективе, но с чего-то надо начинать, и сегодня мы наблюдаем старт широкомасштабного процесса ребрендинга тех традиционных ценностей, о которых идет речь в нашей дискуссии. Почему же мы позволяем себе применять маркетинговый термин к процессу защиты и сохранения ценностей? Вполне логичным было бы предположить, что, если эти ценности прошли проверку временем, они и так всем известны и понятны.

Есть две причины, почему даже самые фундаментальные нравственно-духовные принципы организации общества требуют пересмотра. Во-первых, как отмечает Джоэль Восс, на протяжении многих веков люди ошибочно рассматривают память как аналог видеокамеры. Зафиксированные воспоминания изменяются с течением времени, поскольку «…память предназначена для того, чтобы помочь нам принимать правильные решения в данный момент, и поэтому память должна оставаться актуальной. Информация, которая важна прямо сейчас, может переписать то, что было в памяти изначально». Следовательно, необходимо следить за тем, чтобы сохраняемые ценности правильным образом прошли процесс реактуализации в современных условиях и терминах.

Вторая причина заключается в том, что любой бренд — это совокупность представлений о товаре у потребителей, сформированный образ, а также выраженное отношение к нему. К большому сожалению, новый виток дискуссии о защите традиционных ценностей, возникший в рамках внесения поправок в Конституцию Российской Федерации, во многом свел образ защищаемых традиционных ценностей к крайне узкой сфере личных взаимоотношений и конфликта гендерных ориентаций. При небольшом усилии, к образу защищаемых традиционных ценностей может добавляться представление о том, как должен (или не должен) выглядеть учитель начальных классов и его ученики.

Приведенный пример, хоть и отличающийся гиперболизацией, тем не менее, не так уж далек от действительности. Необходимость защищать и продвигать традиционные ценности, неоднократно озвученная политиками самого высокого ранга как руководство к действию государственных и общественных институтов на всех уровнях, натолкнулась на отсутствие консенсуса по поводу того, что конкретно понимается под традиционными ценностями. В ответ на это непонимание в ноябре 2022 года был выпущен Указ Президента Российской Федерации № 809 «Об утверждении Основ государственной политики по сохранению и укреплению традиционных российских духовно-нравственных ценностей», который перечислил те традиционные ценности, которые необходимо защищать.

Пятый пункт этого указа определяет: «К традиционным ценностям относятся жизнь, достоинство, права и свободы человека, патриотизм, гражданственность, служение Отечеству и ответственность за его судьбу, высокие нравственные идеалы, крепкая семья, созидательный труд, приоритет духовного над материальным, гуманизм, милосердие, справедливость, коллективизм, взаимопомощь и взаимоуважение, историческая память и преемственность поколений, единство народов России».

Эти формулировки максимально далеки от тех коннотаций, которые им стараются навязать недобросовестные СМИ и другие агенты информационного давления. Артикулированные ценности, первыми из которых идут не гендерная ориентация, не обязательная вера в Бога, а жизнь и достоинство, являются прочной основой для консолидации общества и укрепления национального и гражданского самосознания. Полагаем важным на следующем этапе ребрендинга провести широкомасштабную кампанию по повышению информированности социума (в первую очередь, профессионального педагогического сообщества и работников системы государственного управления на всех уровнях) о содержании данного нормативно-правового акта.

В заключение хочется отметить, что специфика современного политического противоборства и новые методы ведения гибридных войн обуславливают критическую значимость приобретения навыков информационной само-

защиты (другими словами — медийной грамотности) для противостояния злонамеренному манипулятивному воздействию. В качестве основного маяка, на который граждане могут ориентироваться при навигации в «бурных водах» медийного пространства, отсеивать ложную и подрывную повестку, выступают базовые духовно-нравственные ценности, продвигаемые и защищаемые на государственном уровне.

Эти ценности должны быть объяснены всем слоям социума в тех терминах, которые будут доступны и приемлемы для представителей каждой конкретной группы. Но для устойчивого формирования коллективно разделяемого знания о моральных и нравственных ориентирах российского общества государство должно не просто их сформулировать и распространить: важнейшим залогом достижения консенсуса по этому вопросу является неукоснительное *соблюдение* государственными акторами провозглашаемых ценностей в рамках своей деятельности. Справедливый суд, уважение достоинства, прав и свобод каждого индивида, созидательный труд на общее благо и т.д. — именно реальное воплощение всех обозначенных нарративов в ежедневных делах будет говорить о серьезности и чистоте намерений государства по сплочению российского общества перед лицом сегодняшних угроз.

В.Р. Григорьев
Заведующий кафедрой
«Информационное противоборство»
РТУ МИРЭА

АКТУАЛЬНЫЕ ВОПРОСЫ РАЗВЕРТЫВАНИЯ СИСТЕМЫ ПОДГОТОВКИ КАДРОВ В ОБЛАСТИ ИНФОРМАЦИОННОГО ПРОТИВОБОРСТВА СОЦИОТЕХНИЧЕСКИХ СИСТЕМ В УСЛОВИЯХ ГИБРИДНОЙ ВОЙНЫ ПРОТИВ РОССИИ

«Хочешь победить врага —
воспитай его детей»
(Восточная мудрость)

«Холодная война» против СССР в настоящее время трансформировалась в глобализационное и даже, можно сказать, цивилизационное противостояние «коллективного Запада» с Россией и остальным не прозападным миром и имеет свойство тотальности нескрываемых, и даже открыто декларируемых целей по установлению полной монополии на власть на планете по принципу Pax Americana. «Холодная война» в новой сетевой редакции ведется на новых фронтах: культурном, цивилизационном, этническом, религиозном и т.д. **Эта война является по содержанию духовно-нравственной, по сути — гибридной, а по организации — сетецентрической.**

В условиях использования против России широкого спектра подрывных гибридных технологий вполне реальной является перспектива в ближайшие 10–20 лет превращения современной гибридной войны в особый вид конфликта, который кардинально отличается от классических и рискует трансформироваться в перманентное, крайне жестокое и нарушающее все нормы международного права разрушительное противостояние.

Гибридная война многомерна, поскольку включает в свое пространство множество других подпространств (военное, информационное, экономическое, политическое, социокультурное, спорт и др.) (см. рис.1). У каждого из подпространств — своя структура, свои законы, терминология, сценарий развития. Многомерный характер гибридной войны обусловлен беспрецедентным сочетанием комплекса мер военного и невоенного воздействия на противника в реальном масштабе времени, разнообразие и различная природа которых обусловливают свойство своеобразной «размытости» границ между действиями регулярных сил и иррегулярным повстанческим/партизанским движением, действиями террористов, которые сопровождаются вспышками неизбирательного насилия и криминальными акциями.

Тотальное геополитическое противостояние вовлекло в свою орбиту и проблемы использования образовательной среды в качестве инструмента ведения информационных войн. Более того, учитывая исключительную роль образования в формировании будущей личности, ее ценностной ориентации, оно представляется одним из важнейших элементов информационной войны и получило название «мягкой силы». Потребность в развитии теории и практики «мягкой силы» особенно возрастает в сочетании с быстрым расширением и интенсификацией процессов использования Западом технологического превосходства в области технологий передачи и управления глобальными информационными потоками, а также технологий влияния на молодёжь в социальных ресурсах Интернет. При этом «оцифрованное» образование включает систему образовательных учреждений, средства массовой информации, процесс самообучения, дистанционные формы (on-line) на основе монополизации соответствующих

Рис. 1. Сферы проведения сетецентрических операций в условиях гибридной войны

электронных образовательных платформ (Zoom, Skype, Discord и др.). При этом пользователи неоднократно сообщали о недостатке безопасности, который позволял вмешиваться в конференции, создаваемые, например, через Zoom. Воспользовавшись ошибкой, злоумышленник может взять под контроль онлайн-конференцию, перехватить управление экраном, заменить сообщения и удалить участников конференции.

Доминирование США в информационно-телекоммуникационных технологиях привело к возможности использования Западом адресных воздействий информационного оружия и в сфере образования. Очевидно, что политику образования можно рассматривать как социокультурный феномен, потенциально имеющий уязвимости перед когнитивным информационным оружием. В своей статье «Железная хватка «мягкой силы». Новые технологии социальной инженерии в действии» (журнал «Однако» от 25.02.2013) доктор политических наук Елена Пономарева утверждает: «Именно проводники «мягкой силы» определяют, что есть «хорошо» или «справедливо», какая страна становится «изгоем» или образцом демократической трансформации, подвигая тем самым остальных участников политического процесса согласиться с этой интерпретацией в обмен на поддержку со стороны субъекта soft power». Власть «soft power» основана, прежде всего, не на аргументах разума, а на силе «информации и образов», на влиянии «смыслов».

При этом возрастают угрозы негативных информационных воздействий на население, в первую очередь, на подростковые и молодежные группы социума страны. Цели таких воздействий — решение пропагандистских или контрпропагандистских задач, а, в конечной цели, когнитивного перекодирования сознания конкретных социальных слоев и групп путем извращения информационной картины мира при ее восприятии человеком, навязывания ему некоторой ложной модели поведения и, в конечном итоге, манипулирования поведением людей в нужном направлении (рис. 2).

«США и их союзники навязывают России западные образовательные проекты в сфере образования и чуждые ценности через сеть Интернет», — заявил Секретарь Совета Безопасности России Николай Патрушев на совещании по безопасности Дальнего Востока.

По его словам, против Росии развязана «информационно-психологическая война», цель которой — «разрушение России» и «уничтожение ее жизненного уклада». Это воздействие направлено «преимущественно на молодежную аудиторию в целях искажения идей патриотизма и принижения геополитической

Рис. 2. Сферы использования «мягкой силы» в гибридных войнах.

роли России», — заявил Патрушев. «В этих же целях активно навязываются прозападные проекты в сфере образования, культуры и искусства», — отметил он. Патрушев призвал «поставить надежный заслон» распространению экстремистской продукции в Интернете, а также принять «своевременные и превентивные меры по защите населения от пагубного информационно-психологического воздействия».

По оценке Н. Патрушева, для этого также стоит разработать и реализовать программы, направленные на поддержку научных и социальных проектов по противодействию деструктивной идеологии и фальсификации исторических фактов, обеспечить активное использование информационных технологий в интересах сохранения и защиты культурных, исторических и духовно-нравственных ценностей народов России.

Результаты анализа текущего состояния и перспектив обеспечения информационной безопасности России показывают, что важнейшим, определяющим всю проблему в целом, фактором является целенаправленная подготовка и переподготовка высококвалифицированных кадров, способных эффективно решать постоянно увеличивающийся комплекс задач по гарантированной защите современных телекоммуникационных и информационных технологий и их контентного наполнения, составляющих инфраструктуру информационного базиса государственных организационных систем управления. Информационная безопасность России в период прохождения глобальной «цифровой трансформации» всех государственно значимых инфраструктур во многом определяется именно стратегией подготовки специалистов в области новых информационных технологий, определяющих независимость государства с точки зрения своевременного адекватного ответа на стратегические вызовы в XXI веке. Требования, которые предъявляются к новому поколению специалистов, существенно возрастают в силу беспрецедентной сложности указанных задач при постоянном росте внешних и внутренних угроз информационной безопасности России.

Практика проведения СВО особым образом позволила выпукло выделить инфопространство как один из главных театров войны и информационного противоборства. Именно в инфосфере формируется общественное мнение на те или иные информационные поводы и реальные события, которые в виртуальном пространстве трактуются вплоть до полной их инверсии. Кроме того, в инфопространстве могут быть представлены образы и трактовки событий, которые вообще не имели места в реальной жизни. Известный

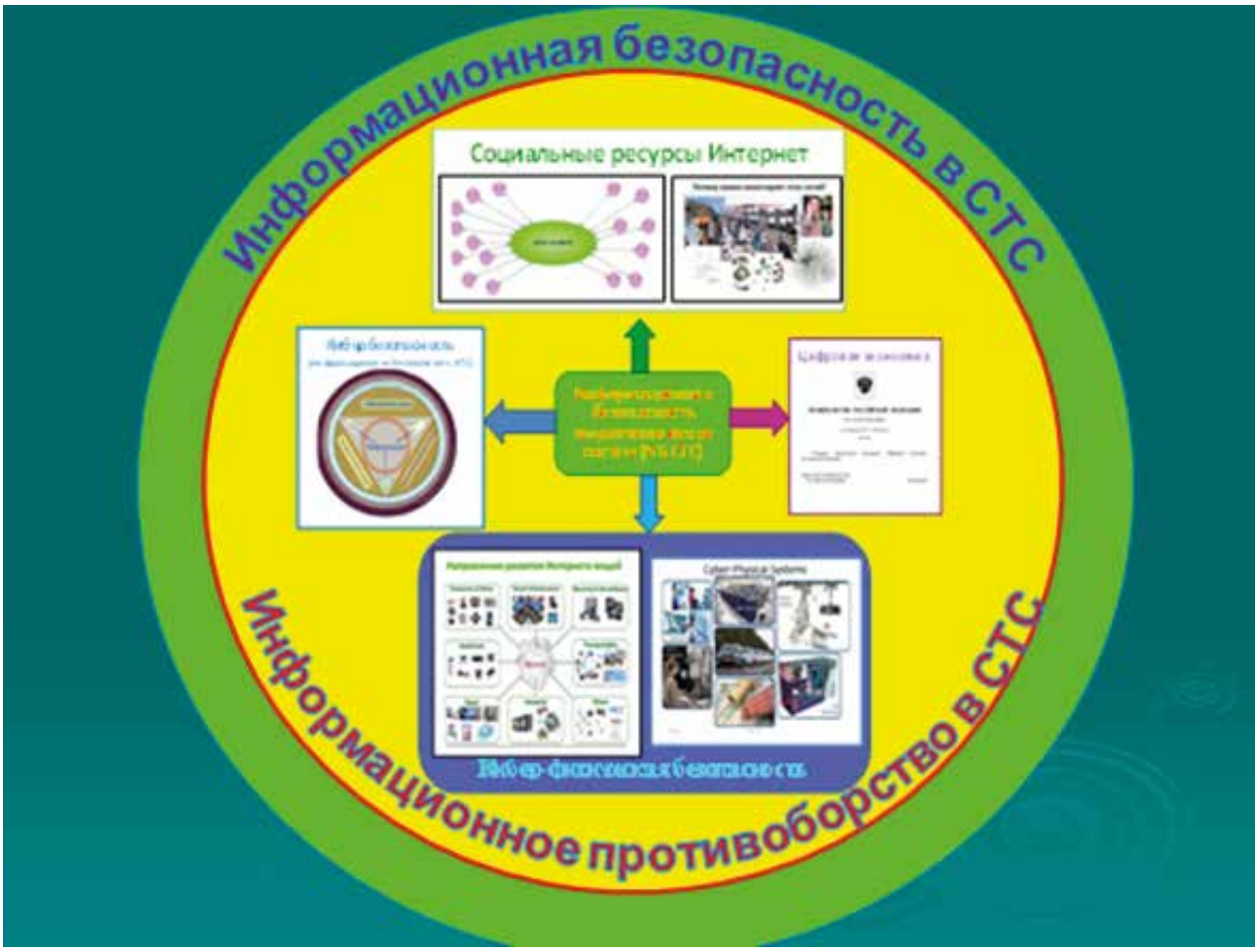


Рис. 3. Схема обеспечения синергетической информационной безопасности всей социотехнической инфраструктуры как единого объекта защиты.

русский поэт начала XX века Максимилиан Волошин говорил о том, что «из патентованных наркотиков газета есть самый сильнодействующий яд, дающий наибольшие доходы». С тех пор из этих слов выросло целое направление в политическом искусстве, так что теперь факты не играют никакой роли, важно лишь то, как их интерпретируют те или иные интересанты в целях манипулирования обществом. Это приводит к фрустрации массового сознания и появлению странных фантомов, когда в каждом событии гражданам навязывается определенный тип поведения и унифицированные взгляды и трактовки рефлексивного реагирования на них.

Комплексный характер актуальных угроз национальной безопасности в информационной сфере, обозначенных в Доктрине информационной безопасности России, требует определения инновационных подходов к реформированию системы подготовки и переподготовки профессиональных кадров в области развития и защиты российского информационного пространства в условиях глобализации, свободного обращения информации и, как следствие, появления новых типов информационных угроз.

Актуальность проблематики подготовки и переподготовки кадров в области информационной безопасности отражена в решении оперативного совещания Совета Безопасности России от 2.12.2022 г. по вопросу «О совершенствовании подготовки кадров для обеспечения информационной безопасности Российской Федерации».

Развитие новой синергетической отрасли информационной среды жизнедеятельности человека в виде взаимосвязанных объектов защиты — «цифровой экономики», «цифрового социума», интернета вещей, «критических информационных инфраструктур», других промышленных и бытовых киберфизических систем — требует, очевидно, развертывания **масштабной подготовки грамотных, профессионально подготовленных специалистов в области информационных тех-**

Рис. 4. Направления реформирования системы образования по подготовке специалистов в области информационной безопасности с учетом угроз, обозначенных новой Доктриной информационной безопасности России.

нологий, цифровой экономики и социо-киберфизических систем и, прежде всего, в области обеспечения информационной безопасности (ИБ) (рис. 3).

Все это определяет **актуальность проблемы улучшения организации процесса подготовки и переподготовки специалистов в данной области, как задачи государственной важности.** К сожалению, следует отметить, что ни один вуз в России не ведёт целенаправленно комплексную подготовку специалистов в этой бурно развивающейся области.

В настоящее время Федеральное учебно-методическое объединение в системе высшего образования по УГСНП 10.00.00 «Информационная безопасность» (ФУМО СВО ИБ) охватывает вузы, готовящие специалистов только в области обеспечения информационно-технической безопасности. Задачи, определенные Доктриной информационной безопасности России в области информационно-психологической и информационно-духовной безопасности, не входят в зону компетенции этого ФУМО. Соответственно, для этих сфер ИБ нет ни образовательных, ни профессиональных стандартов (см. рис. 4).

В связи с этим **становится крайне актуальной задача своевременного оперативного перестраивания всего процесса подготовки и обучения специалистов технических вузов в области ИБ с адаптацией их к новым требованиям времени и спроса потенциальных заказчиков из госструктур, промышленности, академического сообщества, бизнеса и финансовых структур.**

Следует отметить, что реагируя на новые вызовы в информационной сфере, в соответствии с Решением XXVII Пленума ФУМО СВО ИБ в **рамках образовательной программы базового высшего образования по специальности 34.05 «Организация и технологии защиты информации» предложено создать новую специализацию № 5 «Технологии информационного противоборства в социотехнических системах»** подготовки специалистов в рамках специалитета со сроком обучения 5 лет.

Гибридные войны и информационное противоборство в настоящее время все более становятся инструментом государственной политики западных стран, направленной на разрушение традиционных ценностей России, на противодействие доведению до российской и международной общественности достоверной информации о государственной политике Российской Федерации, ее офи-

циальной позиции по социально значимым событиям российской и международной жизни, на разрушение внутриполитической стабильности нашего государства. Отрицание очевидного, беззастенчивая ложь со стороны руководителей западных стран, ставших, по факту, непосредственными участниками информационного фронта, не имеющими ни чести, ни совести, их стремление переложить ответственность за все неудачи во внутренней и внешней политике своих стран на Россию — отличительные черты современного этапа развития прозападных информационных социальных ресурсов электронных СМИ. Изменившиеся реалии мира обусловливают необходимость пересмотра наших подходов к пониманию сущности и содержания таких войн современности, как гибридные войны и информационное противоборство. В этих условиях необходимо провести ревизию существующей нормативной правовой базы, оценить ее соответствие создавшимся условиям и нашим национальным интересам. Следует поставить вопрос о подготовке для органов государственного управления специалистов по информационному противоборству. Вопросы воспитания подрастающего поколения целесообразно определить важной государственной задачей, основанной на традиционных ценностях нашего народа, любви к Родине, добросовестном отношении к труду и учебе, честности и правдивости, нравственной чистоте, уважении к институту семьи, заботе о воспитании детей, почитании заслуг наших предков, создавших наше могучее и непобедимое многонациональное, многоконфессиональное и многоэтническое государство.

Требуется совершенствование системы обеспечения информационной безопасности государства с широким привлечением ученых, работников и экспертного сообщества в процессы принятия решений и управления, создания теоретического фундамента, актуализации и стандартизации терминологии в области информационного противоборства и гибридных войн, что позволит достичь единого понимания участников системы во всех аспектах совместной деятельности.

Конечной стратегической целью подготовки и переподготовки таких комплексных специалистов является освоение ими компетенций, навыков и умений по противодействию гибридным угрозам национальной безопасности с одной стороны, а с другой — профессиональных компетенций, навыков и умений по эффективному воздействию на агентов влияния, политические, экономические и когнитивные институты враждебного социума, технологии и мотивации ведущих против России информационную войну центров НАТО, составляющих инфраструктуру противостоящего нам и нашим союзникам враждебного Запада, а также на глобальное состояние социобиофизических систем, в свою очередь, составляющих основу нынешнего геостратегического доминирования «коллективного Запада» в информационной сфере.

Очевидно, что, учитывая агрессивный характер прозападной фейковой трактовки в контролируемых США социальных ресурсах Интернет реальных актуальных событий и информационных поводов, а также тотальное насаждение и навязывание, вопреки традиционным национальным религиозным и социокультурным цивилизационным кодам живущих в этих странах народов, ЛГБТ-ценностей всему мировому сообществу, представляющих угрозу «цифровому суверенитету» для всех суверенных государств, необходима дальнейшая консолидация дружественных государств по сближению, совместимости и гармонизации национальных образовательных программ подготовки специалистов, создающих и эксплуатирующих технологии обеспечения национальной и международной информационной безопасности на транснациональных стратегических коммуникациях.

С.В. Коротков
Генерал-майор (в отставке), кандидат военных наук, начальник экспертного отдела Национальной Ассоциации международной информационной безопасности

О НЕКОТОРЫХ НАПРАВЛЕНИЯХ ПРОТИВОДЕЙСТВИЯ УГРОЗАМ В ИНТЕРЕСАХ ЗАЩИТЫ СИСТЕМЫ ТРАДИЦИОННЫХ РОССИЙСКИХ ДУХОВНО-НРАВСТВЕННЫХ ЦЕННОСТЕЙ, ОТЕЧЕСТВЕННОЙ КУЛЬТУРЫ И ИСТОРИЧЕСКОЙ ПАМЯТИ

Из обращения Президента Российской Федерации В.В. Путина к участникам XI Московской конференции по международной безопасности: *«Мы видим, как последовательно идет формирование многополярного мира. Большинство государств готово отстаивать свой суверенитет и национальные интересы, традиции, культуру и уклад жизни».*

Происходящие в мире поистине революционные события со всей очевидностью свидетельствуют о нарастании накала цивилизационного противостояния между странами коллективного Запада под эгидой США и государствами не-Запада.

В основе этого турбулентного конфликта лежит гипертрофический рост противоречий между пассионарной культурно-исторической самобытностью народов на основе их традиционных ценностей и агрессивной античеловечной неолиберальной моделью глобализации.

Западные стандарты общественного поведения, которые предполагают отказ от общезначимых моральных ориентиров при абсолютизации свободы личного выбора, **не могут обеспечить развитие человеческой цивилизации.**

В отношении оценки этой ситуации отчасти был прав американский социолог и политолог Сэмюэл **Хантингтон**[1], который утверждал, что будущие войны будут вестись не между странами, а между культурами. Многие малообразованные представители западной элиты не допустили бы принятия знаковых ошибочных решений, если бы учитывали этот прогноз как закономерную тенденцию. Вместо этого «властители мира» были привержены идее Фрэнсиса **Фукуямы**[2]. Для их ума желанной являлась высказанная американским философом японского происхождения гипотеза, что распространение либеральных демократий во всём мире завершит социокультурную эволюцию человечества и приведет к окончательной форме мирового правительства.

В результате идущие в мире закономерные изменения вызывают, тем не менее, неприятие у ряда государств, привыкших мыслить согласно логике глобального доминирования и неоколониализма. Они отказываются признавать реалии многополярного мира и договариваться на этой основе о параметрах и принципах мироустройства. Предпринимаются попытки сдержать естественный ход истории, устранить конкурентов в военно-политической и экономической сферах, подавить инакомыслие.

Используется широкий набор противоправных инструментов и методов, включая **манипулирование сознанием отдельных социальных групп и целых народов, наступательные и подрывные операции в информационном пространстве. Распространенной формой вмешательства во внутренние**

1 С. Хантингтон, «Столкновение цивилизаций», 1993 г.

2 Ф. Фукуяма, «Конец истории и последний человек», 1992 г.

дела суверенных государств стало навязывание им деструктивных неолиберальных идеологических установок, противоречащих традиционным духовно-нравственным ценностям. Как следствие, разрушительное воздействие распространяется на все сферы международных отношений[3], включая информационную, культурную и образовательную среду.

В борьбе с Россией и ее влиянием в мире Запад основным оружием избрал **деструктивное информационно-психологическое воздействие** под лозунгом «культуры отмены» («cancel culture») всего, что связано с понятием «Русского мира». «Русофобия» и «переписывание истории» стали «константным стержнем» не только в политике англосаксов, но и значительной части европейских государств.

Для решения геополитических задач характерным явлением в 21 веке стало использование противоборствующими сторонами глобального информационного пространства, прежде всего за счет развития и применения эффективных информационно-коммуникационных технологий.

В этой связи руководством России к основным угрозам международной информационной безопасности отнесено *использование информационно-коммуникационных технологий в военно-политической и иных сферах в целях подрыва (ущемления) суверенитета, нарушения территориальной целостности государств, осуществления в глобальном информационном пространстве иных действий, препятствующих поддержанию международного мира, безопасности и стабильности*[4].

Опасным воплощением данной угрозы России в информационной сфере является злонамеренная и вредоносная деятельность Украины при поддержке и пособничестве Запада. По оценкам специалистов Международного института стратегических исследований в Лондоне *«методы информационной войны Украины, несомненно, будут изучаться и, возможно, широко применяться.*

Приверженность общественным коммуникациям, несомненно, была исключительным преимуществом в этом отношении, как и довоенное существование на Украине крупной рекламной индустрии, которую правительство смогло мобилизовать для реализации сложной коммуникационной стратегии, высокоэффективно используя социальные сети и средства массовой информации.

Превосходство украинского правительства в информационной сфере усилилось за счет массы онлайн-сторонников и сочувствующих, что придало спонтанную и самоорганизующуюся динамику информационным операциям Украины.

Успех Украины в информационной сфере предполагает, что это действительно может быть областью сравнительных преимуществ. Вывод из ситуации на Украине должен представлять особый интерес для Тайваня и Республики Корея в их отношениях с КНР и КНДР соответственно. В обоих контекстах информационное «поле битвы» предполагается рассматривать аналогично динамике российско-украинских отношений из-за высокой степени языковой и культурной общности»[5].

Данный вывод является еще и ярким подтверждением планирования англосаксами прокси-войн в Азиатско-Тихоокеанском регионе с учетом культурно-исторической идентичности проживающих там народов.

Другой поучительный пример планирования злонамеренной деятельности в ИКТ-среде можно найти в отчете Британского королевского института международных отношений, в котором утверждается необходимость отвергнуть концепцию «единой русской нации», включающей Украину и Белоруссию. По мнению «ученых» Чатем-Хаус, *«утверждение России о том, что ключевые славянские нации представляют »один народ« является попыткой легитимизации вмешательства в дела этих наций. Идея должна быть оспорена, поскольку является серьезным препятствием для стабильного развития обеих стран»*[6].

3 Концепция внешней политики Российской Федерации от 31 марта 2023 г.

4 Основы государственной политики Российской Федерации в области международной информационной безопасности (Указ Президента Российской Федерации от 12 апреля 2021 г. № 213).

5 https://www.iiss.org/publications/strategic-dossiers/asia-pacific-regional-security-assessment-2023/ The International Institute for Strategic Studies (IISS). Джеймс Крэбтри и доктор Юэн Грэм. «Война на Украине и баланс сил в Азиатско-Тихоокеанском регине», 2023 г.

6 Отчет «Chatham House»: «16 мифов о России», 13 мая 2021 г.

В организации и ведении пропаганды в целях **манипулирования сознанием** населения западные специалисты в области пиар-технологий все больше уделяют внимание использованию социальных сетей, ТГ-каналов и социальной рекламы с учетом снижения доли людей, склонных к критическому мышлению. Особую опасность для психического состояния населения такая зловредная деятельность представляет с учетом ее совершенствования за счет использования искусственного интеллекта.

Для достижения поставленных целей на Западе создана взаимосвязанная мощная **организационно-технологическая система информационной войны,** в которой задействуются **150–200 тыс. специалистов**[7].

При этом особую, лидирующую роль в этой системе продолжают выполнять силы ЦРУ. По этому поводу журнал **«NEWSWEEK» (США)** отмечает следующее. *«Все заслуживающие доверия эксперты и официальные лица, с которыми побеседовал Newsweek, согласились, что ЦРУ успешно и незаметно играло свою роль во взаимоотношениях с Киевом и Москвой, в перемещении массивов информации и материалов, а также в отношениях с различными другими странами…»*[8].

Деструктивная деятельность США и их союзников осуществляется **по следующим основным направлениям:**

- продвижение тезисов и аргументов в глобальном информационном пространстве в соответствии с политикой США, НАТО и ЕС;
- дискредитация института семьи и поддержка нетрадиционных сексуальных отношений;
- внедрение ценностей западной массовой культуры;
- содействие реализации западных систем образования.

Особым приоритетом на российском направлении является дискредитация Русской православной церкви, а основным объектом воздействия определена молодежь и социально незащищенные категории граждан.

Приведенные примеры злонамеренной деятельности коллективного Запада свидетельствуют об игнорировании странами, являющимися членами НАТО и ЕС, норм, правил и принципов ответственного поведения государств, призванных способствовать обеспечению открытой, безопасной, стабильной, доступной и мирной ИКТ-среды[9].

В условиях гибридной войны сохранение традиционных российских духовно-нравственных ценностей становится стратегическим национальным приоритетом.

Объективная оценка обстановки и понимание исторической миссии России обусловили разработку и утверждение Президентом Российской Федерации 9 ноября 2022 г. «Основ государственной политики по сохранению и укреплению традиционных российских духовно-нравственных ценностей»[10], а также внесение 25 января 2023 г. изменений в «Основы государственной культурной политики»[11], в том числе для достижения целей и выполнения задач в области обеспечения национальной безопасности и социально-экономического развития. Концептуальные положения этих документов стратегического планирования еще предстоит должным образом оценить и реализовать через конкретные целевые мероприятия в рамках программирования.

В этой связи важно в текущем году **завершить подготовку плана реализации «Основ государственной политики по сохранению и укреплению традиционных российских духовно-нравственных ценностей»** в целях организации и выполнения мероприятий всеми органами власти с участием институтов гражданского общества для противодействия социокультурным угрозам национальной безопасности Российской Федерации в части, касающейся защиты традиционных ценностей.

В этом ключе следует **сосредоточиться на:**

- реализации государственной информационной политики, направленной на усиление роли традиционных ценностей в массовом сознании и противо-

7 Сущность и содержание данной системы раскрыты в статье, опубликованной в журнале «Международная жизнь» 9.02.2022 г. («Западная глобальная система информационной войны набирает обороты»).

8 https://www.newsweek.com/2023/07/21/exclusive-cias-blind-spot-about-ukraine-war-1810355.html

9 Поддержаны резолюциями 70-й и 76-й сессии Генеральной Ассамблеи ООН.

10 Указ Президента Российской Федерации от 09.11.2022 г. № 809.

11 Указ Президента Российской Федерации от 25.01.2023 № 35.

действие распространению деструктивной идеологии;

- поддержке проектов, направленных на продвижение традиционных ценностей в информационной, культурной и образовательной среде;
- защите от внешнего деструктивного информационно-психологического воздействия, пресечение деятельности, направленной на разрушение традиционных ценностей в России.

Одним из важнейших направлений является **консолидированная информационная поддержка** борьбы против притеснения традиционных религиозных объединений на постсоветском пространстве с опорой на укрепление взаимодействия ведущих мировых религий.

Важным условием в достижении цели защиты традиционных духовно-нравственных ценностей является понимание государством и его многонациональным народом, что «сдерживание России» рассчитано нашими геополитическими противниками на длительный период, в котором значительная роль отводится провоцированию неконвенциональных действий[12] в рамках информационной войны со стороны «альянса демократий» во главе с США, Великобританией и Евросоюзом.

12 Неконвенциональные действия — действия, противоречащие принятым в обществе нормам морали и нормам закона.

А.В. Бирюков
Кандидат исторических наук, доцент, ведущий научный сотрудник Центра международной информационной безопасности и научно-технологической политики МГИМО

ДУХОВНО-НРАВСТВЕННЫЙ АСПЕКТ ГИБРИДНОЙ ВОЙНЫ НОВОГО ПОКОЛЕНИЯ

Гибридная война — постоянное состояние международных отношений. В условиях однополярного мира она превратилась в основной инструмент деятельности США на международной арене. Движение в направлении международного полицентризма усугубляет положение. Ставки на гибридную войну возрастают.

Непосредственное столкновение с Россией чревато крайне негативными сценариями для США с сателлитами. Они раздувают локальные прокси конфликты. События на Украине — пример прокси войны, с помощью которой надеются ослабить нашу страну. Однако ход этого вооруженного конфликта убеждает коллективный Запад в том, что победить русских на поле боя — задача сложно выполнимая. Укрепляется понимание, что попытки изолировать и разрушить Россию должны быть скорректированы.

Следует учитывать в этой связи, что США с союзниками делают ставку на гибридную войну нового поколения. В чем состоит новизна? Прежде всего акцентируется внимание на когнитивной борьбе и ментальном противостоянии. Объектом воздействия в этом случае становятся сознание, разум и воля человека, социальных групп и целых народов.

Контекст информационного общества создает благоприятные условия для ведения такой войны. В частности, в обществе быстро распространяются цифровой аутизм, информационное оглупление, клиповое мышление, которые создают питательную среду для ментальной войны. Эти явления, к сожалению, универсальны и в цифровую эпоху охватили все страны мира. Особенно деструктивный эффект они имеют в случае попадания в негативную общественную среду.

Именно такая среда сложилась в современном западном обществе потребления, в котором доминирует атмосфера лжи, элегантно именуемой постправдой. Сейчас только ленивый не говорит о системном кризисе капитализма в США, построивших свою систему за счет отстающих и зависимых государств. Цифровая эпоха только обостряет кризис однополярного миропорядка, построенного на сложившемся способе производства. Многие эксперты ищут способы преодоления негативных тенденций и противоречий современного мира.

Пути выхода из этого системного кризиса видятся ими через построение нового инклюзивного капитализма. По заданию американских властей Институт сложности в Санта Фе разработал модель пост-капиталистического будущего человечества, которое могло бы включать внедрение цифровой валюты и базового дохода, системы углеводородных рейтингов для государств и корпораций, жесткого социального контроля для граждан. Предлагаемая модель нацелена на рационирование потребления продовольствия с опорой на искусственную белковую пищу, контроль над рождаемостью, размывание половых различий, обязательную вакцинацию.

Все эти тезисы описывают пост-капиталистическое общество, через которое имеется в виду присвоить духовную сферу, то есть нарушить принцип принадлежности культуры народу. Лишить его исторической памяти, создать биологическую массу без национальной

и тем более цивилизационной идентичности. По существу, этот план, призванный спасти современное капиталистическое общество, взращивает своеобразный тоталитаризм цифрового формата, отрицая альтернативные модели общественного развития.

По глубокому умозаключению известного российского историка и политолога А.И. Фурсова, инициаторы и авторы подобного будущего стремятся не просто создать в глобальном масштабе удобный для себя пост-капитализм, но, во-первых, хотели бы перезапустить историю в том виде, в каком она развивалась со времен неолитической революции и направить её в сторону варварства в новом варианте и, во-вторых, поставить под контроль социо-биологическую эволюцию, повернув её вспять и превратив основную массу населения планеты в социальных животных без качеств и идентичностей[1].

В этой связи человечество ожидает ожесточенная борьба с подобными идеями, в которой духовные и гуманитарные ценности займут лидирующее место. В этом деле особую роль будет играть общественная наука, которая в сочетании с прогрессивными политическими силами подготовит фазовый переход к гармонии биосферы, техносферы и социума[2]. Такое сочетание составит основу и смысл эры гармогенеза, которая мыслится как мироустройство пост-информационного общества. Однако организация подобного фазового перехода и строительство пост-информационного общества — дело сложное и трудное, требующее эпохальных инноваций в гуманитарной сфере и качественных изменений в системе общественного управления.

По крайней мере за рамками такой духовно-нравственной системы окажутся все те антиценности, которые культивирует современный Запад типа трансгуманистического подхода к историческому процессу, экстремального индивидуализма, разрушения семей и культивирования однополой любви, выращивания пост-человека, входящего в качестве винтика в систему, управляемую искусственным супер-интеллектом, резкого и по существу насильственного сокращения населения, а также цифровое рабство.

1 См. Фурсов А.И. Наше «время Босха». М.: Изд.-во «Наше завтра», 2023.

2 См., например, книгу Хохловой М.Н. Сетевые мир и война. Новый миропорядок или новое мироустройство. Идеология будущего. Управление развитием. Гармогенез. М.: Книжный мир, 2023.

И.Ю. Тарасова
Кандидат политических наук, Комитет по международным делам Совета Федерации ФС РФ

АКТУАЛЬНЫЕ АСПЕКТЫ СУВЕРЕНИЗАЦИИ ИНФОРМАЦИОННО-ОБРАЗОВАТЕЛЬНОЙ ПОЛИТИКИ РОССИИ

Суверенизация предполагает совершенствование и органичное развитие российского самобытного фундаментального образования на базе лучших достижений отечественной и мировой науки. Вопросы суверенного образования следует рассматривать в контексте суверенизации всех сфер деятельности государственной власти и общественной жизни.

Президент России В. Путин: на совещании с членами Правительства, май 2023 г.: «Укрепление суверенитета России — ключевой фактор самосохранения нашего государства и территориальной целостности страны, запрос на суверенитет и самодостаточность страны формируется в сфере образования»[1].

«Школа наставника», март 2023 г.: «Мы продолжим формирование суверенной системы образования <…> Это чрезвычайно важная, базовая абсолютно вещь. Причем будем это делать на всех ее уровнях — от школы до колледжей и ВУЗов». 28 апреля 2023 г., на заседании Совета законодателей в Санкт-Петербурге: «В России формируется суверенная система образования. В этом будущее нашей страны».

На встрече с лауреатами и финалистами Всероссийского конкурса «Учитель года»[2]: **«Россия была и будет суверенной. Для этого сейчас на поворотном этапе развития нашей страны, да и всего мира нужно укреплять, выстраивать суверенную национальную систему образования и воспитания подрастающего поколения». По словам главы государства, нужно передать детям «нравственный, культурный код нашего народа»**, а также исключать любые попытки навязать детям чужие ценности.

Вернемся на 16 лет назад, когда тогдашний Глава Минобрнауки России А. Фурсенко, выступая на конференции молодёжного форума «Селигер-2007», сказал: «Недостатком советской системы образования была попытка формировать человека-творца, а сейчас задача заключается в том, чтобы взрастить **квалифицированного профессионального потребителя**… …Надо обеспечить »абсолютно равную конкуренцию госструктур и негосударственных структур на рынке предоставления образовательных услуг... …Поэтому целесообразно «разгосударствление» образовательных учреждений».

А до 2007 года были «лихие 90-е», когда фундаментальное образование начали системно уничтожать (в первую очередь изъяли

1 https://edu.gov.ru/press/6952/rossiyskaya-sistema-obrazovaniya-razvivaetsya-v-sootvetstvii-s-nacionalnymi-suverennymi-celyami/#:~:text=%D0%A0%D0%BE%D1%81%D1%81%D0%B8%D0%B9%D1%81%D0%BA%D0%B0%D1%8F%20%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0%20%D0%BE%D0%B1%D1%80%D0%B0%D0%B7%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D1%8F%20%D1%80%D0%B0%D0%B7%D0%B2%D0%B8%D0%B2%D0%B0%D0%B5%D1%82%D1%81%D1%8F%20%D0%B2%20%D1%81%D0%BE%D0%BE%D1%82%D0%B2%D0%B5%D1%82%D1%81%D1%82%D0%B2%D0%B8%D0%B8%20%D1%81%20%D0%BD%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%B0%D0%BB%D1%8C%D0%BD%D1%8B%D0%BC%D0%B8%20%D1%81%D1%83%D0%B2%D0%B5%D1%80%D0%B5%D0%BD%D0%BD%D1%8B%D0%BC%D0%B8%20%D1%86%D0%B5%D0%BB%D1%8F%D0%BC%D0%B8,-02%20%D0%BC%D0%B0%D1%8F%202023&text=%D0%A3%D0%BA%D1%80%D0%B5%D0%BF%D0%BB%D0%B5%D0%BD%D0%B8%D0%B5%20%D1%81%D1%83%D0%B2%D0%B5%D1%80%D0%B5%D0%BD%D0%B8%D1%82%D0%B5%D1%82%D0%B0%20%D0%A0%D0%BE%D1%81%D1%81%D0%B8%D0%B8%20%E2%80%93%20%D0%BA%D0%BB%D1%8E%D1%87%D0%B5%D0%B2%D0%BE%D0%B9%20%D1%84%D0%B0%D0%BA%D1%82%D0%BE%D1%80,%D1%81%D1%82%D1%80%D0%B0%D0%BD%D1%8B%20%D1%84%D0%BE%D1%80%D0%BC%D0%B8%D1%80%D1%83%D0%B5%D1%82%D1%81%D1%8F%20%D0%B2%20%D1%81%D1%84%D0%B5%D1%80%D0%B5%20%D0%BE%D0%B1%D1%80%D0%B0%D0%B7%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D1%8F. (дата обращения 30.08.2023).

2 http://www.kremlin.ru/events/president/news/72432/videos (дата обращения 04.10.2023).

из обращения советские учебники, программы), насытив рынок всевозможными проамериканскими «обучающими» методичками. Частные типографии штамповали учебные пособия авторов как местного, так и западного «розлива». Внедрить в школе очередной «учебник» было лишь вопросом денег и личных знакомств. И если серьезные фундаментальные ВУЗы, обладающие достаточным финансовым и административным ресурсом, еще «держали планку», то в общеобразовательной школе творился «беспредел» от непрофессиональных либо откровенно русофобских горе-авторов.

Помимо многих принципиальных недостатков той «образовательной» системы, в центр обучения и воспитания, в соответствии с либеральной идеологией, возвели учебу по интересам и способностям, т.е. обучение и воспитание должны были прежде всего интересны школьнику, в рамках того поверхностного объема, который он мог усвоить — не более того. Чем схематичнее, чем меньше усилий — тем доступнее (особенно за деньги), тем проще получить желаемый диплом. В содержательной части самые важные, смысловые, фундаментальные компоненты образования стали выбрасываться из программ. Так и духовно-нравственное воспитание из школы «ушло», не успев еще по-настоящему «зайти», и из программ были исключены многие классические произведения литературы, историческую правду начали «перекраивать» и т.д.

То есть **подрастающее поколение России почти 25 лет, до 2014 г., было фактически «подопытным объектом» коллективного Запада, так как на них испытывалось системное уничтожение основ фундаментального образования, «впитавшего» в себя все выдающиеся завоевания отечественной и мировой науки.**

Теперь обратимся к выступлению Председателя Объединенного комитета начальников штабов ВС США генерала Марка Милли[3], который недавно обозначил три новых приоритетных операционно-технологических направления, определяющих характер войны XXI века. Они, по заявлению Милли, обеспечат глобальное доминирование США и НАТО:

- искусственный интеллект в сочетании с робототехникой, как эффективный инструмент нанесения стратегического поражения противнику;
- подготовка к войне XXI века в мегаполисах. То есть, мегаполис — это приоритетное поле сражений, где возможно максимальное поражающее воздействие на инфраструктуру, перегруженную социально-техногенными точками напряжения с высокой плотностью населения;
- перед США и НАТО поставлена задача перехода от информационного к когнитивному доминированию, как определяющему фактору стратегической победы над противником.

Иными словами, война XXI века — война за умы, ментальная война.

И если по первым двум «пунктам» России есть, чем ответить коллективному Западу, то информационно-когнитивную войну мы, к сожалению, практически еще не начинали. Остановимся подробнее на третьем «условии».

Что из себя представляет ментальная война в XXI веке? Это геополитическое противоборство нового типа, где при всем многообразии составляющих можно выделить два определяющих фактора.

С одной стороны, это грамотно выстроенная подача аудитории информационного материала «на опережение». Ибо противник осуществляет переформатирование информационного поля — «перезагрузку» данных, фактов, воздействие через ИКТ, СМИ и т.п., что в итоге угрожает национальной безопасности государства.

С другой стороны, необходимо обеспечить соответствующее «когнитивно-духовное» восприятие обществом самой информационной повестки. Психоэмоциональная составляющая ментальной войны — навязывание своей воли противнику — направлена на манипуляцию сознанием объекта, как индивидуума, так и группы людей, и общества в целом.

Определяющей целью врага является стирание национальной идентичности русского народа, разрушение духовно-нравственных ценностей, деморализацию армии и всего населения, его ассимиляция с чуждыми ценно-

3 https://www.pnp.ru/politics/inducirovannaya-degradaciya-mira.html (дата обращения 30.08.2023).

стями и фальшивыми установками, навязанными противником, уничтожение цивилизационных, культурно-исторических основ России, **а в конечном итоге — ослабление многонационального российского государства, поражение в войне и установление мирового порядка, основанного на «правилах», которые обеспечат глобальное доминирование США и их приспешников, включая НАТО.**

Президент Путин в телеобращении к гражданам России: «Цель ...Запада — ослабить, разобщить и уничтожить в конечном итоге нашу страну. Они уже прямо говорят о том, что в 1991 году смогли расколоть Советский Союз, а сейчас пришло время и самой России, что она должна распасться на множество смертельно враждующих между собой регионов и областей»[4].

Для победы в этом беспрецедентном геополитическом противоборстве нашей стране нужна, помимо прочего, мощная, консолидирующая общество государственная идеология, которую поддержит абсолютное большинство населения, от правящих элит до нижних социальных слоев.

Идеологию невозможно насадить искусственно — например экспертами или чиновниками. Она формируется всей прожитой историей государства, совокупностью его культурных и духовных ценностей, и представляет накопленный опыт поколений и мудрость народного сознания, которые сформировали систему смыслов и мировоззрение народа.

Возрождение государственной идеологии — это один из важнейших инструментов защиты национальных интересов. Так, после Второй мировой войны объединенная Европа сделала идеологией «европеизм»[5]. Китай объединен идеологией китайской глобализации (при наличии конфуцианства как основы всей дальневосточной культуры[6]), а США — идеологией национальной исключительности и правом мирового господства. В Японии присутствует идеология национальной самобытности (государственный национализм[7]), в Индии — (нео)гандизм[8].

И хотя идеология не зафиксирована в Конституциях данных стран, она последовательно внедряется государствами через практические механизмы. Примеров тому бесчисленное множество. Так, например, в США учащиеся школ каждое утро перед уроками произносят клятву верности американскому флагу...

Запад пытается заставить другие народы отказаться от национальной идеологии именно потому, что она является объединяющим фундаментом для большинства геополитических процессов.

Для отстаивания национальных интересов, для победы в войне обществу необходимо знать, для чего именно это нужно. Что гражданин Российской Федерации ответит, если иностранец спросит его, почему хорошо стать русским и жить в России? При наличии разделяемой в обществе государственной идеологии ответ на такой «проверочный» вопрос будет патриотичным и приблизительно схожим у разных слоев населения.

В западных СМИ хорошо работает пропаганда еще и потому, что она ложится на подготовленную в каждой стране с младенческого возраста «идеологическую почву». А в России национально ориентированный, «скрепный» контент отечественных СМИ зачастую производит впечатление лишь на небольшую часть населения.

Идеологическая зрелость человека возникает не сама по себе, а при получении в семье и обществе соответствующего воспитания и образования, которые распространяют научные знания и культуру.

В.В. Путин на заседании «Дискуссионного клуба «Валдай»: «Основные качества государства-цивилизации — многообразие и самодостаточность. Каждое государство

4 https://rg.ru/2022/09/21/obrashchenie-prezidenta-rossijskoj-federacii.html (дата обращения 21.09.2023).

5 https://dic.academic.ru/dic.nsf/ruwiki/482242 (дата обращения 15.09.2023).

6 https://anashina.com/konfucianstvo/ (дата обращения 15.09.2023).

7 https://ru.wikipedia.org/wiki/%D0%AF%D0%BF%D0%BE%D0%BD%D1%81%D0%BA%D0%B8%D0%B9_%D0%BD%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%B0%D0%BB%D0%B8%D0%B7%D0%BC#:~:text=%E5%9B%BD%E6%B0%-91%E4%B8%BB%E7%BE%A9%20%D0%BA%D0%BE%D0%BA%D1%83%D0%BC%D0%B8%D0%BD%2D%D1%81%D1%8E%D0%B3%D0%B8)%2C,%D1%84%D0%BE%D1%80%D0%BC%D1%83%20%D0%BE%D1%80%D0%B3%D0%B0%D0%BD%D0%B8%D0%B7%D0%B0%D1%86%D0%B8%D0%B8%20%D1%8F%D0%BF%D0%BE%D0%BD%D1%81%D0%BA%D0%BE%D0%B9%20%D0%BF%D0%BE%D0%BB%D0%B8%D1%82%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%BE%D0%B9%20%D0%BD%D0%B0%D1%86%D0%B8%D0%B8. (дата обращения 15.09.2023).

8 https://old.bigenc.ru/world_history/text/2343969 (дата обращения 15.09.2023).

и общество хотят самостоятельно выработать свой путь развития. В основе его — культура и традиции, укреплённые в географии, историческом опыте, как давнем, так и современном, и в ценностях народа. Российскую цивилизацию … нельзя разделить …она существует только в своей целостности, в духовном и культурном богатстве»[9].

Кстати, принципы развития образования «в русле национальных традиций и в интересах национального развития» используются и в дружественных странах, например, в Белоруссии, Армении, Таджикистане. В Китае же закон утверждает, что образование должно «служить народу», а также «поддерживать и упрочивать прекрасные исторические и культурные традиции китайской нации, перенимая все выдающиеся достижения человеческой культуры».

Как мы видим, **для российской цивилизации знания, история и культура имеют определяющее и формирующее значение, они лежат в основе нашего цивилизационного кода.** Это та стратегическая среда, защиту которой обязано обеспечить государство, с опорой на консолидирующую общество национальную идеологию.

Образование и воспитание молодежи — одно из главных направлений ментального удара по нашей стране, потому что дети и молодые люди — психологически самая незащищенная часть населения[10], при этом именно они формируют духовно-нравственные основы многонационального народа России. (**«Сегодня — дети, завтра — народ»,** — (Сергей Михалков).

Характерно, что в современных документах по образованию, начиная с «Закона об образовании в Российской Федерации», основная цель отечественного образования до сих пор четко не сформулирована.

На наш взгляд, глобальная цель — создать отечественное образование как лучшее в мире с точки зрения смысла, содержания и методов. При этом всестороннее развитие человека — это конечный результат получения такого образования, а суверенность, самобытность образования — это средство достижения цели.

Какие «подводные камни» могут ожидать общество на этом пути?

1. Возникает опасение, что представители несуверенной элиты во власти и чиновники «на местах» могут подойти формально к поставленным Президентом задачам по суверенизации образования, продемонстрировать «потемкинские деревни», навредив таким образом процессу суверенизации по сути. Так, учителя уже жалуются, что школу наводнили массой обязательных конкурсов, посещениями театров и другими развлекательными мероприятиями, отнимающих у педагогов и учеников значительную часть времени, заложенного на обучение. Причем самые высокие положительные оценки школы получают за участие именно в этих мероприятиях, а не за работу по образованию и воспитанию детей на уроках.
2. Нельзя допустить изоляции российского образования. Развивать отечественное образование следует во взаимодействии с мировым образовательным сообществом и брать от последнего то, что необходимо нам в первую очередь. Делать акцент на сотрудничество с дружественными странами, активно продвигать свою позицию и достижения в области образования и культуры в другие страны. Это будет самая действенная, привлекательная гуманистическая пропаганда Русского мира. Россия всегда славилась умением перенимать у соседей все лучшее и трансформировать это в национальный русский продукт.
3. Не приравнивать уникальную самобытность отечественного образования исключительно к мероприятиям, демонстрирующим русское народное творчество, песни и пляски («суверенность» в стиле a la russe). Цивилизационный код и Русский мир — это качественно иные и более глубокие понятия.
4. Необходимо исключить излишне быстрый переход к шестилетнему специ-

9 http://kremlin.ru/events/president/news/72444 (дата обращения 05.10.2023).

10 http://www.kremlin.ru/events/president/news/72432/videos (дата обращения 04.10.2023).

алитету, так как это снизит качество нашего образования, как уже произошло ранее при стремительном переходе на двухуровневую систему обучения. Безусловно, скоропалительно и непрофессионально введенное разделение на бакалавриат и магистратуру нанесло серьезный вред отечественному образованию, нельзя «наступать на те же грабли», запуская теперь обратный процесс.

5. Не допустить механическое выполнение указания Президента ради «галочки», не вникая в научную суть вопроса.

Ниже приведем некоторые направления, на которые стоит обратить внимание в процессе суверенизации отечественного образования:

1. На протяжении последних 30 лет из системы образования выхолащивались фундаментальные естественно-научные дисциплины. Государственным приоритетом следует поставить задачу воспитания инженерного-технического и интеллектуального потенциала России, ибо без этого невозможно обеспечить обороноспособность и безопасность страны. Оборонно-промышленный комплекс должен стоять в фарватере современной науки.
2. Симбиоз фундаментальной и прикладной науки должен укрепляться подготовкой кадров, способных действовать в условиях ожесточенного кибер-противоборства. В этом направлении нужны совместные усилия на межведомственной основе, с привлечением специалистов Министерства обороны, Министерства иностранных дел и силовых ведомств, Минцифры, Российской академии наук и т.п.
3. Нужно восстановить военно-учебную систему государства. В целях возрождения преемственности специализированных педагогических кадров в данной области, необходимо приглашать старые военные кадры как со всей России, так и из стран Содружества.
4. В преподавании гуманитарных дисциплин сделать приоритетным обучение РОДНОЙ истории и географии, русскому языку и литературе, всех остальных дисциплин. И уже в контексте изучения выдающихся отечественных произведений и достижений обучать зарубежным дисциплинам и мировой культуре в ее лучших образцах.
5. На всех уровнях, от начальной школы до ВУЗов, разработать либо кардинально обновить фундаментальные учебные программы и пособия. Для решения этого вопроса потребуется несколько лет напряженной работы управленческих, научных, педагогических кадров и всех образовательных учреждений.
6. Сформировать систему непрерывного отечественного образования как новой ступени развития мирового образования XXI века. Возникновение непрерывного образования обусловлено многообразием возникающих перед населением научно-практических задач, все более усложняющихся в процессе развития человечества.

Непрерывное образование решает одновременно несколько задач:

- во-первых, обеспечивает получение и совершенствование профессионального образования в течение всей жизни (сегодня это возможно только в некоторых профессиональных областях, например, в науке);
- во-вторых, дает общее образование в максимально полном объеме, которое обеспечит всесторонний кругозор личности;
- в-третьих, предоставляет возможность получить новую профессию, если человек переходит в иную профессиональную сферу. Переобучение для освоения новой специализации должно быть доступно, в том числе, в зрелом возрасте.

В процессе непрерывного образования формируется «духовно-нравственная подпитка», так как человек получает возможность в течении всей жизни развиваться, осваивать интересующие его новые виды деятельности, формировать в соответствии с этим свое рабочее время и досуг.

Важным условием содержания непрерывного отечественного образования должна быть его идеологическая заряженность, а целью — всестороннее развитие человека на протяжении всей его жизни.

Научно-педагогическому сообществу предстоит разработать Концепцию развития непрерывного образования, как одно из направлений суверенного отечественного образования.

Переход к суверенному отечественному образованию предполагает не только кардинальное обновление российской образовательной политики. С учетом важности воспитания и обучения молодого поколения в духе защиты национальных интересов Родины желательно создание единого научно-практического центра, который будет анализировать и давать рекомендации по теоретическому обоснованию, апробации всего образовательного процесса и осуществлять контроль выполнения поставленных государством задач. Во избежание бюрократических и иных препятствий, такой центр должен быть подотчетен напрямую Главе государства.

Государственными структурами уже проводится работа по совершенствованию отечественного образования. В ВУЗы постепенно возвращают специалитет, Министерство просвещения утвердило программу школьного образования с военной подготовкой на ОБЖ и блоком про специальную военную операцию (СВО) по защите Донбасса на уроках истории.

Министерство просвещения России сообщило о введении нового предмета под названием «Основы духовно-нравственной культуры народов России». Школьники будут изучать его с пятого по девятый класс включительно.

При этом новые учебники пока требуют тщательной доработки, в том числе учебник истории, где зачастую встречаются неуклюжие перегибы, например, с отечественной «пропагандой». Так, утверждается, что Сталин проводил борьбу с «иноагентами», которую одобряло советское население. Не хватает грамотных разъяснений, например при критике правления М.С. Горбачева и Б.Н. Ельцина. Написано, что личный успех и материальное благополучие — это вражеские ценности, а глубокого понимания наших духовно-нравственных основ автор не предлагает, ограничиваясь недопустимыми для исторической науки жаргонными штампами.

Говоря о прямом воровстве Западом российских активов, автор заявляет: «Также были ...украдены средства российских корпораций... Такая воровская »лихость« не снилась даже Наполеону при установлении континентальной блокады Англии». Детям, не имеющим пока исторического образования, сложно правильно понять последний абсолютно неуместный пассаж. Или, например, практике ЕСПЧ по работе с жалобами на Россию даётся определение «издевательское избирательное право», без какого-либо объяснения школьникам хотя бы основного смысла данного определения.

Старшеклассникам в любом случае придётся отстаивать позиции российской внешней политики и идеологии с представителями других точек зрения. В этом случае они должны уметь оперировать логическими доводами, а не цитировать ярлыки и обвинения, которые иногда предлагает учебник. Вероятно, в дальнейшем следует тщательнее редактировать содержательную часть, либо привлекать более профессиональных авторов. Однако, сам факт начала работы над новыми учебниками внушает надежду на успех такого начинания в ближайшем будущем.

Российской Федерацией разработан целый ряд внутренних и международных документов в области международной информационной безопасности (МИБ), охватывающих, в том числе, как идеологический, так и правовой аспекты. Была принята новая Стратегия национальной безопасности, где много внимания уделяется защите духовно-нравственных ценностей, а также «Основы государственной политики в области МИБ». В апреле 2023 г. была опубликована «Концепция информационной безопасности детей»[11]. Последняя требует отдельного анализа и доработки. Тем не менее, в ней присутствуют такие необходимые пункты, как профилактика преступности в онлайн среде и вовлеченности в экстремистскую и террористическую деятельность, обучение цифровой гигиене и ответственному отношению к новым ИКТ, необходимость борьбы с деструктивным контентом в Интернете, координация деятельности родителей, общественных организаций и образовательных учреждений и т.п.

Стоит отметить, что с начала проведения специальной военной операции (СВО) изменилась ситуация в некоторых «областях»,

11 http://static.government.ru/media/files/0vjjsdBmSsIdUZ4c8Z2eOAiGkCbCf7OJ.pdf (дата обращения 10.09.2023).

связанных с защитой информационной безопасности детей. Так, благодаря грамотным действиям российских спецслужб, удалось остановить развитие «Русского Колумбайна», уменьшилось количество и популярность так называемых трэш-стримов («смерть в эфире» и др.); суицидальные «группы смерти» и детская порнография в сети Интернет вынуждены были сократить активность и существенно «завуалироваться» (при этом борьба с данным деструктивным контентом остается важнейшей государственной задачей).

Вместе с тем, расширяется география распространения среди несовершеннолетних наркотических и психотропных веществ, приобретает более радикальные формы буллинг, в условиях СВО получила «новое звучание» экстремистская и террористическая деятельность, участились преступления на почве межнациональной розни, этнорелигиозных конфликтов, обострения миграционного кризиса и т. п. **Вовлечение детей и молодых людей в преступную деятельность — один из опаснейших вызовов современного информационно-когнитивного противоборства, который требует скоординированных усилий государства и общества по суверенизации информационно-образовательной политики.**

От реализации Концепции информационной безопасности детей авторы ожидают, в том числе, следующих позитивных изменений:

- повышение уровня информационной безопасности и цифровой грамотности детей;
- формирование среди детей устойчивого спроса на получение высококачественной информационной продукции;
- повышение охвата педагогических работников мероприятиями в области обеспечения безопасности и развития детей в информационном пространстве;
- увеличение числа родителей (законных представителей), проинформированных о существующих возможностях услуги «Родительский контроль»;
- сокращение числа детей, пострадавших от жестокого обращения и травли, в том числе в сети «Интернет»;
- снижение фактов вовлеченности несовершеннолетних в деструктивные группы с использованием сети «Интернет»;
- сокращение количества информации, причиняющей вред здоровью и (или) развитию;
- увеличение в сети «Интернет» контента, направленного на формирование у детей традиционных ценностей.

В подтверждение реальности достижения поставленных задач ниже один из положительных примеров отечественного детского Интернет-контента:

Как известно, видеоигры вовлекают в сферу своего влияния представителей большинства социальных групп и возрастов, а в первую очередь — детей и подростков.

По данным аналитической компании DFC Intelligence[12] по состоянию на начало 2023 года аудитория компьютерных видеоигр насчитывала 3,7 млрд человек (46% от всего населения Земли). Контент платформы большинства таких игр содержит насилие и жестокость, сексуальные извращения, асоциальное поведение, скрытую пропаганду экстремизма, абьюзинг (физическое либо эмоциональное унижение) и другие виды деструктивного поведения.

По данным InfoWatch и Крибриум в последние годы наблюдается существенный рост российского игрового внутреннего рынка: 60% активного населения использует интернет для игр (данные Datareportal, январь 2023). 88 млн человек на территории России «подсажены» на видеоигры и тратят на это от 100 до 160 млрд рублей в год.

Значительное число игр производства недружественных стран (в частности, Японии и США) включают персонажей нетрадиционной сексуальной ориентации. Например, вся серия «The Sims» признана игровой франшизой, самой дружелюбной к ЛГБТ-контенту, а при этом данную игру по-прежнему активно популяризируют в России.

Нашей стране необходим свой игровой контент и система продвижения положительного имиджа России, и такая работа постепенно начинается.

Так, в Minecraft от Microsoft российские игроки воссоздали битву за оккупированный

12 https://gameworldobserver.com/category/market-analysis (дата обращения 15.09.2023).

Соледар. На канале российской версии игры World of Tanks отметили 78 годовщину поражения нацистской Германии воссозданием парада танков Советского Союза в Москве в 1945 году. На популярной платформе для создания игр Roblox пользователь организовал виртуальное празднование Дня России. Это хорошие примеры развития деятельности по обеспечению информационной безопасности молодого поколения.

В заключение стоит еще раз подчеркнуть, что усилия по развитию суверенного образования увенчаются успехом лишь в том случае, если параллельно будет происходить суверенизация других видов государственной и общественной деятельности. Так, суверенная экономика способствует проведению независимой внутренней и внешней политики, а например, суверенизация информационной политики невозможна, если контроль над ней осуществляют представители несуверенной элиты. И это — предмет для отдельного обсуждения.

Суверенная система образования должна выступать в качестве фактора стабильности государственной системы Российской Федерации. Образование — это то самое идеологическое оружие и одновременно «щит», который поможет выиграть любое информационное и ментальное противоборство.

Я.А. Бурляй
Директор Центра ибероамериканских программ Московского государственного лингвистического университета, заслуженный профессор МГЛУ, Институт международных отношений и социально-политических наук, профессор

РПЦ И ФАЛЬСИФИКАТОРЫ ИСТОРИИ

Интерпретировать по-разному историю той или иной страны — дело обычное. Однако, когда речь заходит об Отечестве, то включаются идеологические стереотипы прошлого, которые препятствуют обогащению духовной жизни народа. Это сразу же становится заметно, если в данном процессе принимают участие не только серьезные ученые, но и любители сенсаций, прибегающие к явным фальсификациям. Представители определенных политических сил тоже зачастую грешат этим.

Известно, что правда — это первая ложь в информационной войне. Однако нередко правдивые факты, изложенные без критического анализа, могут стать токсичной информацией. Посмотрим через данную призму на нижеприведенные исторические факты.

Наиболее ожесточенная полемика ведется, как правило, вокруг имен Ивана Грозного, Петра I и Сталина. В докладе подобраны оценки, высказанные наиболее авторитетными священнослужителями.

В 2008 году был опубликован доклад митрополита Ювеналия «К вопросу о канонизации царя Ивана Грозного и Г.Е. Распутина», в котором говорилось о том, что Ливонская война и опричный террор привели страну к жесточайшему социально-экономическому кризису и разорили ее население. При этом, делалась ссылка на Н.М. Карамзина, который ставил результаты правления Ивана Грозного в один ряд с татаро-монгольским игом [1].

У историков нет точных данных о числе лиц, пострадавших от рук опричников. В докладе говорится, что во время похода на Новгород было уничтожено 2 тыс. новгородцев и разорена Тверь, где казнили 9 тыс. человек. «При этом зверства опричников напрямую поощрялись самим царем» — отмечает Митрополит Ювеналий [2].

Те, кто стремится «обелить» Ивана Грозного заявляют об отсутствии свидетелей того, что митрополит Московский Филипп, который обличал царя за казни невинных людей, был убит по указанию тирана, и утверждают, что убийцы действовали по собственной инициативе. В докладе говорится также, что, ни один из приближенных царя не смог бы решиться на убийство церковного иерарха без высочайшего одобрения.

Поведение царя вообще нарушало основные христианские нормы. Иван Грозный был женат 7 раз, причем последние три раза вступал в брак без согласия со стороны церковной власти.

Итогом его правления стала гражданская война, а затем — и Смутное время. Иван Грозный не оставил своим наследникам мощного государства и боеспособной армии.

Не меньшие споры вызывает и фигура Петра I, упразднившего институт Патриархии в нашем Отечестве. Положительная оценка деятельности Петра I, также вызывает у некоторых экспертов серьезные сомнения.

Еще в 2009 году Патриарх Московский и всея Руси Кирилл в интервью, опубликованном на портале «Правмир» заявлял, что Петр I подчинил Церковь, сделал ее частью государственной машины, ввел в России модель абсолютизма, которого до него не было. При этом он задавался вопросом «не потому

ли так сильно ударила революция по Церкви, что в сознании многих людей Церковь отождествлялась с властью?» [3].

Как бы резюмируя, Патриарх говорил: «Я не оспариваю многого из того, что Петр сделал, но он сделал и нечто очень опасное для страны: привил на нашу, не предрасположенную к этому культурную основу, идеи западного абсолютизма» [4].

В 2022 году в Москве проходили XXX Международные образовательные чтения «К 350-летию со дня рождения Петра I: секулярный мир и религиозность». В докладе Патриарха Московского и всея Руси Кирилла говорилось, что отношение к личности Петра I и его реформам неоднозначно, поскольку в ходе их реализации приоритет отдавался светскому началу. Церковная реформа Петра I оттолкнула от Православия многих представителей образованной части российского общества [5].

По словам Его Святейшества, внедрение Петром I секулярной идеологии в России привело к разлому культуры на духовную и светскую. Секулярная идеология, как было сказано в докладе, «выдавливает религию на обочину общественной жизни и готова терпеть ее лишь в качестве культурной традиции».

И в заключение — несколько слов о Сталине, который по утверждению митрополита Илариона (Алфеева) принес в этот мир столько горя, что никакими военными или политическими успехами нельзя искупить его вину перед человечеством. Не стоит пересказывать интервью, данное 14 лет назад начальником Отдела внешних церковных сношений Московской Патриархии Русской Православной Церкви. Кто захочет, может прочитать полный текст в соцсетях [6].

Приведем более актуальное высказывание Главы синодального Отдела по взаимоотношениям Церкви с обществом Владимира Легойды. Комментируя информацию о готовившемся размещении мозаики с портретом Сталина в главном храме Вооруженных сил Российской Федерации, он выразил личное мнение о том, что изображения Сталина в храме быть не должно, поскольку «с его именем связаны многие беды в жизни людей, которые невозможно вычеркнуть из истории» [7].

Все вышеизложенные мысли могут послужить основой для противодействия фальсификаторам истории. Но успокаиваться рано. Борьба с манипуляторами коллективной памятью продолжается.

Список литературы:

1. К вопросу о канонизации царя Ивана Грозного и Г.Е. Распутина. http://www.patriarchia.ru/db/text/420877
2. К вопросу о канонизации царя Ивана Грозного и Г.Е. Распутина. http://www.patriarchia.ru/db/text/420877
3. О симфонии, Петре I и свободе Церкви от политических оценок. https://www.pravmir.ru/o-simfonii-petre-i-i-svobode-cerkvi-ot-politicheskix-ocenok/
4. О симфонии, Петре I и свободе Церкви от политических оценок. https://www.pravmir.ru/o-simfonii-petre-i-i-svobode-cerkvi-ot-politicheskix-ocenok/
5. Выступление Святейшего Патриарха Кирилла на пленарном заседании XXX Международных образовательных чтений. http://www.patriarchia.ru/db/text/5928249.html
6. Интервью журналу «Эксперт» «Миссия в миру» https://www.pravmir.ru/mitropolit-ilarion-alfeev-stalin-byil-chudovishhem-duhovnyim-urodom/
7. Светлый вечер с Владимиром Легойдой. https://radiovera.ru/svetlyj-vecher-s-vladimirom-legojdoj-01-05-2020.html.

КРУГЛЫЙ СТОЛ № 4
ПРОТИВОДЕЙСТВИЕ КОМПЬЮТЕРНОЙ ПРЕСТУПНОСТИ В ГЛОБАЛЬНОЙ ИКТ-СРЕДЕ

Ведущий:
Вураско А.А., руководитель группы ООО «Солар Секьюрити»

М.А. Богатиков
Консультант отдела международного сотрудничества в области безопасности Департамента международного права и сотрудничества, Минюст России

ПРОТИВОДЕЙСТВИЕ КОМПЬЮТЕРНОЙ ПРЕСТУПНОСТИ В ГЛОБАЛЬНОЙ ИКТ-СРЕДЕ

Уважаемые коллеги!

На сегодняшний день ИКТ получили повсеместное распространение: их используют государства, вооруженные силы, коммерческие и научные организации, а также обычные граждане. Но не всегда такое использование происходит в добросовестном ключе. Злонамеренное использование ИКТ всеми вышеперечисленными субъектами стало угрозой для безопасности мирового сообщества.

Возрастанию международной ИКТ-преступности способствует также и ряд юридических проблем. Именно на них мне хотелось остановиться в рамках своего выступления.

Во-первых, в международном сообществе на данный момент отсутствует универсальный договор, регулирующий вопросы борьбы с ИКТ-преступностью. Его разработка определена в качестве особо значимого направления деятельности государств для будущего формирования глобальной системы правового регулирования ИКТ.

Наше ведомство также участвует в работе по данному направлению.

В частности, представители Минюста России в составе межведомственных делегаций постоянно принимают участие в субстантивных сессиях Специального комитета ООН по разработке всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях для экспертного содействия продвижению и последующему принятию российского проекта универсальной конвенции по борьбе с информационной преступностью.

Тем не менее, важно отметить, что в условиях отсутствия универсального международного договора, регулирующего вопросы борьбы с информационной преступностью, международно-правовой основой для сотрудничества государств в вопросах расследования информационных преступлений и противодействия им выступают двусторонние и многосторонние международные договоры о правовой помощи по уголовным делам и выдаче.

Минюст России ответственен за разработку и заключение двусторонних и присоединение к многосторонним международным договорам Российской Федерации о взаимной правовой помощи по уголовным делам и о выдаче.

На настоящий момент у Российской Федерации имеется порядка 60 действующих двусторонних международных договоров о правовой помощи.

В активной переговорной стадии диалог о заключении таких договоров ведется более чем с 40 государствами. Таким образом, общий территориальный охват действующих для Российской Федерации международных договоров о взаимной правовой помощи по уголовным делам составляет 110 государств.

Мы, будучи ответственными за укрепление международного сотрудничества на данном направлении, понимаем, что в условиях возрастания международной ИКТ-преступности действующая правовая база не полностью отвечает тем особенностям, которыми обладают информационные преступления.

По итогам внутренней проработки этого вопроса было принято решение о необходимости разработки правовых инструментов, которые повысят эффективность и ускорят темпы международного сотрудничества как на внешнем, так и на внутреннем «кругах» оказания правовой помощи.

Таким инструментом выступает проект Протокола к договорам Российской Федерации о взаимной правовой помощи по уголовным делам, который был разработан Минюстом России совместно с заинтересованными органами государственной власти в целях совершенствования действующих двусторонних международных договоров о взаимной правовой помощи по уголовным делам.

Положения проекта протокола предусматривают ряд важных изменений по сравнению с классической процедурой оказания правовой помощи.

В частности, проект протокола позволяет устанавливать сжатые сроки исполнения запросов о правовой помощи, направлять запросы об оказании содействия в предварительном сохранении данных, которые хранятся или обрабатываются с использованием ИКТ на терри-

тории или в юрисдикции государства, а также осуществлять передачу данных в электронной форме.

По итогам работы проект Протокола будет взят за основу для экспертных консультаций с отдельными стратегическими партнёрами по вопросу совершенствования действующих договоров о взаимной правовой помощи по уголовным делам в части противодействия преступлениям в сфере информационно-коммуникационных технологий.

И в заключение хотелось бы остановиться на проблеме, которая красной нитью проходит через каждый переговорный процесс по любому из элементов международной информационной безопасности — проблеме терминологии.

Как нами уже не раз отмечалось на международных площадках, расхождения в понимании специализированных терминов продолжают оставаться камнем преткновения при осуществлении международного сотрудничества.

Вернемся к работе Спецкомитета ООН. Уже на протяжении нескольких лет государства не могут прийти к консенсусу в использовании терминов «преступления с использованием ИКТ» или «киберпреступления». Российская Федерация из сессии в сессию продолжает приводить аргументы в пользу ИКТ-подхода, который позволит нам бороться не только со злонамеренным использованием сугубо компьютеров и иных компьютерных систем, к чему нас склоняет киберподход, но и с использованием любого ИКТ-устройства в преступных целях. Всем очевидно, что основа данного разногласия чисто политического характера, потому что де-юре мандат Спецкомитета дает все основания говорить именно об ИКТ.

В целях осуществления вклада в процесс унификации терминологии в сфере международной информационной безопасности в рамках действующей при Минюсте России Подгруппы по выработке списка терминов в области безопасности в сфере использования ИКТ и самих ИКТ, их наполнению и межведомственному согласованию были разработаны «Подходы Российской Федерации к универсализации терминологии в области обеспечения безопасности в сфере использования ИКТ и самих ИКТ». Этот документ представляет собой видение Российской Федерации по вопросу, на каких принципах такая унификация должна осуществляться, а также он содержит основные термины и определения по данной проблематике. Перечень, представленный в Подходах, также содержит определения ИКТ-преступности и самих ИКТ, отражающие российское видение.

Подходы уже были представлены нами международному сообществу как в рамках многосторонних форматов, к примеру совместно с МИДом России нами ежегодно проводится семинар по проблематике терминологии на площадке Регионального форума АСЕАН, так и в двусторонних контактах с нашими партерами. Наше видение было воспринято с интересом, а самое главное — давало почву для поиска компромиссных формулировок.

Спасибо за внимание!

А.А. Бартош
Член-корреспондент Академии военных наук, директор Информационного Центра по вопросам международной безопасности МГЛУ

СОПОСТАВИТЕЛЬНЫЙ АНАЛИЗ ПОДХОДОВ ВЕДУЩИХ ГОСУДАРСТВ К ИСПОЛЬЗОВАНИЮ КИБЕРНЕТИЧЕСКИХ СРЕДСТВ В ИНФОРМАЦИОННОМ ПРОТИВОБОРСТВЕ В УСЛОВИЯХ ГИБРИДНОЙ ВОЙНЫ

Основные вопросы:

- 1.Подходы России, США и Китая к использованию киберсредств
- 2. Кибернетические средства в информационном противоборстве в военной сфере
- 3. Заключение

Мировая гибридная война

Многомерный межцивилизационный военный конфликт, в ходе которого большинство государств мира прибегают к целенаправленному адаптивному применению военно-силовых способов борьбы и экономического удушения противника, используют подрывные информационно-психологические и кибертехнологии.

США. Факторы стратегического планирования в киберсфере

- 1.Упор на долговременную стратегию развития киберсферы и готовность к ведению жёсткого геостратегического противоборства в глобальном мировом киберпространстве
- 2. Использование всех доступных инструментов, в том числе дипломатических, информационных, военных (как кинетических, так и кибернетических), финансовых, разведывательных механизмов, публичной дипломатии, действий правоохранительных органов
- 3. Развитие внутригосударственной системы управления рисками в цепочках поставок федерального уровня
- 4. Обновление законодательство об электронном надзоре и компьютерных преступлениях

ВЫВОДЫ по докментам стратегического планирования США

- США создали себе возможность для бездоказательных обвинений о причастности любой страны к инциденту в киберпространстве, что создаёт условия для эскалации международной напряженности вплоть до применения силы.
- Предполагаемые инициаторы злонамеренных подрывных действий в киберсреде уже определены Вашингтоном и не подлежат сомнению — это Россия, Китай, Иран, Северная Корея и международный терроризм

ПРОДОЛЖЕНИЕ СЛАЙДА «ВЫВОДЫ»

- В документах США не обозначены планы по созданию международных правовых механизмов, которые могли бы независимо, объективно и с должной компетенцией провести легитимное расследование и вынести судебное решение относительно злонамеренных актов в ИКТ-среде.
- В отсутствие официальных контактов раскол между американским, российским и китайским видением будущего ИКТ-среды только нарастает, и в результате может привести к серьёзным взаимным обвинениям в подрывной кибердеятельности, вплоть до открытой конфронтации и к фрагментации ИКТ-среды и Интернета

Основные положения закона КНР о кибербезопасности

- Особое внимание уделяется безопасности критически важных областей (государственные коммуникационные и информационные услуги)
- Жёсткий контроль уязвимостей в области безопасности и решительные меры по их устранению
- Защита личных данных
- Жёсткие требования к профессиональной подготовке кадров ИКТ

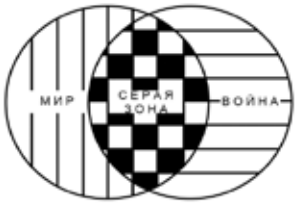
Государственные структуры киберпротивоборства России, США и Китая в военной сфере

- **Россия- Кибервойска МО РФ**
- **США- Киберкомандование. Единое боевое командование вооружённых сил США**
- **КНР - Бюро сетевых систем Сил стратегической поддержки (ССП) НОАК**

Серая зона

- **Политическое и географическое стратегическое пространство в пределах которого международная система, балансируя на грани войны и мира, переформатируется под правила нового миропорядка**

Рисунок 1. Серая зона



Стратегическая культура

- **совокупность стереотипов устойчивого поведения соответствующего субъекта при масштабном по своим политическим задачам и военным целям применении военной силы, в том числе при подготовке, принятии и реализации стратегических решений. Стратегическая культура является атрибутом не только вооруженных сил или даже государственной машины, а всего народа в целом**

Принуждение
(или политическое насилие)

- **это насилие, применяемое государственными либо негосударственными акторами с целью достижения определенных политических мотивов.**

Сдерживание путем отрицания

Рассчитано на то, чтобы создать физические препятствия противнику, затруднить ему достижение своей цели. Эффективность этой формы сдерживания также зависит от опасения, связанного с издержками, которые будут понесены противником во время акта агрессии в том месте, где она произойдет.

«Многослойная» модель сдерживания:

- Элементы «Многослойной» модели сдерживания:
- - стратегическое ядерное сдерживание;
- - стратегическое неядерное сдерживание;
- сдерживание принуждением.
- - сдерживание посредством отрицания;

Военная доктрина России: современные информационные угрозы

- **«Смещение военных опасностей и военных угроз в информационное пространство и внутреннюю сферу Российской Федерации».**
- **«Деятельность по информационному воздействию на население, в первую очередь на молодых граждан страны, имеющая целью подрыв исторических, духовных и патриотических традиций в области защиты Отечества;**
- **Провоцирование межнациональной и социальной напряженности, экстремизма, разжигание этнической и религиозной ненависти либо вражды».**
- **Нарастание «соперничества ценностных ориентиров и моделей развития цивилизации в странах Востока и Запада».**
- **«Использование ИКТ в военно-политических целях для осуществления действий, противоречащих международному праву, направленных против суверенитета, политической независимости, территориальной целостности государств и представляющих угрозу международному миру, безопасности, глобальной и региональной стабильности».**

События на Украине: первые уроки новой войны:

- Геополитика:
  1. Цель Запада – полное уничтожение России
  2. Началось активное возрождение фашизма
  3. ООН и международные структуры беспомощны
- Информационная сфера: особая значимость информационного оружия
- Военная сфера: высокая роль космических и беспилотных систем, высокоточного оружия
- Наука и образование: фактор понимания
- Культура: приоритет духовных ценностей

Цивилизационный характер противостояния Востока и Запада

- Причина противостояния – принципиальное различие базовых духовных ценностей
- Интеграция культур Востока и Запада сегодня невозможна
- Единственный выход – консолидация стран мирового сообщества для противодействия общим глобальным угрозам XXI века

Нарастание гуманитарного кризиса современной цивилизации:

- Интеллектуальная безопасность: снижение качества интеллектуальной элиты и интеллектуального потенциала общества;
- Снижение уровня образованности;
- Моральное разложение общества: рост насилия, жестокости, жадности, равнодушия;
- Кризис традиционной семьи на Западе;
- Одиночество и рост самоубийств на Западе.
- Деградация личности в цифровом обществе.

Этические проблемы культуры безопасности:

"Пять выше" - Этический кодекс империи Чингисхана:

- Общее - выше частного;
- Духовное - выше материального;
- Власть - выше владения (собственности)
- Закон - выше власти;
- Справедливость - выше закона.

Наука о безопасности - Софитология:

- Философия безопасности
- Система терминов в сфере безопасности
- Структура проблем, вызовов и угроз в сфере безопасности
- Прогнозирование последствий развития угроз и опасностей
- Методология противодействия угрозам и опасностям
- Гуманитарные аспекты безопасности

Заключение

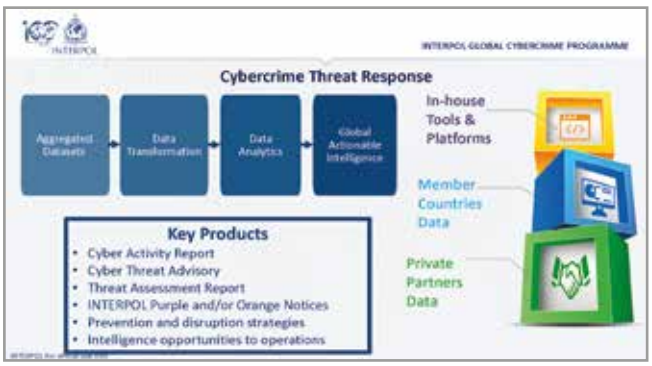
- Безопасность является ключевой проблемой развития цивилизации в XXI веке
- Формирование культуры безопасности - это необходимое условие выживания человечества в эпоху Антропоцена
- Необходимо формирование науки о безопасности - Софитологии. Научный потенциал для этого в России имеется.
- Образование должно давать фундаментальные знания и формировать адекватное мировоззрение элиты России в сфере безопасности.

Публикации по теме доклада:

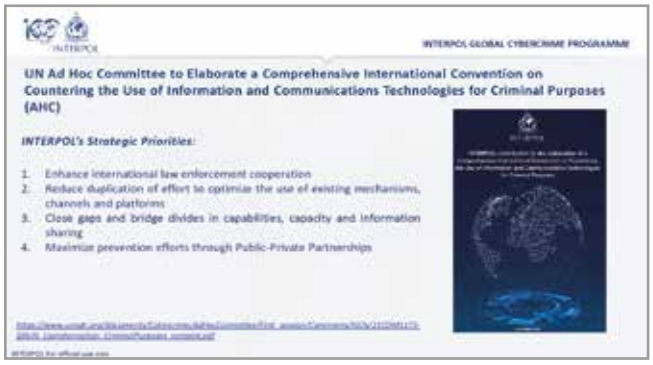
- Ильинский И.М. Главный противник. МосГУ, 2006..
- Ильинский И.М. О "культуре" войны и культуре мира. 2-е изд. 2003. - 128 с.
- Дашкевич В.С. Великое культурное одичание: Арт-анализ. 2013. - 720 с.
- Колин К.К. Глобальные угрозы развитию цивилизации в XXI веке. // Стратегические приоритеты, 2014, № 1.
- Колин К.К. Системный кризис культуры. // Стратегические приоритеты, 2014, № 3.

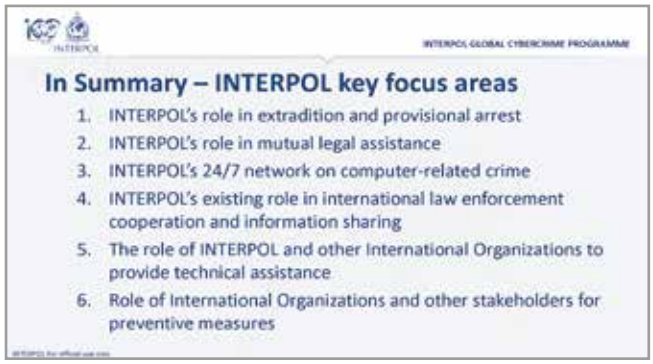
Пэй Лин Ли
Глава отдела разработки киберстратегии и кибер возможностей, Интерпол

ГЛОБАЛЬНАЯ СТРАТЕГИЯ ИНТЕРПОЛА ПО ПРОТИВОДЕЙСТВИЮ КИБЕРПРЕСТУПНОСТИ




89th GENERAL ASSEMBLY - Istanbul, Türkiye, 2021
Resolution No. 11 GA-2021-89-RES-11
Tackling global cybercrime threats through INTERPOL channels
17th ANNUAL HEADS OF NCB CONFERENCE


INTERPOL GLOBAL CYBERCRIME PROGRAMME
UN Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes (AHC)
INTERPOL's Strategic Priorities:
1. Enhance international law enforcement cooperation
2. Reduce duplication of effort to optimize the use of existing mechanisms, channels and platforms
3. Close gaps and bridge divides in capabilities, capacity and information sharing
4. Maximize prevention efforts through Public-Private Partnerships


INTERPOL GLOBAL CYBERCRIME PROGRAMME
In Summary – INTERPOL key focus areas
1. INTERPOL's role in extradition and provisional arrest
2. INTERPOL's role in mutual legal assistance
3. INTERPOL's 24/7 network on computer-related crime
4. INTERPOL's existing role in international law enforcement cooperation and information sharing
5. The role of INTERPOL and other International Organizations to provide technical assistance
6. Role of International Organizations and other stakeholders for preventive measures


INTERPOL
نشكركم جزيل الشكر على انتباهكم
Thank You Merci-Gracias
p.lee@interpol.int
https://www.interpol.int/en/Crimes/Cybercrime

Т.В. Исаева
Помощник директора Центра международной информационной безопасности и научно-технологической политики МГИМО МИД России

АКТУАЛЬНЫЕ ТЕНДЕНЦИИ МЕЖДУНАРОДНОГО СОТРУДНИЧЕСТВА В СФЕРЕ ПРОТИВОДЕЙСТВИЯ ПРЕСТУПНОСТИ В ИКТ-СРЕДЕ

Проблема киберпреступности в различных ее проявлениях растет и обостряется параллельно с процессом проникновения информационных технологий в различные сферы жизнедеятельности государства и общества, и о ее актуальности свидетельствует постоянно расширяющийся список всевозможных видов, способов и методов совершения компьютерных преступлений.

Сфера информационной безопасности, как никакая другая, породила своеобразную гонку между средствами нападения и средствами защиты. Любая инновация, которая получает широкое распространение, рано или поздно берется на вооружение киберпреступниками. Эффект от использования передовых разработок, как правило, зависит от того, в чьих руках и с какой целью они применяются.

Использование нейросетей в преступных целях

Не стали исключением и получившие широкое распространение в последнее время технологии искусственного интеллекта (далее — ИИ). В частности, использование нейросетей в преступных целях происходит преимущественно в 3-х направлениях:

- для написания вредоносного программного кода;
- для фишинговых атак;
- для создания дипфейков.

Сложные вредоносные программы с помощью нейросетей из даркнет

Традиционно программный код был результатом работы программистов, однако в настоящее время существующие модели ИИ могут на основе анализа обширных объёмов готового открытого кода понимать суть языков программирования и обобщать их до множества правил и паттернов, распознавать структуру программы и генерировать новый функциональный код, имеющий ту же логику и структуру, что и написанный людьми.

Ранее для создания сложного кода, избегающего обнаружения, даже для опытного хакера требовалось значительное время, теперь использование ИИ существенно облегчает задачу злоумышленникам, позволяя усовершенствовать алгоритмы и сократить трудоемкость и время на исполнение. Эта новая возможность представляет собой существенную угрозу в сфере информационной безопасности.

В рамках политики безопасности нейросетей разработчиками создаются барьеры и ограничения, чтобы не допустить создание вредоносного контента на своей платформе.

Например, если спросить наиболее известную нейросеть ChatGPT, как взломать компьютер, установить вирус или украсть деньги, он откажется отвечать. Однако, злоумышленники научились обходить ограничения с помощью использования подсказок для достижения желаемого результата с помощью инструмента ИИ (инжиниринг подсказок), представляющих по своей сути всего лишь грамотно составленный перефразированный запрос.

ИИ справляется с задачей создания опасных вредоносных программ за несколько часов, тогда как обычным программистам потребовалось бы потратить на эту работу 5–10 недель.

Спрос на применение нейросетей растет среди киберпреступников разного уровня подготовки. Первым ответом на растущий интерес стал появившийся в даркнете чат-бот на основе больших языковых моделей (Large Language Model, LLM), похожий на ChatGPT, но без присущих ему ограничений, под названием WormGPT.

И это только начало: в даркнете появляются новые ИИ-чат-боты — универсальный инструмент киберпреступников, который можно использовать для создания приложений в целях взлома компьютерных сетей, написания фишинговых электронных писем, вредоносного кода, обнаружения утечек и уязвимостей для их использования в дальнейшем в преступных целях. При этом для обучения ИИ-моделей используется вредоносное ПО

злоумышленников, данные, полученные из самого даркнета, и открытые результаты исследований по информационной безопасности.

ИИ-чат-боты из даркнет лишены любых морально-этических ограничений, а потому представляют собой угрозу не только как инструмент для написания вредоносного кода, но и как источник деструктивного контента, например расистского или нацистского содержания, источник информации о способах изготовления оружия, наркотических средств и т.п. Кроме того, использование «темного» чат-бота несет риск для самого пользователя, так как невозможно гарантировать, что разработчиками заранее не внесены в алгоритм чат-бота программные закладки, осуществляющие незаметное заражение компьютера вредоносным ПО, которое разработчики модели впоследствии активируют для решения своих задач.

Несмотря на то, что ИИ модели в настоящее время трудно назвать совершенными, их неконтролируемое использование вызывает обеспокоенность, так как порождает новые угрозы информационной безопасности.

Таргетированные фишинговые атаки с помощью нейросетей

Широкое распространение получили схемы таргетированного фишинга, то есть персонализированных обращений, соответствующих «портрету» каждого человека и сформированных на основе данных о нем, собранных в том числе из социальных сетей.

Искусственный интеллект дал в руки преступников мощное оружие. Фишинг становится более изощренным. На основе анализа доступных массивов открытых данных о компании или конкретном человеке, ИИ способствует индивидуализации фишинговых писем, например мошенники могут добавить в письмо фрагменты истории переписки или содержание профиля своей жертвы в социальных сетях, письмо может имитировать стиль общения знакомого человека или быть выдержано в стиле официальной переписки реальной организации или банка, регулятора, госучреждения. Таким образом у жертвы не закрадывается сомнений в подлинности его содержания. Адаптированные к особенностям конкретного человека фишинговые письма более эффективны.

Кроме того, искусственный интеллект может использоваться для конструирования поддельных профилей в социальных сетях, при помощи которых киберпреступники вступают в переписку и получают доступ к конфиденциальным данным, а также способны заменить OSINT-специалистов (open source intelligence — поиск, выбор и сбор и анализ информации из общедоступных источников) и психологов, которых хакеры привлекают для разведки и разбора целевой аудитории.

Следует отметить, что киберпреступность — явление трансграничное. В частности, огромное количество фишинговых писем создается за пределами страны, в которой находится целевая аудитория преступников. Сообщения, которые пишут иностранцы, зачастую можно легко отличить, так как они составлены неграмотно, содержат массу стилистических, орфографических и грамматических ошибок. ИИ способствует устранению ошибок, которые ранее позволяли идентифицировать сообщение как вредоносное.

Фишинговые электронные письма, сгенерированные искусственным интеллектом, легче проходят спам-фильтры и ссылки из них открывают чаще. Кроме того, нейронные сети помогают проходить защиту типа CAPTCHA (проверка, человек или бот зашёл на сайт, основанная на визуальной оценке изображения) и подбирать пароли.

Опасность ИИ заключается в том, что он позволяет хакерам создавать все более сложный и таргетированный контент, повышая вероятность того, что жертва поверит и перейдет по ссылке или выполнит инструкции.

Использование нейросетей для создания дипфейков

С помощью искусственного интеллекта можно изменить изображение или голос одного человека на другого с невероятной реалистичностью и, тем самым, синтезировать убедительные видео и аудиозаписи, в которых люди, говорят или делают то, что на самом деле они никогда не делали. Дипфейки представляют собой серьёзную угрозу, мошенники используют эти подделки для шантажа, дезинформации или создания скандальных новостей. Участились случаи дискредитации известных людей, чьи изображения размещены в большом количестве в свободном досту-

пе в сети Интернет. Дипфейки используются в рамках политической борьбы против отдельных деятелей и целых партий, чтобы манипулировать общественным восприятием, влиять на выборы или разжигать политическую напряженность. Размещение в сети роликов определенного содержания, например, с ложными заявлениями о трудном финансовом положении одной из крупных компаний, может даже изменить фондовый рынок в интересах злоумышленников. И совершенно очевидно, что включение в фишинговую рассылку дипфейков повышает эффективность в разы.

Новые виды противоправных деяний

Как и любая новая технология, искусственный интеллект не только предоставил новый инструмент для ранее известных преступлений, но и породил новые самостоятельные виды противоправных деяний.

Цифровое отравление (data poisoning)

Нейросети обучаются по определённым моделям — массивам данных, которые используются для того, чтобы система искусственного интеллекта могла делать корректные выводы. Если в исходные обучающие данные вносятся какие-то искажения (случайно или преднамеренно), то неверно обученная нейросеть будет выдавать некорректные результаты, причём обнаружить причину будет весьма и весьма сложно. Хакеры могут использовать такие атаки для манипулирования информацией или дезориентации систем, что может нанести значительный ущерб, особенно в области финансов, политики или информационной безопасности.

Использование ChatGPT в качестве приманки

Популярность ChatGPT в настоящее время стремительно растет. Огромное количество пользователей по всему миру пытается подключиться к сервису для его практического использования или просто из любопытства. Для получения доступа необходимо зарегистрировать учетную запись на сайте разработчика OpenAI, указав адрес электронной почты и номер телефона. Однако, в соответствии с политикой компании-разработчика, создание учетной записи возможно для потребителей далеко не из любой страны. В частности, в настоящее время нельзя официально зарегистрироваться жителям России, Китая, Белоруссии, Египта, Ирана и некоторых других стран. Пользователи ищут способы обойти ограничение и завести аккаунт, чем и пользуются мошенники, предлагая пользователям купить доступ к аккаунту для работы с ChatGPT на созданных ими фейковых сайтах.

Искусственный интеллект против киберпреступлений

Киберпреступники постоянно открывают для себя новые методы атак, поэтому специалистам по безопасности приходится постоянно адаптироваться и сохранять бдительность. Крупные IT-компании, предоставляющие услуги в области кибербезопасности, уже используют алгоритмы искусственного интеллекта и машинного обучения для поиска и устранения различных угроз, а также отражения хакерских атак. ИИ способен анализировать огромные объемы и типы данных, распознавать закономерности и аномалии и реагировать точно и быстро. Системы искусственного интеллекта также можно использовать для мониторинга и выявления подозрительного поведения в сетях, обнаружения аномалий в наборах данных и сканирования на наличие вредоносного кода.

Машинное обучение помогает автоматизировать обнаружение угроз, способствует обеспечению проактивной защиты системы, самостоятельно обрабатывая новости и исследования о кибератаках, помогает прогнозировать нападение и наращивать защиту еще до того, как оно произойдет, обозначать точки возможного проникновения в систему и сформировать стратегию предотвращения заражения.

Банковские и финансовые организации активно используют системы на основе ИИ, предназначенные для оценки финансовых транзакций в интернете на предмет наличия признаков мошенничества, при этом технологии ИИ применяются для определения отклонений от установленных бизнес-процессов, тем самым помогая быстро реагировать на возможное финансовое преступление или уязвимость самих процессов. Применение ИИ в таких системах особенно актуально, так как позволяет быстро адаптироваться к изменению логики и различных метрик бизнес-про-

цессов, а также минимизировать количество ложных блокировок транзакций. Более того, ИИ оперативно обнаруживает источник проблемы, так что правоохранители вовремя получают необходимые данные.

Технологии ИИ успешно применяются для защиты системы от DDoS-атак. Боты создают избыточный трафик, перегружая сайты запросами и парализуя их работу. Эта проблема особенно актуальна для организаций, бизнес которых напрямую зависит от интернет-трафика. Искусственный интеллект и машинное обучение помогают проанализировать трафик веб-сайтов и различать запросы поисковых роботов, ботов и людей. Машинное обучение помогает блокировать активность ботов даже при использовании средств анонимизации. На основе данных о поведении злоумышленников алгоритм формирует прогнозные модели и превентивно блокирует новые веб-адреса с похожей активностью.

Высокоэффективные методы контент-анализа, доступные современным системам ИИ, применяются также для анализа входящего трафика электронной почты в целях выявления особенностей, характерных для фишинговых писем. Нейросеть также сканирует содержащиеся в письмах ссылки и изображения, чтобы проверить их подлинность, позволяя тем самым пользователю безопасно просматривать и скачивать файлы. Злоумышленники, чтобы ввести в заблуждение доверчивых пользователей зачастую создают фишинговые сайты копируя визуальный образ настоящих и надежных интернет-ресурсов. ИИ позволяет обнаружить недоработки фишинговой страницы, которые не может заметить человек, и, тем самым, помогает специалистам по безопасности своевременно заблокировать фальшивые сайты.

Деятельность киберпреступников всегда сопряжена с необходимостью избежать какой-либо идентификации или отслеживания и сокрытия следов вредоносной деятельности. С помощью различных инструментов, таких как VPN и браузер Tor, достижение анонимности в сети стало легкой задачей. Принципиально важным можно назвать способность систем ИИ к выявлению анонимных хакеров, идентификации личности таких мошенников с целью последующей передачи информации сотрудникам правоохранительных органов для принятия соответствующих мер.

Таким образом, машинное обучение является ценным инструментом в борьбе с киберпреступностью, в частности ИИ может способствовать предотвращению атак с применением ИИ, однако, прежде чем система защиты будет успешно функционировать, требуется пройти длительный машинного обучения по всем этапам. В это самое время киберпреступники разрабатывают новые способы атаки и взлома. Это означает, что модели обучения ИИ необходимо будет постоянно адаптировать к новым угрозам наряду с разработкой новых стратегий борьбы с ними.

Состояние международного взаимодействия по противодействию киберпреступности

Следует отметить, что несмотря масштабность проблемы, глобального всеобъемлющего инструмента, направленного на противодействие киберпреступности, на международном уровне нет.

В рамках созданного по инициативе России Специального межправительственного комитета по разработке всеобъемлющей международной конвенции по противодействию использованию информационно-коммуникационных технологий в преступных целях ведется работа по согласованию текста проекта Конвенции.

Итоговый текст конвенции Спецкомитет планирует представить Генассамблее ООН в ходе ее 78 сессии в 2024 году.

Переговоры по согласованию текста конвенции проходят в сложной обстановке. В частности, участие российской делегации в шестой сессии Спецкомитета по разработке всеобъемлющей конвенции ООН о противодействии использованию информационно-коммуникационных технологий в преступных целях в штаб-квартире ООН в Нью-Йорке снова было осложнено невыдачей США виз членам российской делегации.

«Нулевой проект» конвенции, который обсуждался в ходе шестой сессии Спецкомитета, отражает интересы преимущественно тех государств, которые многие годы препятствовали его созданию. Россия выдвинула свой проект Конвенции, который был поддержан несколькими государствами и исходит из необходимости обеспечить широкий охват будущего договора. Вынесенный же на рас-

смотрение «нулевой проект» не учитывает развитие информационно-коммуникационных технологий, возможности которых все шире используются для призывов к нарушению правопорядка, незаконных торговле оружием и обороту наркотиков, в террористических и экстремистских целях.

Россия не согласилась с «нулевым проектом», представленным на рассмотрении Спецкомитета, и настаивает на возвращении в проект конвенции статей по борьбе с экстремизмом, нацизмом, терроризмом, доведением до самоубийства, незаконным распространением наркотиков и оружия. Эти темы были в предыдущей версии проекта, однако, к сожалению, исключены из него.

Второе ключевое противоречие в ходе переговоров — это отсутствие единообразной терминологии, от которой зависит охват конвенции и охват криминализации. Россия настаивает на том, чтобы была разработана всеобъемлющая конвенция об использования именно ИКТ в преступных целях, страны Запада пытаются сузить охват конвенции распространив его действие только на компьютерные технологии, в то время как только термин «ИКТ» позволяет сделать конвенцию универсальной и применять ее, в том числе, и в случае преступного использования новых видов информационно-коммуникационных технологий.

Вместе с тем видится, что будущий документ будет способствовать сотрудничеству между правоохранительными органами в ситуациях, в том числе, когда рассматриваемые государства не были участниками Будапештской конвенции, не только в деле расследования, но и пресечения преступлений, совершаемых с использованием ИКТ.

До настоящего времени на международном уровне также не выработано единого подхода к проблеме регулирования ИИ. Генеральный секретарь ООН А. Гутерриш предложил создать организацию надзора и регулирования ИИ по аналогии с МАГАТЭ. По его словам, новые технологии развиваются с невероятной скоростью, как и связанные с ними угрозы. Генеральный секретарь выразил опасения, что ИИ может облегчить путь преступникам, террористам и другим субъектам, намеревающимся причинить смерть и разрушения, обширные травмы и глубокий психологический ущерб в невообразимых масштабах. Однако работа по созданию единого органа регулирования ИИ представляется очень сложной, так как страны-члены ООН существенно расходятся в подходах к проблеме.

Таким образом, очевидно, что отсутствие унифицированной терминологии и классификации преступлений, связанных с применением информационно-коммуникационных технологий в преступных целях, существенно осложняют работу по принятию единого регулирующего документа на глобальном уровне. Вместе с тем, существенный рост киберпреступлений и активная работа на уровне региональных и международных организаций способствуют прогрессу по достижению консенсуса. Повсеместное внедрение технологий ИИ оказывает существенное влияние на рост количества фиксируемых киберпреступлений в мире. Однако выделение преступлений, совершаемых с применением ИИ, в отдельный класс не представляется целесообразным. Вместе с тем, необходимо активизировать работу на международном уровне по достижению единого подхода к регулированию применения технологий ИИ в целом, что, как представляется, может поспособствовать снижению количества использования этих технологий преступниками. Кроме того, представляется целесообразным создание национальных центров по вопросам обнаружения, предупреждения, фиксации и ликвидации последствий атак с использованием технологий ИИ.

А.О. Вихляев
Член межведомственной рабочей группы Российской Федерации по противодействию информационной преступности

О СОВЕРШЕНСТВОВАНИИ МЕЖДУНАРОДНО-ПРАВОВОГО РЕГУЛИРОВАНИЯ МЕЖДУНАРОДНОГО ПРАВООХРАНИТЕЛЬНОГО СОТРУДНИЧЕСТВА В СФЕРЕ ПРОТИВОДЕЙСТВИЯ ПРЕСТУПЛЕНИЯМ, СОВЕРШАЕМЫМ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Сегодня активное внедрение и использование информационно-коммуникационных технологий во многом определяет прогрессивное развитие каждого государства и мира в целом. Машинное обучение, искусственный интеллект, робототехника и новые продукты в сфере высоких технологий становятся основой роста экономики, а цифровые платформы и электронный документооборот кардинально повышают эффективность работы различных организаций, предприятий, социальных и образовательных учреждений, облегчают решение множества бытовых задач.

При этом развитие информационно-коммуникационных технологий вместе с их полезными свойствами и новыми возможностями несут ещё и новые риски, угрозы и вызовы.

Особую опасность представляет применение информационно-коммуникационных технологий в террористических целях. Они используются террористическими организациями в качестве инструмента пропаганды терроризма, привлечения новых сторонников к их преступной деятельности, совершения террористических атак, а также обеспечения их деятельности: организации и планирования терактов, сбора финансовых средств, осуществления коммуникации между злоумышленниками и т.д.

Информационно-коммуникационные технологии активно применяются и в целях совершения преступлений общеуголовного характера, масштаб нанесения вреда и ущерба от которых пока, к сожалению, увеличивается.

Повсеместное вплетение информационно-коммуникационных технологий вооружает злоумышленников как новыми методами совершения преступления, так и способами их сокрытия.

У преступников появилась возможность дистанционно, в том числе из других стран, совершать противоправные деяния с использованием информационно-коммуникационных технологий. При этом они часто используют ещё и инфраструктуру третьих стран, особенно тех, у которых отсутствуют международные обязательства о сотрудничестве в сфере противодействия преступности. При этом такая информационно-коммуникационная инфраструктура содержит массивы различных данных, необходимых правоохранительным органам для предупреждения, выявления, пресечения и расследования киберпреступлений. Поэтому для успешного решения задач по противодействию таким преступлениям необходимо постоянно совершенствовать международное правоохранительное сотрудничество в этой сфере. Считаем, что эффективно противодействовать таким угрозам можно только вместе, объединив усилия всего международного сообщества.

Привлечение преступников к ответственности — это очень важная задача, стоящая перед правоохранительными органами. Однако, показателем эффективности правоохранительных органов и специальных служб является ещё и способность пресекать преступления на ранней стадии их подготовки, не допуская

нанесения никакого вреда и ущерба от противоправных действий злоумышленников.

Эффективность проведения мероприятий по противодействию преступности во многом зависит от того, насколько оперативно взаимодействуют компетентные органы, в том числе в процессе обмена информацией. Поэтому при формировании положений международных договоров, содержащих механизмы международного правоохранительного сотрудничества, важно предусматривать возможность использования компетентными органами современных средств, обеспечивающих быстрый и безопасный обмен данными, сведениями и информацией, в том числе при помощи использования защищённых каналов связи и электронных подписей в процессе оперативного обмена информацией в электронной форме.

При этом осуществление поиска, хранения, копирования и передачи такой информации для правоохранительных целей тоже имеют ряд особенностей, которые ранее, например, в Конвенции ООН против транснациональной организованной преступности от 15 ноября 2000 г. урегулированы не были. Поэтому её положения не создают всех необходимых условий для эффективного противодействия преступлениям, если они совершаются с использованием ИКТ. Сегодня для успешного решения задач по выявлению, пресечению и расследованию преступлений, совершаемых с использованием современных информационных технологий, требуется применение соответствующих инновационных форм международного сотрудничества. В этой связи наряду с оперативным взаимным обменом информацией важное значение имеет ещё и обеспечение её полноты и сохранности.

При этом под обеспечением полноты и сохранности информации и цифровых следов понимается следующее:

- оперативное сохранение информации, содержащейся у операторов связи и в дата-центрах, в том числе предоставляющих услуги по хранению и обработке данных различных онлайн-сервисов;
- создания образа дисков, содержащих как копию самих файлов, имеющихся на электронном носителе информации (например, документов в электронной форме, фотографий, видео и т.д.), так и сведений об этих файлах (например, геолокации, датах создания и изменения файлов, применяемых технических устройствах и т.д.);
- розыска электронной информации с учётом того, что она может быть воспроизведена только в том случае, если будут найдены все её элементы (данные), хранение которых может осуществляться не на одном носителе, а распределено между несколькими физическими дисковыми устройствами.

Такие данные могут быть полезны правоохранительным органам для успешного проведения мероприятий по предупреждению, выявлению и пресечению преступлений, нахождению злоумышленников их планирующих, а также обеспечения правоохранительных органов соответствующими доказательствами, необходимыми для привлечения преступников к ответственности.

С ростом киберпреступности возрастает нагрузка на оперативные, следственные и экспертно-криминалистические подразделения правоохранительных органов по всему миру. Статистика преступности, совершаемой с использованием ИКТ, свидетельствует об актуальности тенденции развития государственно-частного партнёрства по противодействию преступлениям в сфере информационных технологий и привлечению частных партнёров к реализации некоторых задач правоохранительной деятельности:

- проведения компьютерных экспертиз;
- разработки специализированного программного обеспечения с учётом потребностей правоохранительных органов;
- ряда других задач.

По всему миру национальные и международно-правовые механизмы регулирования этой сферы также нуждаются в постоянном совершенствовании.

Важным направлением такой работы является создание условий для применения правоохранительными органами современных технологий и средств, в том числе самих информационно-коммуникационных технологий. Разработка и применение международно-правовых механизмов, соответствующих современным реалиям, позволит создать ус-

ловия для совершенствования уже имеющихся и формирования новых форм международного сотрудничества между компетентными органами, позволяющие более эффективно противодействовать киберугрозам.

В этой связи полагаю важным формировать эффективные правовые механизмы обеспечения информационной безопасности, которые должны основываться на лучших практиках выявления, предупреждения, пресечения и расследования преступлений, совершённых с использованием информационно-коммуникационных технологий, а также судебного преследования лиц их совершивших. При этом такое правовое регулирование должно учитывать специфику отрасли и позволять ей успевать развивать цифровые технологии и надёжно обеспечивать безопасность их использования человеком, обществом и государствами.

Н.М. Гудков
Старший прокурор Управления методико-аналитического обеспечения надзора за процессуальной деятельностью органов предварительного расследования и оперативно-разыскной деятельностью Главного управления по надзору за следствием, дознанием и оперативно-разыскной деятельностью Генпрокуратура Российской Федерации

СОВРЕМЕННЫЕ ТЕНДЕНЦИИ И УГРОЗЫ ИСПОЛЬЗОВАНИЯ ИКТ В ПРОТИВОПРАВНЫХ ЦЕЛЯХ И ПРИНИМАЕМЫЕ МЕРЫ ПО ПРОТИВОДЕЙСТВИЮ ПРЕСТУПЛЕНИЯМ В ДАННОЙ СФЕРЕ

Информационные технологии бурно развивались в течение десятилетий во всем мире, при этом в последние годы в повседневную жизнь все активнее внедряется множество новых технологий, таких как искусственный интеллект, deep-fake, цифровое облако, интернет вещей, big-data, метавселенная и другие.

Возрастающая роль информационных технологий и интеграция широкого круга правоотношений в глобальное цифровое пространство сопряжены не только с прогрессом, но и с активной противоправной деятельностью злоумышленников в цифровой среде.

Данные тенденции вызваны совершенствованием схем и инструментария, используемых злоумышленниками для сокрытия следов противоправной деятельности, широкого охвата потенциальных жертв, минимизации этапов преступной деятельности с одновременным повышением уровня анонимности их организаторов и облегчением легализации преступных доходов.

Актуальность сохраняют и традиционные виды преступности, для которой информационно-коммуникационные технологии стали основой формирования новых направлений организации взаимодействия участников противоправной деятельности. Данная активность, в частности обусловлена расширением деятельности теневых торговых площадок, в том числе размещенных в ДаркНете, функционирование которых приводит к все более широкому задействованию ИКТ в противоправной деятельности.

Отмеченное требует дальнейшего внедрения высоких технологий в процессуальную деятельность и совершенствование нормативно-правового регулирования рассматриваемой сферы для обеспечения эффективной борьбы с ИКТ-преступностью.

В последние годы Генеральной прокуратурой Российской Федерации во взаимодействии с федеральными органами исполнительной власти реализованы значительные мероприятия в рамках противодействия мошенничеству и кражам денежных средств с банковских счетов граждан.

Прежде всего это касается борьбы с фишинговыми атаками и социальной инженерией, где удалось пресечь деятельность мошеннических кол-центров, которые находились в местах лишения свободы. Законодательными поправками и техническими мероприятиями была повышена эффективность механизмов финансового антифрода, фильтрации трафика операторами мобильной связи. Усовершенствованы механизмы защиты персональных данных от утечек.

При этом важно понимать, что уголовно-правовые запреты и процессуальные возможности должны отвечать существующим реалиям. Для динамично развивающихся видов преступности, что особенно актуально для цифрового пространства, конструкция уголовно-правовых норм должна учитывать не просто складывающуюся криминогенную об-

становку, а, скорее, возможные будущие угрозы применения информационно-коммуникационных технологий в противоправных целях.

Проблематика своевременного выявления и раскрытия противоправных посягательств в рассматриваемой сфере связана с активностью межрегиональных организованных преступных групп, использующих методы социальной инженерии и иностранные сервисы IP-телефонии, предоставляющие возможность подмены абонентского номера.

Противодействию данным проявлениям призваны положения статьи 46 Федерального закона «О связи» и статьи 13.2.1 КоАП России, регламентирующие требования по исполнению операторами связи обязанностей, касающихся передачи в неизменном виде абонентского номера и уникального кода идентификации, а также по прекращению оказания услуг связи при наличии таких фактов. Кроме того, в указанный закон также введено требование о регистрации в ГИС «ЕСИА» сведений о владельцах сим-карт и порядке их выдачи.

Для решения вопроса, связанного с активизацией борьбы против использования персональных данных граждан в указанных противоправных схемах, с участием всех заинтересованных ведомств разработана законодательная инициатива, предусматривающая внедрение более эффективных уголовно-правовых запретов в отношении незаконного оборота персональных данных и информационных баз их содержащих, которые используются злоумышленниками при дистанционном мошенничестве с использованием методов социальной инженерии.

Отдельно отмечу, что криминализации в рамках инициативы также подлежит создание и (или) обеспечение функционирования информационных ресурсов в сети Интернет, заведомо предназначенных для незаконного хранения и распространения информации, подлежащей обработке в соответствии с требованиями законодательства в области персональных данных.

Реализация инициатив позволит обеспечить защиту конституционных прав граждан и оперативное реагирование на незаконное распространение их персональных данных с использованием информационно-коммуникационных технологий, выявление ресурсов, осуществляющих неправомерный сбор и хранение таких сведений, а также установление и привлечение их создателей и администраторов к ответственности до того момента, как наступит какой-либо ущерб или иные последствия.

Значимым фактором декриминализации ИКТ-сферы — является создание преград для незаконных финансовых операций, совершаемых с использованием различных схем по выводу денежных средств в теневой оборот.

На этом направлении в настоящее время готовятся поправки, криминализующие деятельность «дроповодов» в целях обеспечения эффективного противодействия формированию нелегального рынка платежных инструментов, предназначенных для отмывания преступных доходов.

Данная инициатива также сопровождается проработкой механизма временной блокировки операций по счетам злоумышленников в рамках проведения предварительного расследования.

Особое внимание при этом уделяется совершенствованию электронного документооборота с финансово-кредитными учреждениями, операторами связи и провайдерами Интернет услуг в целях ускорения данной процедуры.

Важным инструментом вывода нелегальных денежных средств остается криптовалюта, в которую они конвертируются с помощью нелегальных сервисов, расположенных как в России, так и за рубежом.

С учетом уже закрепленного в федеральном законодательстве подхода к понятию цифровых финансовых активов и цифровой валюты для отдельных сфер правоотношений выработаны подходы по урегулированию порядка и правил совершения процессуальных и иных действий с цифровой валютой для целей уголовного судопроизводства.

Ключевым является совершенствование законодательства, направленного на возмещение потерпевшим от преступлений рассматриваемой категории ущерба.

Одним из перспективных направлений в этой связи видится поддержанная Генеральной прокуратурой Российской Федерацией работа Банка России над законопроектом, положения которого направлены на внесение изменений в Федеральный закон № 161-ФЗ от 27.06.2011 г. «О национальной платежной системе» (№ 197920-8, принят в июле 2023 г.).

Поправки обязывают банки отказывать в исполнении распоряжений клиентов по осуществлению операций по счетам в случае наличия сведений в базе Банка России о движении средств через реквизиты предполагаемых мошенников. Причем проверка таких операций будет осуществляться одновременно и банком плательщика и банком получателя. Для вывода средств с подозрительного счета потребуется личная явка клиента в банк, что в рамках действующих мошеннических схем фактически невозможно. При этом предлагаемый центральным регулятором срок заморозки или притормаживания операций позволит гражданам осознать, что в отношении них совершаются преступные действия, а следовательно — пресечь их до наступления более тяжких последствий.

Отдельно стоит отметить разработанные критерии отнесения преступлений к сфере ИКТ, утвержденные совместным с МВД России указанием от 29.12.2021 г. № 790/11/1. Использование накапливаемых данных осуществляется в рамках внедрения в правоохранительную деятельность информационно-технических комплексов обнаружения и фиксации цифровых следов.

В частности, это касается ПТК ИБД-Ф «Дистанционные мошенничества», ИБД-Ф «НОН», АБД-Ф «Центр», задачей которых является обеспечение деятельности оперативных и следственных подразделений по противодействию преступлениям в сфере информационно-коммуникационных технологий. Одновременно на данном направлении прорабатываются варианты взаимодействия с ФСИН России, Банком России, Росфинмониторингом, Роскомнадзором.

Практическое применение системы позволило усовершенствовать работу по пресечению волокиты и необоснованной пересылки материалов процессуальных проверок по преступлениям дистанционного характера в рамках подготовки соответствующих указаний, сформулированных в совместном информационном письме Генеральной прокуратуры Российской Федерации и МВД России от 8.02.2022 г.

Внедрение соответствующих инструментов сопровождается проработкой вопросов использования электронных доказательств в уголовном процессе.

Соответствующие положения по инициативе российской делегации включены в проект всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях, разработка которой осуществляется в рамках работы учрежденного в соответствии резолюции Генеральной Ассамблеи ООН от 27.12.2019 г. № 74/247 «Противодействие использованию информационно-коммуникационных технологий в преступных целях» специального межправительственного комитета на площадке ООН.

Подводя итоги, можно констатировать, что нами активно прорабатываются и внедряются в практику современные инструменты и механизмы противодействия киберпреступности, однако для решения всего комплекса проблем одним из ключевых направлений является выработка единых подходов и вектора взаимодействия не только всех государственных структур, но и частных институтов.

Определенные шаги в этом направлении уже предприняты, однако для решения стоящих задач, прежде всего по защите граждан и населения страны, останавливаться на достигнутых результатах недопустимо.

Л.А. Осадчая
Представитель УБК МВД России

ОБ УЧАСТИИ УБК МВД В БОРЬБЕ С КИБЕРПРЕСТУПНОСТЬЮ

Добрый день, уважаемые участники форума!

Прежде всего, хотелось бы поблагодарить организаторов за возможность принять участие в данном мероприятии.

Активное развитие современных информационно-коммуникационных технологий постоянно порождает новые угрозы государственной и общественной безопасности. Как известно, с ростом количества телекоммуникационных устройств и их пользователей одновременно увеличивается число компьютерных преступлений и их потенциальных жертв.

Для противодействия указанным преступлениям в структуре

МВД России в октябре 2022 года создано Управление по организации борьбы с противоправным использованием информационно-коммуникационных технологий.

Хотелось бы отметить при этом, что работа по данной линии в системе МВД ведется уже более 25 лет, т.е. с момента создания в августе 1998 года Управления по борьбе с преступлениями в сфере высоких технологий — УБПСВТ, а далее — Управления «К» МВД России.

Поэтому сегодня работа нового подразделения основана на колоссальном профессиональном опыте и традициях, продолжателями которых являются лучшие профильные специалисты системы МВД.

На УБК *возложены функции* головного подразделения Министерства по борьбе с преступлениями, совершенными с использованием (в сфере) информационно-коммуникационных технологий, а также в области противодействия распространению противоправной информации в сети Интернет.

К *основным задачам* Управления относятся: предупреждение, выявление, пресечение и раскрытие преступлений и иных правонарушений в сфере IT-технологий, а также координация этой деятельности в системе министерства.

Подразделение также *осуществляет анализ данных*, содержащихся в информационно-коммуникационных сетях, в целях выявления запрещенного контента и пресечения этих преступлений. Например, активно осуществляется борьба с распространителями в сети Интернет материалов, содержащих детскую порнографию.

Кроме того, мы *обеспечиваем организацию взаимодействия* подразделений органов внутренних дел Российской Федерации с государственными органами, органами государственной власти субъектов страны, учреждениями финансово-кредитной сферы и иными участниками информационного обмена, включая агрегаторов больших данных.

К сожалению, в текущем году, как и в предыдущем, продолжается рост количества подобных преступлений.

Так, согласно *статистическим данным*, в период с января по июль 2023 года зарегистрировано 430 тыс. преступлений, совершенных с использованием ИКТ, что почти на 30% больше, чем за аналогичный период прошлого года (313 тыс.).

Больше половины данных преступлений (52%) относятся к категориям тяжких и особо тяжких (224,4 тыс.), более чем три четверти (77%) совершаются посредством сети Интернет (330,9 тыс.), почти половина (45%) — с использованием средств мобильной связи (193,8 тыс.). Значительная часть таких преступлений (71%) совершается путем кражи или мошенничества: (305,4 тыс.)

Только в первом полугодии 2023 года в результате совершенных с использованием ИКТ-преступлений причинен ущерб на сумму более 50 миллиардов рублей, он вырос по сравнению с прошлым годом на 5 миллиардов.

Высокая латентность данного вида преступлений обусловлена анонимностью и отсутствием непосредственного контакта злоумышленника с потерпевшим, возможностью охвата максимально широкой аудитории потенциальных жертв, удобством доступа к информации, а также трансграничным характером посягательств.

Большое влияние на увеличение количества преступлений, совершаемых с использованием IT-технологий, оказывает активное развитие новых форм платных услуг и сервисов, содержащих персональные данные граждан, а также использование при расчетах цифровых средств платежа.

Наиболее распространенными схемами телефонных мошенничеств по-прежнему остаются звонки от злоумышленников, обладающих навыками социальной инженерии, и фейковые СМС от банка.

Особую озабоченность вызывают преступления, совершаемые с использованием IT-технологий *в отношении несовершеннолетних*, в частности распространение материалов порнографического характера с участием несовершеннолетних, а также их склонение к суицидальному поведению.

В ходе реализации комплекса мероприятий, направленного на выявление и пресечение деятельности лиц, распространяющих материалы порнографического характера с участием несовершеннолетних, экспертами УБК МВД России в российском сегменте сети Интернет выявлено 260 фактов распространения «детской» порнографии в 85 регионах страны.

Благодаря взаимодействию с *Интерполом* в нашем арсенале имеется возможность использования базы данных Генерального секретариата Интерпола, содержащей изображения несовершеннолетних, пострадавших от сексуального насилия. (International Child Sexual Exploitation Database, «ICSE»). Указанная база представляет собой банк данных фотоизображений несовершеннолетних, в отношении которых были совершены преступления, база содержит около 3 миллионов записей и помогла найти и изобличить тысячи преступников.

В отчетный период также выявлено 1 223 интернет-ресурса, содержащих запрещенную к распространению на территории Российской Федерации информацию. В целях организации мероприятий по ограничению доступа к указанным ресурсам полученные сведения регулярно направляются в Роскомнадзор.

По таким материалам только в первом полугодии было возбуждено 566 уголовных дел, из которых расследовано и направлено в суд 369.

При расследовании преступлений, совершаемых с использованием ИКТ, зачастую встает вопрос об оперативном (незамедлительном) получении сведений о пользователе IP-адреса либо администраторе сервера. Однако в случае, когда указанные электронные ресурсы находятся в распоряжении компании, зарегистрированной на территории зарубежного государства, получить требуемые сведения в короткий срок не представляется возможным.

Поскольку значительная часть киберпреступлений в мире носит *транснациональный характер*, правоохранительные органы остро ощущают необходимость международного сотрудничества в целях их расследования и предотвращения. Именно поэтому мы уделяем большое внимание международному сотрудничеству.

Мы готовы к активному участию в международном многостороннем и двустороннем сотрудничестве по борьбе с киберпреступностью. Поддерживаем линию на разработку международной стратегии комплексного противодействия киберугрозе и создание единых международно-правовых механизмов с целью унификации национальных уголовных законодательств.

Важным фактором строительства системы международной информационной безопасности и защиты граждан в информационном пространстве является активизация взаимодействия по международному каналу сети Национальных контактных пунктов.

Они были созданы для противодействия преступлениям в сфере высоких технологий и для информационного обмена с киберподразделениями органов внутренних дел стран-участников указанной Сети. Это про-

изошло в 1998 году по итогам саммита Большой Восьмерки в рамках работы подгруппы по борьбе с преступлениями в сфере высоких технологий Римско-Лионской группы. Такой пункт активно работал в структуре Управления «К».

Однако, в последние годы активность информационного обмена в этом звене существенно ослабла, что не идет на пользу борьбе с киберпреступлениями. Полагаем целесообразным совместно с заинтересованными ведомствами активизировать работу контактных пунктов, чтобы в оперативном режиме обмениваться с зарубежными коллегами информацией технического характера для совместного расследования компьютерных преступлений и актов компьютерного терроризма, обеспечивать сохранение данных до последующего направления запроса о правовой помощи.

Спасибо за внимание.

П.А. Литвишко
Заместитель начальника Главного управления международно-правового сотрудничества Генеральной прокуратуры РФ — начальник управления правовой помощи и правоохранительного содействия

О РОССИЙСКИХ ИНИЦИАТИВАХ ПО ПРОТИВОДЕЙСТВИЮ ПРОТИВОПРАВНОМУ СБОРУ ДОКАЗАТЕЛЬСТВ В КИБЕРПРОСТРАНСТВЕ ПРЕДСТАВИТЕЛЯМИ ИНОСТРАННЫХ ГОСУДАРСТВ И МЕЖДУНАРОДНЫХ ОРГАНОВ

Как известно, киберпространство включает в себя ряд уровней (слоев), центральный из которых составляет логический (виртуальный) уровень, не имеющий материальных географических границ. В то же время физический, технологический субстрат (носитель) киберпространства образует ИКТ-инфраструктура (аппаратно-программное обеспечение), географически локализированная в пределах отдельных государств, включающая в себя в том числе оборудование пользователей (которые, в свою очередь, образуют социальный слой) и имеющих конкретную национальность провайдеров ИКТ-услуг и иных кастодианов данных.

Так, на глобальном международном уровне признается, что суверенитет государств и международные нормы и принципы, проистекающие из суверенитета (такие как невмешательство во внутренние дела других государств), применяются к осуществлению государствами деятельности, связанной с ИКТ, и к их юрисдикции над ИКТ-инфраструктурой, расположенной на их территориях[1]. Поэтому страны, как правило, склонны расценивать дистанционные действия представителей иностранного государства, осуществляемые с его территории и физически достигающие лиц (объекты), заведомо находящихся (расположенных) в указанных странах, в качестве предпринимаемых в пределах их собственной территории; к таким действиям относятся трансграничные контакты по сетям любой связи с лицами, заведомо находящимися и использующими оконечное оборудование на территории соответствующей страны. В случае таких действий без ведома ее властей они могут расцениваться как нарушающие международно-правовые принципы суверенного равенства государств, невмешательства во внутренние дела другого государства, образовывать преступление или иное правонарушение, либо международно-противоправное деяние.

Показательным с точки зрения различной оценки затронутыми государствами правомерности трансграничных обысков и выемок данных в информационных системах и сетях является известное уголовное дело начала 2000-х годов «США против российских хакеров А. Иванова и В. Горшкова», которых американские агенты путем проведения легендированного мероприятия в Интернете выманили из России в США. В рамках оперативного эксперимента от них получили средства доступа к их российским информационным ресурсам; затем в отношении данных ресурсов в одностороннем порядке были проведены трансграничные обыск и выемка. Иванов и Горшков были осуждены в США, а российскими следственными органами в отношении американского агента, проводившего названные обыск и выемку, возбуждено уголовное дело о неправомерном доступе к компьютер-

1 Резолюция Генеральной ассамблеи ООН 73/27 от 5.12.2018 «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности».

ной информации, совершенном лицом с использованием своего служебного положения.

Текущая геополитическая обстановка, системные недружественные действия правоохранительного и судебного характера в отношении нашего государства, предпринимаемые странами «коллективного Запада» и рядом международных органов и организаций, сокращение, либо отсутствие возможностей взаимного антикриминального сотрудничества привели к осознанию высокой актуальности и существенно ускорили выработку нормотворческих инициатив по защите Россией своего географического и информационного суверенного пространства от таких действий, в том числе с использованием опыта тех же западных стран.

1. Для предупреждения рассматриваемых ситуаций Российской Федерацией, начиная с 2022 г. в заключаемые двусторонние межправительственные соглашения о сотрудничестве в области обеспечения международной информационной безопасности вносится норма о запрете одностороннего трансграничного доступа[2].

2. В целях предотвращения односторонних трансграничных негласных оперативно-разыскных мероприятий в киберпространстве путем установления четких требований об обращении с международным запросом о правовой помощи или правоохранительном содействии для их проведения, а также к содержанию такого запроса Российской Федерацией в разрабатываемый в рамках ООН проект всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях внесена соответствующая статья о специальных методах расследования (в текущей редакции проекта — ст. 48 bis)[3].

Несмотря на классический характер подобной нормы, имеющейся в действующих универсальных и региональных конвенциях, со стороны развитых кибердержав коллективного Запада, заинтересованных сохранять в правовой серой зоне свои односторонние проактивные трансграничные кибероперации т.н. правительственного хакинга, такие попытки установить минимальные универсальные правила их проведения вызывают ожесточенное сопротивление.

3. В целях противодействия принятию иностранными и международными органами односторонних мер по нелегитимному самостоятельному сбору доказательств, включая электронные, и иных сведений в Российской Федерации, в том числе посредством дистанционных трансграничных контактов из-за рубежа с физическими и юридическими лицами, находящимися на территории Российской Федерации, проведению мероприятий по выманиванию таким путем российских граждан за рубеж в целях их задержания, Генеральной прокуратурой РФ с учетом зарубежного опыта разработан проект «блокирующего» федерального закона (ст. 294[1]. Незаконное осуществление следственных, иных процессуальных действий и оперативно-розыскных мероприятий на территории Российской Федерации), который в настоящее время находится на рассмотрении в Государственной Думе Федерального Собрания РФ.

В случае принятия закона он будет криминализировать, в том числе неприемлемые для России действия, аналогичные предусмотренным п. «b» ст. 32 Будапештской конвенции о киберпреступности 2001 г. (Россия в ней из-за наличия данного положения не участвует).

4. В России сейчас совершенствуются и другие аспекты легитимизации сохранения и предоставления электронных доказательств как по иностранным, так и российским запросам, направленные на обеспечение своего и чужого суверенитета в информационном пространстве.

Так, в Государственной Думе Федерального Собрания РФ рассматривается разработанный Генеральной прокуратурой РФ (также с учетом зарубежного опыта) законопроект, направленный на имплементацию в УПК РФ норм международного права о проведении за рубежом допросов, в том числе путем использования систем видео-конференцсвязи (вид электронного доказательства), консульскими

2 Соглашение между Правительством Российской Федерации и Правительством Азербайджанской Республики о сотрудничестве в области обеспечения международной информационной безопасности от 24.06.2022 г. (ст. 2).

3 Заявление делегации Российской Федерации на пятой сессии Спецкомитета по разработке всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях (Вена, 11–21 апреля 2023 года). URL: https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home (дата обращения: 15.09.2023).

должностными лицами РФ в дипломатических представительствах и консульских учреждениях РФ[4].

В соответствии с планом работы межведомственной рабочей группы по противодействию информационной преступности на 2023 год, утвержденным заместителем Генерального прокурора РФ 26.12.2022 (п. 6–7), осуществляются:

- проработка вопроса о закреплении в российском законодательстве обязанности операторов связи и организаторов распространения информации в сети «Интернет» обеспечивать сохранение «электронных доказательств» по запросам российских и иностранных компетентных органов, связанным с расследованием или судебным рассмотрением уголовного дела, свыше установленных действующим законом сроков их хранения в случаях истечения этих сроков, а также допустимых сроков обеспечения их сохранности и установлении административной ответственности за нарушение такой обязанности;
- подготовка предложений по совершенствованию организации направления и исполнения запросов российских правоохранительных органов о сохранении и предоставлении «электронных доказательств», адресуемых филиалу или представительству иностранного лица, осуществляющего деятельность в сети «Интернет» на территории Российской Федерации, либо российскому юридическому лицу, учрежденному иностранным лицом, осуществляющим деятельность в сети «Интернет» на территории Российской Федерации (то есть так называемым «приземленным» иностранным ИТ-компаниям), на основании ст. 7 Федерального закона от 01.07.2021 № 236-ФЗ «О деятельности иностранных лиц в информационно-телекоммуникационной сети »Интернет« на территории Российской Федерации».

Реализация перечисленных инициатив позволит существенным образом укрепить цифровой суверенитет России в антикриминальной сфере.

4 Проект федерального закона № 280226-8 «О внесении изменений в статьи 453 и 456 Уголовно-процессуального кодекса Российской Федерации» (по вопросу о консульской функции по выполнению отдельных процессуальных действий по уголовным делам по запросам компетентных органов представляемого государства).

Н.В. Михайленко
Доцент кафедры противодействия преступлениям в сфере информационно-телекоммуникационных технологий Московского университета МВД России имени В.Я. Кикотя, кандидат юридических наук; заместитель руководителя образовательного проекта «Университет цифровой полиции» (секция Центр компетенций); вице-президент Московского регионального отделения Международной полицейской ассоциации

АРХИТЕКТУРА УПРАВЛЕНЧЕСКОГО ПРОЦЕССА ПРИ РАССЛЕДОВАНИИ IT-ПРЕСТУПЛЕНИЙ В СОВРЕМЕННЫХ РЕАЛИЯХ

В сложившихся условиях цифровизации государственного управления выходит на передний план повышение эффективности управленческого процесса: это и знание основ проектного менеджмента с использованием цифровых технологий и планирование своей работы, включая долгосрочное планирование; и развитие и расширение базовых и специальных навыков сотрудников органов внутренних дел при расследовании IT-преступлений. Количество имеет устойчивую тенденцию роста. В действительности, система организации работы органов внутренних дел при расследовании ИТ-преступлений является сложной системой.

В целях повышение эффективности управленческого процесса при расследовании IT-преступлений целесообразно сосредоточить внимание на следующих задачах:

1. Повышение эффективности научно-методического обеспечения деятельности по борьбе с преступностью в сфере высоких технологий.

Например. *В ходе проводимого мониторинга законодательства и участия в заказных научно-исследовательских работах при участии нашего Университета подготовлен ряд изменений в законодательство в области кибербезопасности, направлены предложения по совершенствованию информационного обмена, в том числе: возможности рассмотрения вопроса перехода на электронный документооборот, разрешение проблемных вопросов в области борьбы с IT-преступлениями в кредитно-банковской сфере, преступлениями, совершаемыми с использованием цифровых активов и цифровых прав, IT-преступлениями, посягающими на объекты критической инфраструктуры (и иными), а также в области межведомственного нормативного регулирования применения искусственного интеллекта.*

В Университете функционирует инновационное образовательное пространство на основе интеграции отдельных структур, осуществляющих учебную, учебно-методическую и другие работы. С 2020 года в Университете созданы и реализуются учебно-научные проекты «Школа киберполиции», «Университет киберполиции» в рамках постоянно действующей рабочей группы по совершенствованию образовательного процесса в условиях цифровой трансформации и исследования вопросов противодействия преступлениям в сфере информационно-телекоммуникационных технологий (функционирует с 2016 года).

2. Совершенствование системы правоприменения и разработке новых форм и методов борьбы с преступлениями, совершаемыми с использованием высоких технологий (методическое обеспечение).

Хорошо продуманная и составленная методология противодействия киберпреступлениям помогает успешно использовать законодательные акты в практической работе. В силу

разнородности нормативной базы (правоохранительных органов и иных государственных учреждений, общественных организаций, коммерческих структур) неизбежно возникают проблемы взаимодействия в процессе правоприменения, которые не позволяют эффективно противодействовать преступности. Несогласованность субъектов предупреждения преступлений в этой сфере зачастую предоставляет дополнительные возможности для преступных комбинаций.

3. Принятие организационно-управленческих мер.

Ключевым моментом здесь стало выступление Президента Российской Федерации на расширенной Коллегии МВД России 3 марта 2021 года, в котором обращено внимание, что вопросы противодействия киберпреступлениям в широком смысле являются приоритетными в связи со стремительным развитием цифровизации и интенсивной информатизации общества, вызывающими риски и угрозы использования информационных технологий и средств телекоммуникаций в незаконной плоскости. Президент указал: «Ваша задача — эффективно ответить на этот криминальный вызов, защитить граждан и добросовестный бизнес, который активно осваивает цифровое пространство. Для этого важно своевременно информировать людей о способах защиты от мошенников, повышать профессиональную подготовку и техническое оснащение органов внутренних дел. И, конечно, нужно наладить более четкое взаимодействие с банковским сообществом, интернет-провайдерами, операторами сотовой связи». Это в полной мере относится ко всей правоохранительной системе.

Соответственно к ним следует отнести:

3.1. Вопросы кадровой политики.

Цифровые технологии предоставляют новые инструменты для работы при расследовании IT-преступлений, что обуславливает необходимость обновления архитектурных компетенций сотрудников, участвующих в расследовании IT-преступлений.

Сохраняется «дисбаланс поколений» среди преступников и работников правопорядка, при котором последним довольно часто попросту не хватает компетенций использовать передовые технические разработки.

Непрерывное формирование, развитие и увеличение компетенций руководителей и сотрудников органов внутренних дел является насущной необходимостью для успешной и продуктивной деятельности.

Существует несколько уровней повышения организации служебной деятельности органов внутренних дел: базовые знания, специальные познания, профилактика коррупции внутри подразделений, организация взаимодействия внутри правоохранительной системы и на уровне государственно-частного партнерства.

Знания, навыки, которыми должны обладать сотрудники органов внутренних дел для эффективного противодействия IT-преступлениям, включают общие базовые навыки и компетенции.

Отдельно следует указать на пока еще существующую необходимость привлечения квалифицированного специалиста при проведении осмотра места происшествия, обыска и в случаях выемки, но в перспективе, при получении новых навыков, этого, возможно, и не потребуется.

Важным в преодолении «кадрового голода» является развитие прежде всего государственных проектов, направленных на подготовку и обучение квалифицированных специалистов в рассматриваемой области.

Это и подготовка сотрудников правоохранительных органов по специальностям «Защита информации и информационно-телекоммуникационных сетей», «Информационная безопасность» в образовательных учреждениях МВД, ФСБ, МО, ФТС России и др. Данная мера позволит обеспечить комплектование правоохранительных органов компетентными и профессиональными сотрудниками. Частью данной системы являются проводимые на регулярной основе курсы повышения квалификации, стажировки в практических органах, обмен опытом, семинары и круглые столы для сотрудников и профессорско-преподавательского состава вузов в государственных образовательных учреждениях, а также российских компаниях, занимающихся информационной безопасностью.

Только опираясь на опыт и заглядывая в будущее можно уловить настоящее в его подлинности. Принимая во внимание данный фактор, следуя общегосударственной стра-

тегии развития, по указанию руководства МВД России 11 июля 2022 года в Московском университете МВД России имени В.Я. Кикотя была создана кафедра противодействия преступлениям в сфере информационно-телекоммуникационных технологий. Создание кафедры явилось своевременным и справедливым решением.

Важным шагом стало создание в системе МВД России Указом Президента Российской Федерации от 30 сентября 2022 г. № 688 «О внесении изменений в некоторые акты Президента Российской Федерации» Управления по организации борьбы с противоправным использованием информационно-коммуникационных технологий (УБК МВД России), как головного подразделения в осуществлении функций по борьбе с киберпреступлениями, положение о котором утверждено Приказом МВД России от 29 декабря 2022 г. № 1110 «Об утверждении Положения об Управлении по организации борьбы с противоправным использованием информационно-коммуникационных технологий Министерства внутренних дел Российской Федерации».

3.2. Переход к функциональному, стараясь не прибегать к используемому в большинстве случаев территориальному принципу работы в сфере предупреждения киберпреступности.

Существующая структура правоохранительных органов и принципы организации работы их отдельных подразделений вызывают проблемы координации как внутри этих ведомств, так и в рамках межведомственного взаимодействия. Одной из главных особенностей преступности в сфере ИКТ является ее многоэпизодность и трансграничный характер.

3.3. Совершенствование информационно-аналитического и технического обеспечения деятельности правоохранительных органов.

Как видится, при таких условиях очередной рывок может быть сделан при продолжении использования последних достижений науки и техники в области противодействия преступлениям в сфере информационно-телекоммуникационных технологий.

Данная работа связана с решением целого ряда задач, включающих сбор и систематизацию криминологически значимой информации, ее анализ и классификацию, определение на этой основе реальной картины состояния дел и перспективное прогнозирование развития ситуации. Эта работа имеет смысл лишь при четкой интеграции ее результатов в законодательную деятельность и правоохранительную практику.

Другим немаловажным аспектом при расследовании IT-преступлений является использование и применение технологий и различных методик, среди которых машинное обучение, внедрение в процесс работы технологий искусственного интеллекта и другие. Внедрение машинного обучения доказало свою состоятельность в области Legal Tech, и широко используется в сфере онлайн-консультирования и электронного документооборота. Немаловажным сегментом в информационно-технологическом сопровождении выступает и система распознавания речи. Система распознавания лиц является одной из наиболее распространенных систем, применяемых российской полицией. К примеру, с помощью таких систем возможно обнаружить в толпе лицо и в это же время сверить его с изображениями людей в имеющихся базах данных.

3.4. Организация взаимодействия (межведомственное взаимодействие, взаимодействие со средствами массовой информации и с общественными организациями, государственно-частное партнерство, международное сотрудничество).

4. Проведение комплекса целенаправленных мероприятий по устранению причин и условий, способствующих совершению киберпреступлений в отношении государственных и иных учреждений, предприятий и организаций (кибергигиена и киберэтика).

В условиях значительного увеличения количества преступлений, совершенных с использованием информационно-коммуникационных технологий, особое значение приобретают: повышение эффективности управленческого процесса при расследовании IT-преступлений; подготовка специалистов, которые будут обладать необходимыми знаниями, умениями и навыками противодействия данным преступлениям; использование цифровых технологий. В этой связи целесообразно продолжить цифровую трансформацию органов

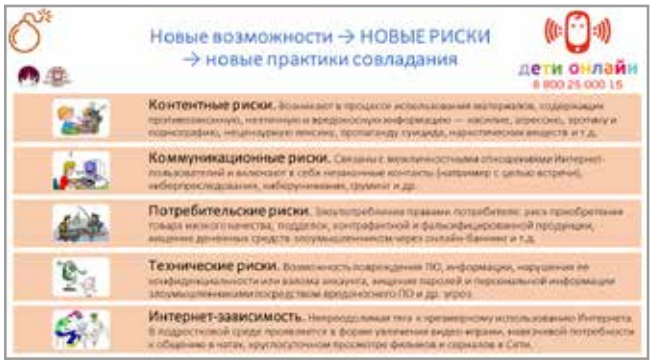
внутренних дел в условиях обеспечения кибербезопасности, обеспечить научную преемственность в рамках разработки основ функционирования; рассмотреть возможность создания алгоритма по адаптации действующего законодательства и правоприменительной практики в условиях ускоренной цифровизации общества.

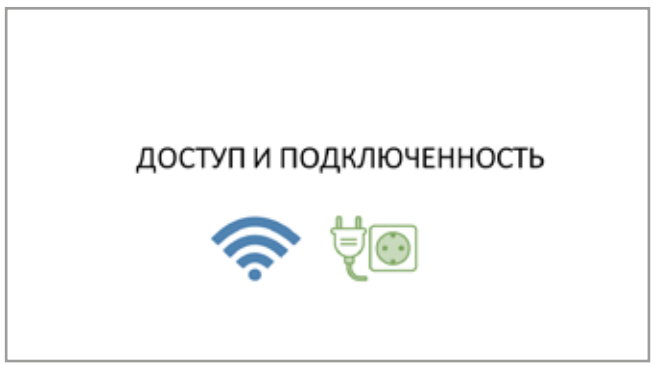
КРУГЛЫЙ СТОЛ № 5
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ДЕТЕЙ, ПОДРОСТКОВ И МОЛОДЕЖИ В УСЛОВИЯХ ЦИФРОВЫХ ТРАНСФОРМАЦИЙ: ПРИОРИТЕТЫ, ПРИНЦИПЫ И МЕХАНИЗМЫ ОБЕСПЕЧЕНИЯ

Ведущий:
Солдатова Г.В., профессор МГУ им. М.В. Ломоносова, академик Российской академии образования

Г.В. Солдатова
Академик РАО, профессор факультета психологии МГУ им. М.В. Ломоносова, директор Фонда Развития Интернет

ПОКОЛЕНИЕ ЦИФРОВОЙ СОЦИАЛИЗАЦИИ В СМЕШАННОЙ РЕАЛЬНОСТИ: НОВЫЕ РИСКИ И БЕЗОПАСНОСТЬ





Степень подключенности (пользовательская активность, экранное время)

Экранное время – количество часов за экраном смартфона, планшета, приставки, компьютера или телевизора

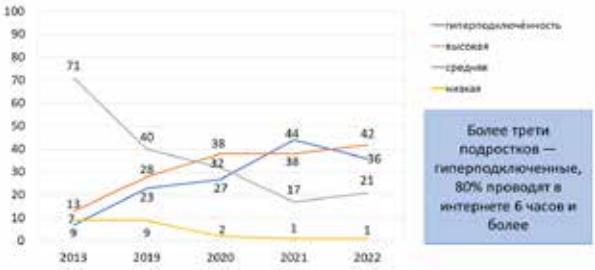
тип пользовательской активности, при котором половина времени бодрствования субъекта опосредована цифровыми устройствами

Пользовательская активность	Низкая	Средняя	Высокая	ГИПЕР-ПОДКЛЮЧЕННОСТЬ
	< 1 ч/день	<3 ч/день	< 6 ч/день	> 8 ч/день

Большинство подростков (78%) недооценивают экранное время

Цифровое неравенство в ограниченности или отсутствии доступа к использованию новых технологий — один из вероятных механизмов влияния цифровизации на благополучие детей

Динамика пользовательской активности подростков: с 2013 г. число гиперподключенных выросло в пять раз



Более трети подростков — гиперподключенные, 80% проводят в интернете 6 часов и более

Насыщенная цифровая среда+перманентность взаимодействия с ней

Источник изображений: нейросеть Kandinsky

Риски гиперподключенности

Чрезмерная увлеченность интернетом

Проблемное использование интернета

Интернет-зависимость – применение технологий во вред себе и другим, порождает конфликт с другими сферами жизни и потерю контроля над своим временем

Зависимость от видеоигр

МКБ-11
С 2022 года включена в классификацию
6C51 Gaming disorder

DSM-V
Internet gaming disorder
включено в III раздел, как феномен, требующий дополнительных клинических исследований

Последствия:
- Больше возможностей встретиться с различными рисками
- Нарушения режима сна/хронические недосыпания/бессонница
- Снижение физической активности, гиподинамия
- Хроническая усталость глаз/снижение остроты зрения
- Последствия для психологического благополучия: личностные, социальные, когнитивные и т.д.

СМЕШАННАЯ РЕАЛЬНОСТЬ

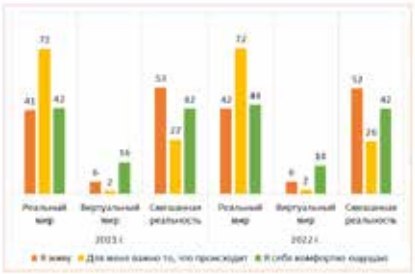
Смешанная (конвергентная) реальность, как основа новой социальной ситуации развития

Смешанная (конвергентная) реальность – киберфизическая среда, характеризующаяся сложной системой физических, социальных и виртуальных субъектов, объектов и стимулов, которые представлены одномоментно в рамках единого временно-пространственного континуума и единого (целостного) восприятия его участниками

Смешанная реальность характеризуется размыванием границ между онлайн- и офлайн-мирами и диктует необходимость усвоения новых норм и правил взаимодействия с ней, а также технологий, с помощью которых возможна реализация этого взаимодействия

Переживание ребенком смешанной (конвергентной) среды своего обитания и себя в этой среде составляет основу его социальной ситуации развития в XXI веке. В смешанной реальности **благополучие, как интегральное ощущение удовлетворенности, комфорта и счастья**, не может не учитывать всех аспектов новой киберфизической среды.

Каждый второй подросток живет в смешанной реальности



Для подростков однозначно наиболее важен реальный мир.

Каждый второй подросток ощущает, что живет в смешанной реальности, почти половина опрошенных чувствует себя комфортно как в реальном мире, так и в смешанной реальности.

В недалеком будущем подростки будут осваивать метавселенные – конвергенцию физической, дополненной и виртуальной реальностей в общем онлайн-пространстве

Общение, обучение, игры в смешанной реальности

Деструктивные коммуникационно-контентные риски – онлайн-риски смешанной реальности

Рекрутинг в экстремистские сообщества, манипулятивное воздействие, распространение радикальных идей
Одно из самых опасных последствий распространения рисков подобного рода – это переход от действий в Сети к действиям в реальной жизни. К таким последствиям относят преступления на почве ненависти по расовому, религиозному, половому признаку и др (Keipi T. et al., 2016).

АУЕ – движение, которое признано экстремистским на территории Российской Федерации
Тюремно-криминальная субкультура (АУЕ – «арестантский уклад единя), изначально существовавшая в стенах исправительных учреждений, в частности с помощью онлайн-сообществ популяризируется среди подростков, становясь частью молодёжной культуры.

Колумбайн или school shooting (Верховный суд России признал террористическими и запретил 19 января, 1922 г.)
В 1999 году два старшеклассника школы «Колумбайн» в США Э.Харрис и Д.Клибольд устроили массовое нападение, после чего совершили самоубийство (Schildkraut, Muschert, 2019; Flowers, Pixley, 2020). Случай вызвал широкий общественный резонанс и привёл к появлению подражателей, в том числе и в России (Vith, 2019).

Рекрутинг в наркокурьеры и пропаганда употребления психоактивных веществ
Контент втягивает подростков и молодёжь в наркотрафик в качестве курьеров, а также популяризует наркотические вещества, демонстрируя их как норму «молодёжной» культуры. Стремление заработать быстрые деньги оборачивается тюремным сроком. Период безнаказанной работы закладчиком длится от 3-х дней до 5 месяцев.

Риски смешанной реальности

- Сложности в адаптации к гибридному миру (переходы между мирами, совмещение и замещение миров)
- Проблемы деятельности в множественной реальности
- Риски адаптации к разным виртуальным средам
- Различия когнитивных процессов и психологических феноменов в разных мирах
- Риски расщепления личности

РАСШИРЕННАЯ ЛИЧНОСТЬ

Технологически достроенное (расширенное) «Я»: риски развития

Новые технологии как часть внешней среды, **«расширяют» личность**, они **достраивают когнитивную, личностную и социальную систему** человека, интегрируются с ней и видоизменяют ее.

Человек достроенный – это единый организм, а не организм, просто использующий что-то из своего окружения. **Это организм, достроивший себя и уже нежизнеспособный (в своем новом качестве) без этих достроек** (Иосиф Фейгенберг)

Риски расширенной личности

- Снижение жизнеспособность без «достроек»
- Безопасность цифровой личности
- Чрезмерное расширение личности за пределы границ индивидуального
- Снижение чувства телесности, способности понимать и интерпретировать тело
- Редукция практик самопознания исключительно к цифровым
- Иллюзия цифрового бессмертия
- Фобии, связанные с отсутствием гаджетов и цифровых платформ
- Перекладывание на цифровые устройства все больше функций
- Потеря, размывание и расщепление идентичности
- Сращивание когнитивных систем с цифровой средой и сложными интеллектуальными системами

2022 г. Подростки и молодёжь 14-30 лет

Риски расширенной личности: цифровые устройства, цифровые среды, искусственный интеллект

70% российских школьников 12-13 лет общались с Алисой, Сири и Алексой

Подростки демонстрируют высокий уровень доверия к голосовым помощникам

Подростки чаще взрослых знают или используют интернет вещей и ИИ

Подростки активнее взрослых готовы использовать новые цифровые умные вещи: умные дома, беспилотные такси, ИИ-врачей. Соревновались в роботе-вкруге и меньше всего хотели ИИ-учителей

За новейные годы в два раза выросло число подростков, которые использовали Интернет вещей (**до 60 процентов**), в три раза ИИ (**треть подростков**).

По данным исследования 2019 г.

Опасность сращивания когнитивных и личностных систем с цифровой средой и ИИ

- дефицит развития высших психических функций
- выученная беспомощность
- снижение самооценки
- экзистенциальные кризисы
- деградация человеческих функций
- дезадаптация в физической среде
- потеря контроля над цифровыми устройствами
- потеря контроля над персональными данными
- утрата человеческой автономии и неспособность принимать решения без ИИ
- излишнее доверие к гаджетам и ИИ
- конкуренция с ИИ
- поглощение личности
- риски киборгизации и расчеловечивания

Обращение за поддержкой при столкновении с онлайн-рисками

Основную поддержку подросткам оказывают его **друзья**. К родителям подростки обращаются довольно редко (менее трети). Каждый шестой в принципе хранит в тайне случившееся. Лишь немногие готовы рассказывать о произошедшем специалистам и учителям.

Цифровая компетентность, как главный навык XXI века

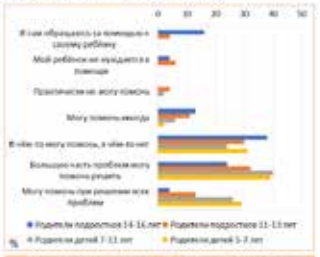
Цифровая компетентность

– готовность и способность личности применять инфокоммуникационные технологии уверенно, эффективно, критично и безопасно в разных сферах жизнедеятельности (информационная среда, коммуникации, потребление, техносфера) на основе овладения соответствующими компетенциями, как системой знаний, умений, ответственности и мотивации.

Солдатова Г. У., Нестик, Т. А., Рассказова, Е. И., Зотова, Е. Ю. Цифровая компетентность подростков и родителей. Результаты всероссийского исследования /М.: Фонд Развития Интернет. – 2013.

Цифровая компетентность детей и родителей

ИЦК подростков постепенно растёт с каждым годом.



Родители миллениалы уверены в своей способности помочь своим детям. Родители подростков менее уверены в своей компетентности.

Родители-миллениалы поколения Альфа: цифровой разрыв сокращается

- ✓ Активные пользователи Интернета
- ✓ Склонны к цифровому образу жизни
- ✓ Технофилы
- ✓ Не представляют будущего своих детей без интернета и технологий
- ✓ Видят в технологиях образовательный потенциал
- ✓ Имеют неплохой уровень цифровой грамотности
- ✓ Стремятся дать детям наилучшие возможности, в том числе цифровые новинки

Комплексный и системный подход к развитию цифровой компетентности

Риски: индивидуальные и коллективные механизмы регуляции и профилактики

Больше возможностей решения проблемы «снизу»

Развитие цифровой компетентности, саморегуляции, критического мышления, коммуникативной компетентности и т.д. ДЕТИ, СЕМЬЯ и ШКОЛА

Риски гиперподключенности – интернет-зависимость
Риски смешанной реальности – риски адаптации к новой реальности, расщепление личности, когнитивные сложности
Риски расширенной личности – потеря и размывание идентичности, «поглощение» личности, сращивание когнитивных систем с цифровой средой
Риски цифровой социальности – киберагрессия, фейки, информационная перегрузка, цифровая этика

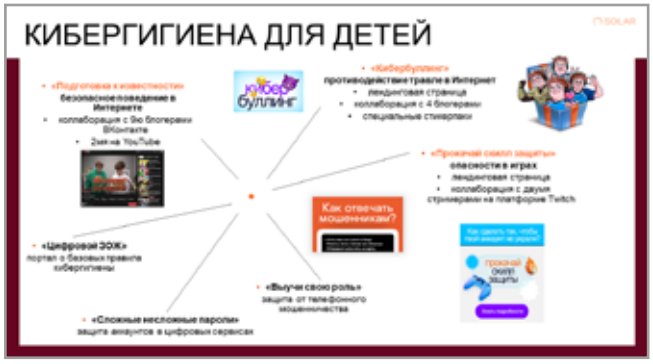
Необходимость вмешательства «сверху»

Совместные усилия государства и IT-индустрии при экспертизе институтов социализации

Риски гиперподключенности – цифровое неравенство
Риски смешанной реальности – потеря цифровой личности
Риски расширенной личности – потеря цифровой личности; регуляция этики киборгизации
Риски цифровой социальности – запрещенный контент, вовлечение подростков в онлайн-мошенничество, целевой маркетинг, сбор, использование и раскрытие личной информации детей, кибератаки

Е.Ю. Амелькина
Менеджер по взаимодействию с государственными органами «Ростелеком-Солар»

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ДЕТЕЙ, ПОДРОСТКОВ И МОЛОДЕЖИ В УСЛОВИЯХ ЦИФРОВЫХ ТРАНСФОРМАЦИЙ: ПРИОРИТЕТЫ, ПРИНЦИПЫ И МЕХАНИЗМЫ ОБЕСПЕЧЕНИЯ



А.А. Воробьев
Директор Координационного центра доменов RU/РФ

СИСТЕМА УПРАВЛЕНИЯ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ ДОМЕННОГО ПРОСТРАНСТВА (ГЛОБАЛЬНОГО ДОМЕННОГО ПРОСТРАНСТВА, НАЦИОНАЛЬНЫХ ДОМЕННЫХ ЗОН)

Безопасность российского доменного пространства является одной из важнейших задач Координационного центра доменов .RU/.РФ. Мы не только проводим большую работу в рамках наших проектов «Нетоскоп» и «Доменный патруль», но и изучаем опыт других регистратур национальных доменов в этом направлении. Ещё в 2012 году Координационный центр внедрил практику взаимодействия с организациями, компетентными в определении нарушений в сети Интернет. Такие организации предоставляют Координационному центру и регистраторам доменных имен информацию о ресурсах с противоправным контентом, о случаях фишинга, несанкционированного доступа к информационным системам и распространения вредоносных программ с доменных имен, находящихся в зонах.РФ/.RU. Регистраторы вправе прекратить делегирование доменных имен для подобных ресурсов. Сегодня с Координационным центром сотрудничают 96 аккредитованных регистраторов и 12 компетентных организаций — Национальный координационный центр по компьютерным инцидентам, Лига безопасного интернета, F.A.C.C.T., Лаборатория Касперского, RU-CERT, РОЦИТ, Роскомнадзор, BI.ZONE, Банк России, Доктор Веб и Интеграл.

Слайд 2

Вопросы безопасности сети и защиты пользователей от фишинга стали ключевыми темами обсуждений на конференции 11–13 сентября 2023 г. TLDCON 2023. Так, по данным:

- Лаборатории Касперского: за I полугодие 2023 года нейтрализовано свыше 1,5 млрд веб-атак, среди которых 462 млн вредоносных URL-адресов и около 80 млн вредоносных объектов.
- Координационного центра: с начала 2023 года в зонах .RU и. РФ заблокировано более 33 тысяч фишинговых доменов. Чаще всего мошенники имитируют бренды Авито, Youla, Ozon, Сбербанк, Альфа банк, Telegram, Yandex, VK, Booking и Nalozhka.
- OZON: каждый второй россиянин попадался на мошенничество при онлайн-покупках, и треть из них потеряла при этом более 5000 рублей.
- F.A.C.C.T.: из заблокированных компанией фишинговых доменов в зонах .RU и .РФ 35% пришлось на онлайн-сервисы, 28% — на финансовые учреждения и 21% — на службы доставки. При этом доля фишинга в зоне .RU невелика и составляет всего 5% от общего числа обнаруженных фишинговых страниц, а в зоне. РФ — менее 1%.
- BI.ZONE: расходы мошенников на создание, поддержание и рекламу одного фишингового сайта составляют 5000–7000 рублей. При этом доходы от фишинга могут составлять до 1 млрд рублей в год.

Слайд 3

1. **Однако перечисленные проблемы безопасности имеют не только национальный, российский характер, но и глобальный международный характер.** Фишинговые атаки

все чаще организуются нерезидентами и не с национальной территории жертв, но с использованием как национальных доменов атакованной территории, так и доменов из других национальных юрисдикций.

2. Много внимания уделяет этой проблеме и ICANN. Хотя фишинг выходит за рамки компетенций и полномочий ICANN, но все же Корпорация дает определение этому международному явлению: **«Фишинг» — это процесс использования электронной почты и/или веб-сайтов для неправомерного получения имен пользователей, паролей и финансовой информации.**
3. В сложившейся геополитически напряженной ситуации проблемы совместного международного обеспечения безопасности национального ИКТ-пространства все более актуальны. Однако, отсутствие взаимного доверия или **проблемы преодоления недоверия при техническом взаимодействии и обмене технологиями пока недостаточно проработаны.**

Одна из целей проекта Конвенции по международной информационной безопасности, внесенной Россией в ООН — укрепление доверия и развитие сотрудничества государств в сфере международной информационной безопасности в целях преодоления напряженности, возникшей в результате злонамеренного использования информационно-коммуникационных технологий.

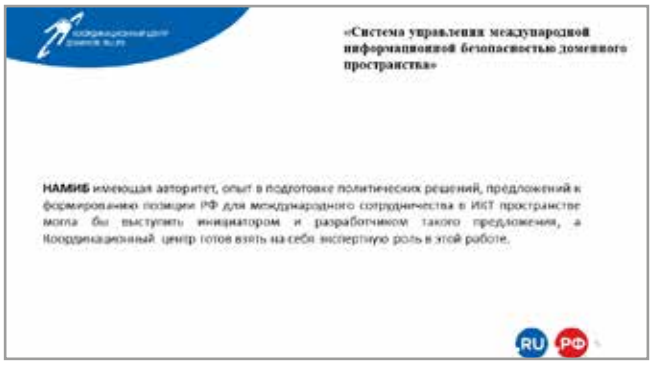
Укреплять доверие и развивать сотрудничество в области обеспечения международной информационной безопасности Россия призывает при помощи предоставления друг другу данных о национальном законодательстве в этой сфере, оперативного обмена информацией о кризисных событиях и угрозах в киберпространстве, разработки стандартизированного набора технической информации, необходимой для передачи в целях реагирования на соответствующие инциденты, а также проведения консультаций между странами.

Об этом же говорят и наши зарубежные эксперты: «Своевременное распределение индикаторов угроз будет работать только в среде, где сохраняется доверие. Доверие — это не вопрос технологии, но языка политики и структурированного понимания проблем.

Таким образом, мы видим, что это явление относится к системе общей проблематики международной информационной безопасности в ИКТ-пространстве.

Слайд 4

В этой связи Координационный центр доменов .RU/.РФ. предлагает для рассмотре-



ния Систему международного сотрудничества в области управления международной информационной безопасностью доменного пространства (глобального доменного пространства, национальных доменных зон).

Важным направлением международного сотрудничества в области предотвращения и урегулирования инцидентов в ИКТ-среде, по мнению Группы правительственных экспертов является создание системы контактных пунктов на политическом и техническом уровнях. В отсутствии доверия международное сотрудничество в противодействии использованию доменов в злонамеренных целях имеет ограниченный характер, не позволяющий создать рабочую экосистему полного цикла, способную решать проблемы на глобальном уровне. Мы предлагаем выделить хотя бы одну или несколько важных задач (на начальном этапе сотрудничества): **Разделегирование скомпрометированного домена по запросу международного партнера и на основе формально прописанного протокола взаимодействия международных и национальных операторов (Регистратуры, Регистраторы, Компетентные организации) по взаимодействию.**

Предлагаемый подход, по нашему мнению, и мнению международных экспертов, решается исключительно на политическом уровне и поможет противодействию фишингу, как международному вызову, а также будет способствовать формированию и последующему укреплению доверия.

Цель: Разработка научно-обоснованных предложений по подходам к решению проблемы создания системы международной информационной безопасности доменного пространства (СМИБдп), которая должна базироваться на взаимодействии государственных и коммерческих организаций, обладающих объектами национальных сегментов ИКТ-среды.

Слайд 5

НАМИБ имеющая авторитет и опыт в подготовке политических решений и предложений для формирования позиции РФ для международного сотрудничества в ИКТ-пространстве, могла бы выступить инициатором и разработчиком такого предложения, а Координационный центр готов взять на себя экспертную роль в этой работе.

В рамках деятельности данной системы обеспечивается взаимодействие Национальных Регистратур, аккредитованных Регистраторов и Компетентных организаций. Международные Компетентные организации направляют Национальным компетентным организациям аргументированный запрос о прекращении делегирования доменных имен, используемых для зловредных ресурсов. В свою очередь, Национальные компетентные организации после рассмотрения такого Запроса направляют его национальным Регистраторам, которые в свою очередь, вправе прекратить делегирование скомпрометированных доменных имен.

Формы и направления международного сотрудничества, как и стандартизация в сфере информационной безопасности, имеют известную и сложившуюся практику. Наиболее распространенной формы современного межгосударственного сотрудничества является деятельность международных организаций, созданных на основе двухсторонних и многосторонних соглашений.

М.Е. Бурлаков
Заместитель генерального директора АНО «Центр изучения и сетевого мониторинга молодежной среды», доцент кафедры безопасности информационных систем Самарского национального исследовательского университета им. Академика Королева, эксперт по направлению «Судебная компьютерно-техническая экспертиза» палаты экспертов им. Корухова

АКТУАЛЬНЫЕ РИСКИ И УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЕТЕЙ

Вопросы цифровой безопасности несовершеннолетних являются приоритетными в реализации комплексной стратегии безопасности населения.

АНО «Центр изучения и сетевого мониторинга молодежной среды» создана в соответствии с поручением Президента Российской Федерации в целях осуществления мониторинга распространения в информационно-телекоммуникационных сетях, включая информационно-телекоммуникационную сеть «Интернет», информации, склоняющей или иным способом побуждающей детей к совершению действий, представляющих угрозу их жизни и (или) здоровью, а также жизни и (или) здоровью иных лиц.

Основная задача Центра — выявление потенциальных и реальных сетевых угроз посредством мониторинга распространения информации деструктивного содержания, а также изучение интересов и потребностей молодежного контингента пользователей на основе анализа их сетевой активности.

Выявление и анализ распространения деструктивной информации среди несовершеннолетних в открытом сегменте русскоязычного Интернета на предмет их вовлеченности в потребление и распространение противоправного контента осуществляется посредством использования **нейросетевого программного комплекса, разработанного специалистами Центра.**

В настоящее время выявлено перемещение аудитории с деструктивными интересами в мессенджер Телеграм, что обусловлено более слабой модерацией контента. Мессенджер используется для создания тематических телеграм-каналов и вербовки пользователей в личной переписке для совершения противоправных действий.

Дополнительно было выявлено возрастание интереса пользователей к **децентрализованному мессенджеру** (системе общения) **«Matrix»**.

По информации из открытых источников количество ежемесячных активных пользователей удвоилось за 2022 г. и достигло 80 миллионов к 2023 г. Особенностями мессенджера являются отсутствие единого сервера управления и возможность регистрации без привязки телефонного номера.

В настоящее время Центром выявлены **наиболее актуальные сетевые угрозы** по следующим направлениям:

- национализм и религиозный радикализм;
- деструктивные молодежные субкультуры;
- сваттинг и доксинг;
- пропаганда нетрадиционных сексуальных отношений;
- пропаганда наркотических средств;
- стриминговая деятельность.

Национализм и религиозный радикализм

Активность националистических движений возросла после начала проведения СВО.

Аудиторию этих движений составляют как русские националисты, так и этнические националисты на территории республик в составе Российской Федерации. Пропаганда националистических идей и противоправная деятельность националистических организаций поддерживается иностранными государствами. В качестве каналов распространения информации используются менее регулируемые действующим российским законодательством информационные площадки, в особенности мессенджер Телеграм.

Основная задача групп и сообществ националистической направленности — вовлечение молодежи и несовершеннолетних в диверсионную деятельность на территории России.

Религиозный радикализм (как православного, так и мусульманского направления) представляет опасность при смешении с националистическими идеями. В частности, православно-националистический дискурс распространен среди отдельной части патриотов, которые остро реагируют на информационные поводы, в особенности, связанные с проведением СВО.

Потенциальной угрозой является нарастание межнациональных противоречий и возникновение на этом фоне внутренних конфликтов. Даже бытовые происшествия с участием представителей различных национальностей или мигрантов, особенно несовершеннолетних, тиражируются в сетевом пространстве как межэтнические столкновения.

Деструктивные молодежные субкультуры

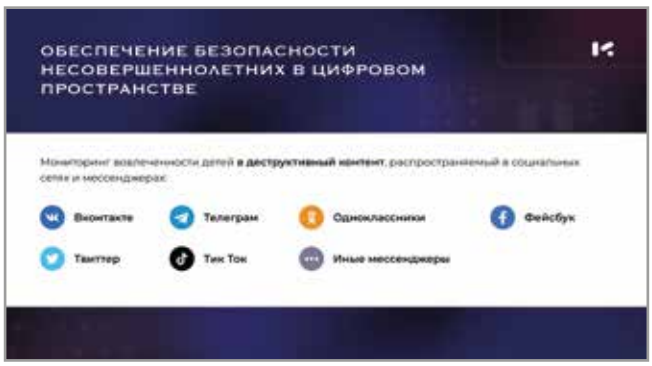
В настоящее время место привычных молодежных субкультур заняли неформальные молодежные объединения, активные преимущественно в интернет-пространстве.

К деструктивным субкультурам относятся те движения, в основе которых лежит система норм, ценностей, интересов и убеждений, негативно влияющих на общественные устои и разрушающие традиционные ценности. Вне зависимости от направления деятельности такие движение создают угрозу безопасности личности и общества. К указанной тематической категории относятся:

- АУЕ;
- околофутбольщики;
- мужское государство;
- антифа;
- анархисты;
- зацеперы;
- руферы.

Риски неформальных молодежных объединений связаны с направлением стратегий социализации молодежи по неадаптивному пути:

- искажение истинных духовных ценностей и трансляция запрещенной



идеологии и опасных моделей поведения;

- формирование агрессивной среды среди субкультур идеологически противоположных по взглядам;
- демонстрация конфликтного потенциала и оправдание злонамеренных действий в медийном пространстве;
- распространение негативного влияния на менее защищенные слои населения.

Сваттинг и доксинг

В 2022 г. после начала проведения СВО зафиксирован резкий скачок случаев ложных сообщений о минировании. Установлено, что системный сваттинг объектов социальной инфраструктуры курируется с территории иностранных государств.

Следствием стало появление *«культуры сваттинга»*. «Лжеминирование» обрело популярность в совокупности с кражей и/или использованием в корыстных целях персональных данных. Выявлены случаи администрирования несовершеннолетними сообществ, в которых продаются курсы или иные методические материалы и инструменты по доксингу (*получение и злонамеренное использование персональной информации о человеке с целью травли, шантажа или получения выгоды*) и сваттингу персон.

Несовершеннолетние, которые не осознают возможную ответственность и при этом имеют желание зарабатывать деньги, могут стать как жертвами террористической деятельности, так и ее соучастниками.

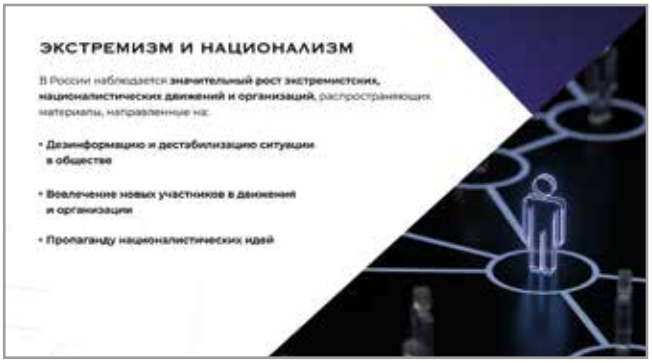
На современном этапе для сваттинга характерно использование современных технических достижений и возможностей Интернета, что дополнительно усложняет ситуацию по пресечению преступной деятельности.

В 2022 году зафиксирован резкий скачок случаев сваттинга **+670%** по отношению к данным за 2021 год.

В настоящее время участились случаи доксинга, связанные со сливами баз персональных данных, «деаноном» публичных личностей, публикацией персональных данных несовершеннолетних их сверстниками.

Пропаганда нетрадиционных сексуальных отношений

Пропаганда нетрадиционных сексуальных отношений в большинстве случаев не ведется напрямую, а носит скрытый характер. Используются привлекательные для несовершеннолетних образы, нормализующие нетрадиционные сексуальные отношения, например рисованные изображения.



Пропаганда наркотических средств

Среди публикаций, распространяемых в сети Интернет, связанных с наркотическими веществами, можно выделить два основных вида социально-опасного контента.

В первом случае — это реклама наркотических веществ и вовлечение несовершеннолетних в противозаконную деятельность в качестве наркокурьеров, «закладчиков». Онлайн-магазины наркотических веществ проводят агрессивный маркетинг сети Интернет, рассылая предложения приобрести незаконный товар. Большая часть контента распространяется в мессенджере Телеграм. Таким же образом через мессенджеры распространятся публикации с вакансиями закладчиков.

Во втором случае угрозу представляет популяризация наркотических веществ как части «молодежной» культуры, создание образа психоактивных веществ как того, что модно, и означает принадлежность к определенной привилегированной группе. Это может привести к возникновению наркотической зависимости, экспериментам с разными видами и большими порциями веществ. Возрастает риск смертности или нанесения вреда здоровью употреблением «кустарных» видов запрещенных веществ.

В мессенджере Телеграм появилось множество каналов и ботов, через которые можно приобрести наркотические средства, что значительно упростило процесс покупки запрещенной продукции.

Стриминговая деятельность

Стрим — это прямой эфир на Интернет-сервисе, потоковое видео, записываемое и транслируемое в режиме реального времени.

Для проведения стримов часто используются такие платформы как «Twitch», «YouTube», «ВКонтакте» (VK Play Live), «Telegram», «Trovo Live». «Twitch» является наиболее популярной и специализированной площадкой, аудитория которой в России в 2022 году составила **5,6 млн** человек.

Стимулом для развития стримингговой деятельности является возможность ее монетизации. Авторы стримингового контента могут размещать рекламу и получать вознаграждение от зрителей в форме денежных переводов (донатов).

Треш-стримы представляют собой трансляцию деструктивного видеоконтента, который может оказывать негативное влияние на психическое здоровье несовершеннолетних. Контент в данной категории содержит сцены жестокости и насилия по отношению к людям или животным. Прямой эфир с одной стороны, обеспечивает доступ к достаточно большой аудитории, с другой стороны, создает дистанцию между возможной жертвой и зрителем, что дает ощущение контроля над происходящим. Анонимность большинства зрителей и ведущих (блогеров) стримов способствует их «безнаказанному» противоправному поведению в сети.

Одним из деструктивных направлений стриминга является употребление запрещенных веществ в прямом эфире, реклама психоактивных веществ в формате баннеров или нативной рекламы.

Онлайн трансляции азартных игр, реклама сайтов онлайн казино, трансляции для сбора денежных средств в поддержку ВСУ также несут в себе сетевые угрозы для молодежной аудитории.

Особую угрозу несет в себе распространение информации, вовлекающей пользователей в экстремистские движения и течения.

Экстремизм — это идеология или система взглядов, направленные на оправдание терроризма, насильственное изменение конституционного строя, возбуждение социальной, расовой, национальной или религиозной вражды, пропаганду исключительности,

превосходства или неполноценности по тем же признакам. **Терроризм — один из самых радикальных методов экстремизма.**

Терроризм — это одна из форм психологической войны. Ведение такого вида войн стало возможным из-за массовой информатизации всех сфер общества. Сеть Интернет активно используется террористами для дезинформации, распространения угроз, создания в обществе ощущений страха и беспомощности. При этом формируется информационно-психологический шок — благоприятная почва для достижения основных целей преступников. В основе такого воздействия лежит специальное структурирование информации, организация ее подачи, манипулирование, дозирование в целях деструктивного воздействия на сознание людей и через него на обстановку в стране в целом.

Сеть Интернет используется для вербовки сторонников, способных на активную роль в поддержке террористических действий. В дополнение к таким средствам привлечения новых членов, как технологии веб-сайтов (звук, видео и т.п.), террористические организации собирают информацию о пользователях, просматривающих их сайты. С теми из них, которые кажутся наиболее заинтересованными в деятельности организации или подходящими для выполнения ее поручений, устанавливают контакт. Вербовщики применяют онлайн-технологии: перемещаются по чатам и форумам в поиске наиболее восприимчивых пользователей, особенно из числа подростков и молодежи.

Процесс вовлечения несовершеннолетних пользователей в деструктивную деятельность осуществляется плавно, часто в «игровой» форме, пользователь получает небольшие задания, которые на первый взгляд не несут значимого ущерба и достаточно безопасны для выполнения.

Киберпространство активно используется для установления контактов и осуществления координации действий при подготовке терактов. С помощью Интернета автономные ячейки террористической сети имеют возможность поддерживать связь между собой и с другими террористическими структурами. Члены террористических группировок регулярно используют социальные сети, интернет-конференции и электронную почту для обсуждения и планирования будущих акций в достаточно безопасном скрытом режиме, применяя современные программные средства для обеспечения анонимности. В сети Интернет доступно для скачивания программное обеспечение для шифрования и анонимизации трафика. Инструкции в виде карт, фотографий и рисунков маскируются с помощью стеганографии, т.е. сообщения скрываются внутри графических файлов.

Специалистами Центра на постоянной основе проводятся работы **по развитию действующих ресурсов и разработке новых систем** в целях повышения эффективности механизмов защиты информационного пространства от распространения деструктивного контента, в том числе террористической и экстремистской направленности.

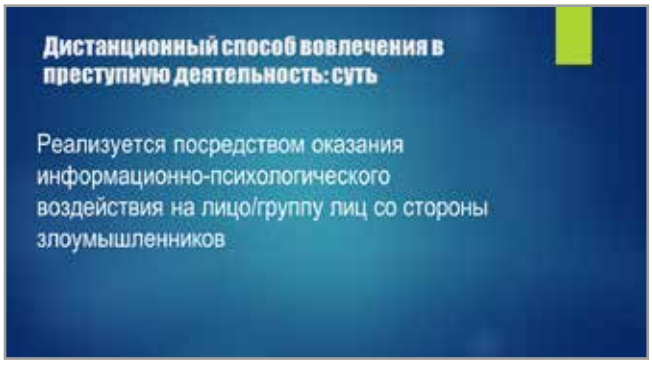
На основании проводимого мониторинга Центром готовятся и направляются в профильные ведомства аналитические срезы по динамике распространения деструктивного контента.

В настоящее время Центром также **активно развивается направление по изучению интересов молодежи** по направлениям позитивного контента посредством мониторинга и анализа их сетевой активности в информационно-телекоммуникационных сетях.

Сведения о тенденциях и направлениях интересов целевой аудитории, полученные в результате проводимых исследований, могут быть использованы при составлении профилактических и воспитательных программ, а также при создании позитивного контента в цифровой среде, который будет интересен и востребован в молодежной аудитории.

А.А. Смирнов
Ведущий научный сотрудник НИЦ 4 ВНИИ МВД России, старший научный сотрудник сектора информационного права и международный информационной безопасности Института государства и права РАН

МЕХАНИЗМЫ ПРОТИВОДЕЙСТВИЯ ВОВЛЕЧЕНИЮ ПОДРОСТКОВ В ПРОТИВОПРАВНЫЕ ДЕЙСТВИЯ С ИСПОЛЬЗОВАНИЕМ СЕТИ ИНТЕРНЕТ



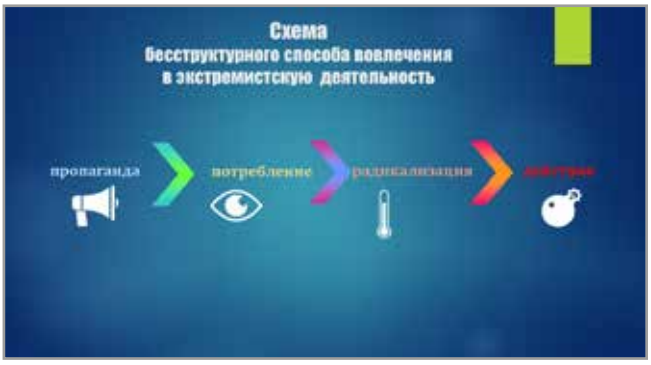


Схема
бесструктурного способа вовлечения
в экстремистскую деятельность
пропаганда
потребление
радикализация
действие


Применение бесструктурного способа
вовлечения в экстремистскую деятельность
индивидуальный уровень
групповой уровень


индивидуальный
уровень

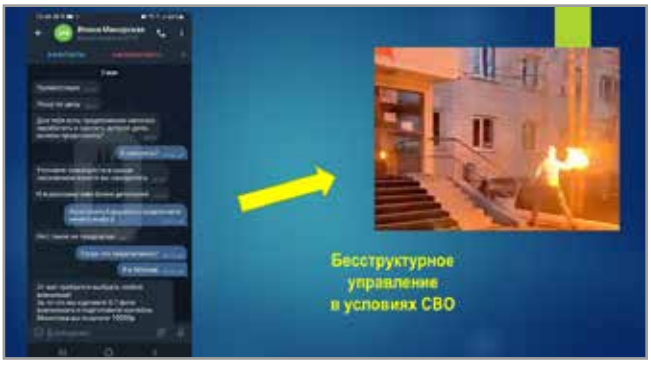

Саморадикализация


Ведение штормовой пропаганды
JIHAD
DOWNLOAD
CLICK
THE DAILY STORMER


Насыщение радикальным контентом
YouTube
gab
4chan
Fascist Forge


CALIPHATE
CYBER
UNITED
Wolves
Individual
GET READY


ISLAMIC
STATE
WOLFS
JUST TERROR
TACTICS


Бесструктурное
управление
в условиях СВО


ФСБ сообщила о поимке
организатора поджогов
военкоматов в
Новосибирске

Схемы вовлечения

1. Вербовка на идеологической основе.

2. Вовлечение на коммерческой основе.

Конвергенция информационных угроз

- Использование технологий социальной инженерии, «обкатанных» в сфере интернет-мошенничества, для дистанционного стимулирования совершения террористических актов и иных экстремистских действий.
- Украинские колл-центры действуют при поддержке спецслужб (СБУ, ГУР МО).

Новая схема вовлечения

1. Хищение средств с помощью технологий социальной инженерии (звонок от «служб безопасности банков» или «сотрудников ФСБ»).
2. Осознание произошедшего потерпевшим.
3. Пострадавшему лицу предлагается отомстить или оказать помощь сотрудникам силовых структур в «задержании злоумышленников».

групповой уровень

Использование «воронок вовлечения»

Комплексная стратегия – залог успеха

Спасибо за внимание!

П.А. Сергоманов
Руководитель академической лаборатории ООО «СберОбразование»

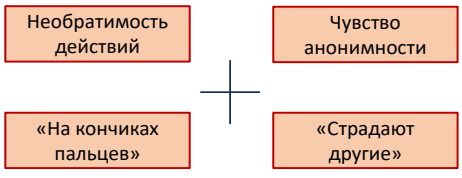
ЦИФРОВАЯ ГРАМОТНОСТЬ И УПРАВЛЕНИЕ РИСКАМ И ЦИФРОВОЙ СРЕДЫ

Круглый стол
«Информационная безопасность детей, подростков и молодежи в условиях цифровых трансформаций: приоритеты, принципы и механизмы обеспечения»

Цифровая грамотность и управление рисками цифровой среды
Павел Сергоманов
20.09.2023

Модели [обучения] грамотности

«Детские» риски цифровой среды: понимание источников



Встреча с риском: грамотность

Риски и управление

Утечка персональных данных
Манипулирование состояниями
Нарушение авторских и других прав
…

КАК: узнать, назвать, управлять

Спасибо за внимание!

А.Ж. Мартиросян
Научный сотрудник Института актуальных международных проблем Дипакадемии МИД России

МЕЖДУНАРОДНАЯ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ГЛАЗАМИ РОССИЙСКОЙ МОЛОДЕЖИ: ОПЫТ ШКОЛЫ МИБ

Хотелось бы на примере деятельности Школы международной информационной безопасности Института актуальных международных проблем (Школа МИБ) остановиться на роли, которую вносит Дипломатическая академия МИД России в тематику международной информационной безопасности.

Школа МИБ создана на базе Института актуальных международных проблем Дипломатической академии МИД России при сотрудничестве с Советом молодых ученых Дипломатической академии МИД России для всестороннего обсуждения и обмена мнениями, позициями и оценками, выработки стратегий комплексного решения проблем международной информационной безопасности.

Основная цель проекта — это создание второго трека дипломатии по МИБ — молодежного трека, где в процессе выработки и принятия решений смогут участвовать представители молодого поколения.

Важно отметить, что Школа МИБ является социально-значимой инициативой:

- благодаря проекту обеспечивается присутствие молодых представителей научного сообщества Российской Федерации в международных инициативах и научных исследованиях;
- это первый проект по созданию коммуникационного пространства среди молодых специалистов в данной области;

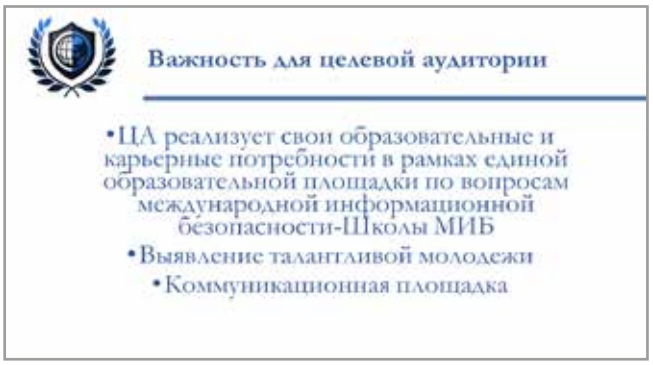
- Школа МИБ единственная научно-аналитическая и образовательная площадка, созданная для формирования механизмов взаимодействия молодых специалистов и уже состоявшихся экспертов в сфере международной информационной безопасности;
- проект также помогает выявлять талантливую молодежь и вовлекать ее в изучение международной информационной безопасности.

Помимо социальной значимости, проект направлен на реализацию Основ государственной политики в области международной информационной безопасности посредством совершенствования механизма участия российских экспертов в международных мероприятиях.

Целевая группа Школы МИБ — обучающиеся, молодые ученые преподаватели и научные сотрудники, эксперты и практики, работники государственных и негосударственных организаций национального и международного уровня, деятельность которых связана с вопросами МИБ.

Что касается реализации проекта, то мы организуем мероприятия различного формата для широкой дискуссии о решении текущих проблем в сфере обеспечения МИБ, проводя научно-практические исследования и мероприятия по наиболее актуальным темам повестки МИБ.

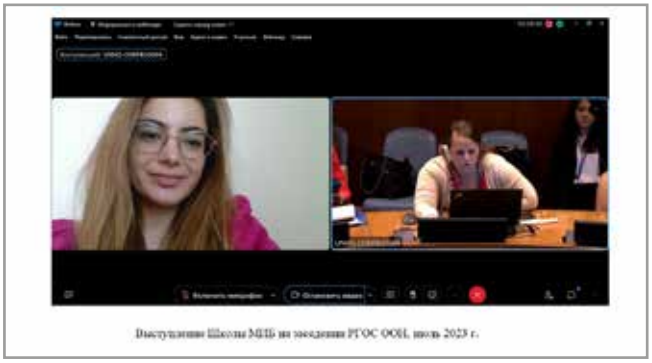
В 2022 г. мы победили в номинации «За вклад в международное сотрудничество в сфере ИТ» в рамках II Всероссийского Молодежного форума по управлению Интернетом. Далее Школа МИБ получила аккредитацию в рамках Рабочей группы ООН открытого состава по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности. Таким образом,



с июля 2022 г. Школа МИБ является участником переговорного процесса в ООН, активно внося свой вклад.

В 2023 г., помимо организации образовательных мероприятий, среди которых, помимо прочего, два круглых стола по ИИ, мы провели в мае «I Международную молодежную конференцию по информационной безопасности». Конференция объединила более 100 молодых ученых. Российская Федерация была представлена участниками из 13 субъектов. В мероприятии также приняли участие студенты и специалисты из Армении, Белоруссии, Казахстана, Узбекистана, Таджикистана и Турции. В октябре будет опубликован сборник по итогам данной конференции.

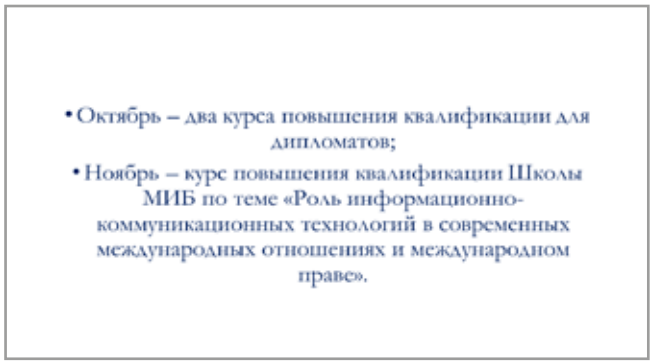
Также совсем скоро усилиями Школы МИБ состоятся два курса повышения квалифика-



Выступление Школы МИБ на заседании РГОС ООН, июль 2023 г.

Москва, февраль 2023

Москва, апрель 2023



ции для дипломатов при привлечении ведущих специалистов области МИБ и открытый авторский курс повышения квалификации по теме «Роль информационно-коммуникационных технологий в современных международных отношениях и международном праве».

Школа МИБ может обеспечить не только квалифицированную подготовку молодых и талантливых кадров, совершенствование механизма участия молодых представителей российского научного и экспертного сообщества в продвижения инициатив Российской Федерации по формированию системы обеспечения МИБ, но и создать новый формат для развития потенциала международного сотрудничества в данной области.

Хотелось бы завершить мыслью, что будущее за молодым поколением, и стоит крайне важная задача — обучать, вдохновлять и направлять его. А Школа МИБ ИАМП ДА МИД России будет и дальше продолжать свою работу в этом направлении.

Уважаемые участники Форума, на этой позитивной ноте хотелось бы завершить свое выступление и поблагодарить НАМИБ за приглашение выступить.

Спасибо за внимание!

Д.Д. Курса
Региональный координатор МСЭ по защите ребенка в онлайновой среде

О ДЕЯТЕЛЬНОСТИ МЕЖДУНАРОДНОГО СОЮЗА ЭЛЕКТРОСВЯЗИ ПО НАПРАВЛЕНИЮ ЗАЩИТЫ ДЕТЕЙ В СЕТИ

1. О деятельности МСЭ по направлению защиты детей в сети. Приветственный слайд.

2. Ни для кого не секрет, что стремительное развитие ИКТ, а также пандемия COVID, увеличили количество детей, использующих преимущества сети, при этом увеличилось количество рисков, с которыми они сталкиваются.

Интернет дает детям возможности социализации, обучения, доступа к информации и самовыражения, именно поэтому так необходимо создать благоприятную и безопасную интернетсреду для них.

Защита ребенка в онлайн среде, на английском child online protection, или сокращенно COP — это глобальная проблема, требующая глобального реагирования, международного сотрудничества и координации на национальном уровне. Если обратиться к международной статистике, если к 8 годам преимущества сети используют 40% детей в мире, то уже к 12 годам Интернет используют 93% детей, что, конечно, беспрецедентно.

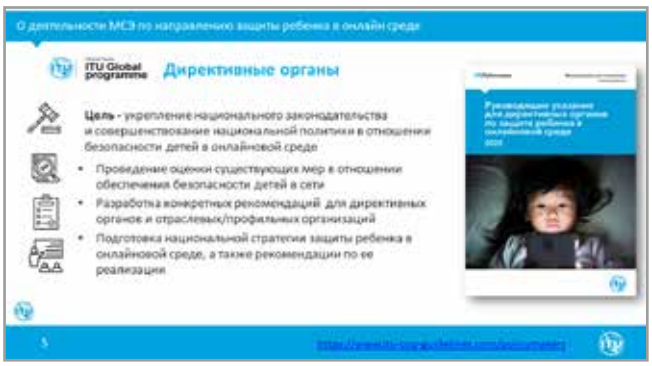
При этом, согласно опросу молодежи, проведенному ЮНИСЕФ в 30 странах, более 70% молодых людей во всем мире сталкиваются с домогательствами и издевательствами в Интернете. Согласно опросу, каждый третий молодой человек говорит, что подвергался издевательствам в Интернете, а каждый пятый говорит, что не ходил в школу из-за киберзапугивания и насилия.

3. Понимая масштабы проблемы Международный союз электросвязи, в 2020 году, через 10 лет после первой публикации, пересмотрел и переработал «Руководящие указания МСЭ по защите ребенка» силами группы экспертов, представляющих широкий круг заинтересованных сторон. Руководящие указания МСЭ по COP включают в себя 4 комплекта: для директивных органов, отрасли, родителей и педагогов, а также для детей.

4. Одновременно с этим МСЭ реализует Глобальную программу по COP, которая включает в себя два основных направления — **наращивание потенциала и поддержка разработки политики по COP.**

Если говорить о первой компоненте, то МСЭ совместно с партнерами в каждой стране:

- переводят Руководящие указания МСЭ на национальные языки;
- разрабатывают и локализуют рекомендации и конкретные указания для всех соответствующих заинтересованных



сторон (родители, педагоги, отрасль ИКТ, государственные организации);
- проводят очные и онлайнтренинги для детей и молодежи, разрабатывают методологии и учебные программы, адаптированные под каждую отдельную страну;
- разрабатывают модульные программы по подготовке инструкторов, так называемые train-the-trainers;
- разрабатывают интерактивные игры и приложения для детей.

Вторая компонента — сотрудничество с государствами в разработке нормативной-правовой базы и проведение исследований текущего состояния законодательства в стране для того, чтобы в дальнейшем это стало полноценной основой для создания **национальной стратегии государства в области СОР.**

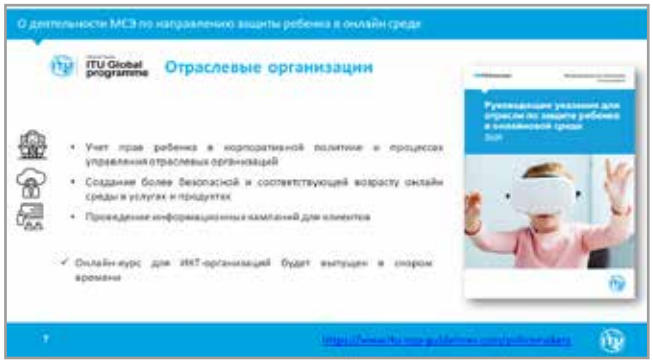
5. Применительно **к директивным органам** Руководящие указания по СОР поддерживают разработку, составление, принятие и реализацию национальной стратегии в области СОР на основании подхода, предусматривающего участие многих заинтересованных сторон.

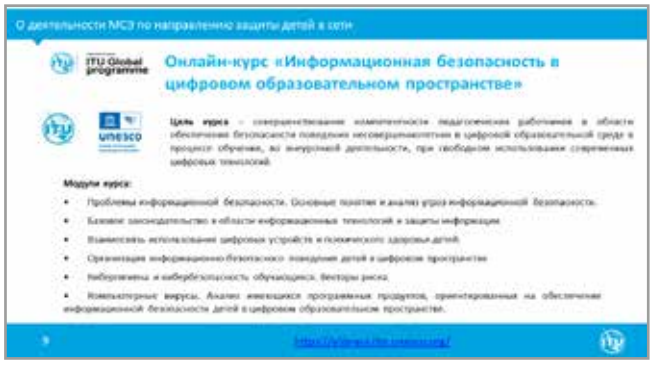
6. Курс для представителей государственных органов.

Курс включает в себя в том числе следующие темы:

- поведение детей в сети и их права;
- влияние ИКТ на детей, риски и вред в сети;
- глобальный и региональный опыт и механизмы защиты детей в онлайн среде;
- международные организации, участвующие в защите детей онлайн среде;
- разработка скоординированной национальной стратегии защиты детей в онлайн среде;
- процесс координации между различными отраслевыми министерствами и национальными заинтересованными сторонами по защите детей в онлайн среде, включая привлечение детей в части разработки политики;
- инструменты для эффективной разработки политики по защите детей в онлайн среде;
- как подготовить национальную политику, адаптированную к возникающим тенденциям в области ИКТ.

7. Применительно **к отрасли** Руководящие указания МСЭ направлены на поддержку отрасли в разработке внутренней политики предприятий в области СОР путем привлечения внимания частного сектора на обеспечение безопасности ребенка в онлайн среде и его благополучия в ходе использования продуктов и услуг ИКТ-организаций.





8. Применительно к **родителям и педагогам** Руководящие указания направлены на оказание поддержки детям путем обучения родителей и педагогов, повышения их осведомленности в вопросах, связанных с безопасностью детей, и содействия развитию цифровых навыков и цифровой грамотности.

В августе прошлого года МСЭ выпустил **тренинги для родителей, а также для академического и неакадемического персонала. Оба курса поделены на базовый и продвинутый уровни.** Базовый курс для родителей повысит осведомленность о том, чем занимаются дети в сети, о рисках и преимуществах сети, а также поможет создать более безопасную онлайн-среду для детей дома, а продвинутый — обучит родителей как помочь детям, столкнувшимся с опасным контентом в Интернете.

Базовый тренинг для преподавателей расскажет о защите и правах детей в Интернете и поможет преподавателям создать более безопасную онлайн-среду для своих учеников в школе. **Продвинутый уровень** — обучит преподавателей распознавать риски, связанные с сексуальной эксплуатацией и насилием над детьми в Интернете, и предотвращать вред от таких действий.

9. Также МСЭ в сотрудничестве с Институтом информационных технологий в образовании ЮНЕСКО выпустил русскоязычный курс, рассчитанный на прохождение 36 часов и включающий в себя следующие модули:

- Основные понятия информационной безопасности и анализ угроз;
- Базовое законодательство в области защиты информации;
- Взаимосвязь использования ИТ и психического здоровья детей;
- Организация безопасного поведения детей в цифровом пространстве;
- Кибергигиена и кибербезопасность обучающихся;
- Компьютерные вирусы.

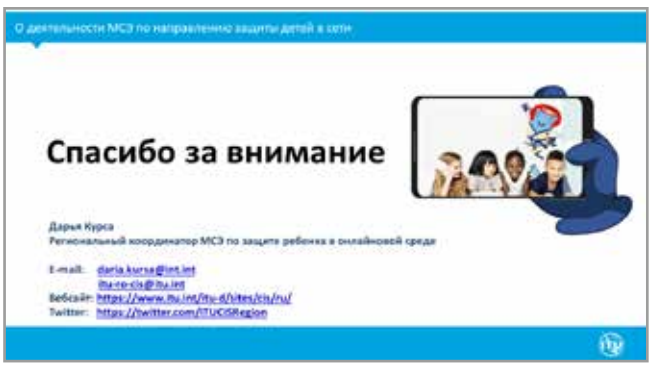
10. Я бы хотела еще особенно подсветить материалы, созданные МСЭ именно для детей, ведь они — ключевая и целевая аудитория.

Материалы подготовлены в доступной для детей интерактивной форме. Будучи адаптированными для различных возрастных групп, данные ресурсы позволяют детям получать знания и укреплять цифровые навыки, помогая им знакомиться со способами управления онлайн рисками

Главный герой ресурсов — вымышленный персонаж Санго — нинзя-смартфон, истории с которым позволяют донести до детей информационный материал понятным им языком.

Сборник рассказов, обучающие игры, рабочие тетради, видеоролики, кампания в соцсетях охватывают основные идеи, которые необходимо донести до детей и которые касаются игр в сети, управления временем перед экраном, неприемлемого контента, конфиденциальности, роли взрослых в формировании положительного примера.

На YouTube опубликованы видеоролики, которые в интересной для детей форме объясняют о соблюдении элементарных правил поведения в сети, которые обеспечат их безопасность и благополучие. Ссылка представлена на слайде.



М.Б. Алборова
Кандидат исторических наук, доцент, ведущий эксперт Центра международной информационной безопасности и научно-технологической политики Института международных исследований МГИМО МИД России

ВЛИЯНИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ НА РАЗВИТИЕ ПОДРАСТАЮЩЕГО ПОКОЛЕНИЯ

Постиндустриальная эпоха активно набирает обороты и становится драйвером для внедрения новых технологий, оказывающих на общество как позитивное, так и негативное влияние. Понимание значения научно-технологического прогресса позволяет оценить скорость, разнонаправленность и масштабность изменений, которые преобразовывают всю окружающую среду и имеют поистине беспрецедентный характер.

На современном этапе все чаще появляются опасения возникновения технологической сингулярности, как определенного этапа эволюции, при котором широкое применение искусственного интеллекта вырастет экспоненциально и даст возможность сформировать основы для появления разума с более высоким уровнем анализа, обработки данных и выработки решения, то есть сложатся основы для нового мышления более высокого уровня, чем у человека. Отсюда и осознание многомерных изменений, которые проявятся в жизни общества и человека.

В последнее время, в рамках западного экспертного сообщества появилось мнение о том, что в результате «интеллектуального взрыва» способности разума человека намного отстанут от возможностей искусственного интеллекта. Это не априорная позиция: прогноз Рэя Курцвейла о том, что искусственный

интеллект усилит, а не заменит нас, не является единственно правильным[1]. Тем не менее, комплекс новых технологий действительно кардинально меняет среду, в которой живет современный человек, и оказывает фундаментальное влияние на цивилизационные основы. В первую очередь эти процессы коснутся нового поколения «альфа», поколения гаджетов и инновационных технологий.

Широкое применение человеком всевозможных инноваций позволило ему снять с себя многие задачи по чтению, вычислению и аналитике. С одной стороны, это дает возможность перераспределить силы и уделить внимание творческим процессам, с другой стороны эксперты все чаще бьют в набат, акцентируя внимание на том, что целое поколение все больше «упрощается». Технологии открывают широкие перспективы для быстрой обработки информации, но здесь и кроется своеобразный «ящик Пандоры»: если все можно с помощью гаджета, то зачем предпринимать усилия? В итоге процент детей, которые не могут выполнить самые простые учебные действия в математике, физике и других науках, растет.

Эксперты фиксируют ежегодное снижение способности к прочтению больших объемов текста, сокращению возможностей долговременной памяти, что, в свою очередь, приводит к невозможности анализа не только научных материалов, но и жизненных событий. Трагичность данного фактора заключается в том, что созидательные и творческие процессы, без которых невозможно развивать общество, базируются именно на долговременной памяти, которая позволяет мышлению человека синтезировать большие объемы данных, анализировать их и на

1 Kurzweil Ray. The Singularity Is Near: When Humans Transcend Biology. 2005.

этой базе создавать инновационный продукт или услугу.

Глубокие исследования, проведенные как в России, так и за рубежом убедительно свидетельствуют о значительных проблемах, которые проявляются у детей XXI века — это и снижение мотивации к обучению, и резкое ухудшение навыков, чтения, письма, вычисления и т.д. Длительное и увлеченное применение гаджетов приводит к значительному снижению не только интеллектуальных способностей, но физического здоровья в целом.

Появился и осознается обществом новый риск — риск сокращения мыслительных способностей человека. Именно в этой фазе и формируется озабоченность вопросом дисбаланса между каскадным ростом многочисленных возможностей технологий и сокращением численности населения, способного управлять этими технологическими процессами[2]. При этом сокращается как физический, так и интеллектуальный потенциал человечества.

Неутешительные прогнозы дает и диагностика заболеваний СДВГ, аутизма, эксперты все чаще наблюдают расширение проблем с нарушением координации у детей и подростков, в целом с задержкой развития. Учителя и воспитатели обеспокоены ростом численности детей, у которых фиксируются трудности с обучением, очевидное расстройство сенсорной обработки информации. Растет число нервно-психологической симптоматики: беспокойство, депрессия и расстройство сна,

2 Ларина Е.С. Человеческое мышление и искусственный интеллект. Российский аргумент в международном сотрудничестве / Е.С. Ларина // Международная информационная безопасность: Новая геополитическая реальность / Под ред. Е.С. Зиновьевой, М.Б. Алборовой. — М.: Общество с ограниченной ответственностью Издательство "Аспект Пресс", 2021. — С. 79–85.

которое все чаще связывается с чрезмерным использованием технологий.

На этом фоне широкая разработка роботов-гуманоидов, способных к эмпатии, внешне похожих на человека, умеющих поддерживать общение и т.п. актуализирует осознание потребности безопасности внедряемых технологий и их антропоцентричности. Все чаще возникает вопрос замещения человека в труде, творчестве, социальной сфере.

Растет многомерность изменений в жизни человечества, снижается фактор ценности человеческой жизни, все больше проявляется эмоциональная скудость, увеличивается озлобленность на фоне безграничного желания потребления и вседозволенности. В этих условиях необходимо поднимать вопрос о комплексной работе по развитию и сохранению человека и человечности в целом в условиях тех цивилизационных изменений, которые мы наблюдаем.

Результаты анализа рисков, проявляющихся в мире в условиях развития современных технологий, требуют и понимания места России в этом технологическом вызове. Важно отметить, что цифровые разрывы между странами приводят не только к уязвимости, но и рискам обеспечения безопасности самого суверенитета страны, поэтому соответствие высокому технологическому уровню необходимо. Преодоление цифровых разрывов без наличия развитого человеческого капитала, имеющего устойчивую поколенную историю преемственности, невозможно.

Уже сегодня проявляется все многообразие последствий масштабного и ускоренного развития технологий, при котором не всегда можно просчитать критические риски. Требуется совершенно новый подход к социальной политике, на основе которого мы сможем попытаться сгладить негативные эффекты ши-

роко внедряемых в жизнь целого поколения технологий. Именно качественно новая социальная политика, основанная на понимании стратегических перспектив, дает возможность построения общества, которое способно развивать технологии, при этом не терять человечности и сохранять фундаментальные научные знания, без которых прогресс невозможен.

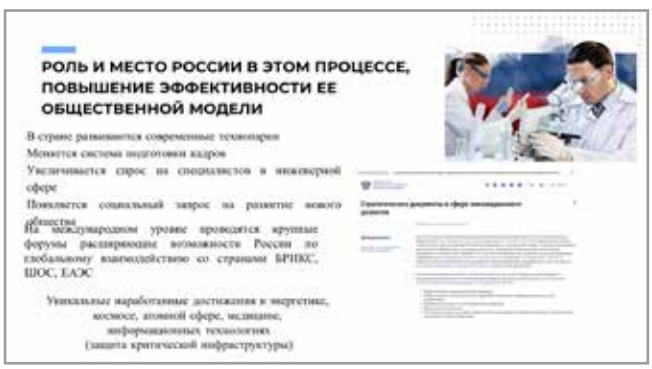
Несомненно, что применение возможностей цифровой экономики, основанной на современных инновациях: это и реальность, и основа стратегического будущего. Инновации дают мощный импульс для устойчивого развития всего общества, вместе с тем, несбалансированность приводит к социальным кризисам, которые каскадным образом меняют всю реальность человеческой жизни[3].

Клаус Шваб, основатель Всемирного экономического форума в своих работах отмечал, что на фоне развития четвертой промышленной революции важно говорить о возрастающей роли общечеловеческих ценностей при условии развития антропоцентрического подхода. Технологии должны быть ориентированы на развитие человека и человечества, именно поэтому необходимо ставить вопрос о повышении ответственности в развитии технологий.

Гонка за высокий уровень конкурентоспособности стала новым идеалом XXI века, отодвинув во многом социогуманитарные аспекты развития человечества[4]. Все чаще

3 Крутских А.В., Бирюков А.В. Новая геополитика международных научно-технологических отношений // Международные процессы. 2017. № 2. С. 6–26.

4 Бирюков А.В., Алборова М.Б. Социально-гуманитарное измерение международной информационной безопасности. М.: Аспект Пресс, 2019. — С. 34.



поднимается вопрос оптимизации, повышения эффективности, политики ресурсосбережения, при этом вопросы уникальности человека, его таланты, духовность во многом игнорируются. Идет очевидная ломка общечеловеческих ценностей, традиций, межпоколенной преемственности. Широко разрекламированная психология потребления и гедонизма, помноженная на технологические возможности, поставила под вопрос ценности самой человеческой жизни, что в свою очередь привело к сокращению рождаемости во многих технологически развитых странах мира.

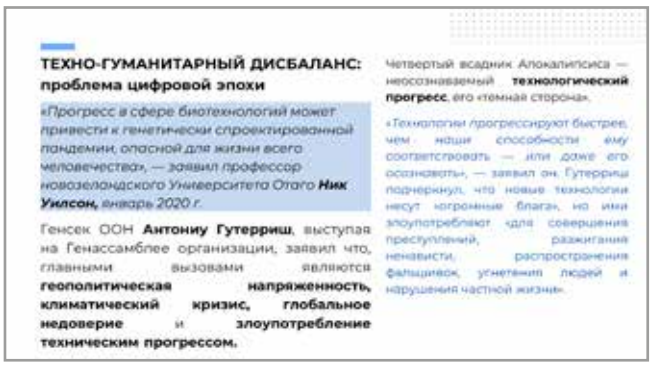
Несомненно, что технологическая сила государств в условиях конкурентного развития технологий во многом определяется наличием у него полноценной комплексной инфраструктуры, которая позволяла бы внедрять инновационные технологии в процессы управления и развития общества при этом обеспечивая безопасность применения этих технологий. Но решение этого вопроса напрямую приведет и к необходимости пересмотра политики управления кадровым потенциалом страны, без которого невозможно обеспечить устойчивое будущее.

Еще в 2017 г. Президент России В.В. Путин подчеркивал значение развития технологий в целом, и усиления работы по внедрению технологий искусственного интеллекта в частности. В своем выступлении он отметил, что страна, добившаяся лидерства в данной сфере «будет властелином мира»[5]. Хорошая технологическая база, заложенная в нашей стране еще на рубеже XIX–XX вв., позволяет сформировать фундамент для реализации стратегического инновационного развития России[6]. Важно помнить, что технологический прогресс противоречив, инновации становятся новой средой жизни, эта среда многогранна, понимание рисков требует от нас конкретных шагов по сохранению человеческого капитала, развитию демографической политики, качественному повышению уровня образования и воспитания молодого поколения.

Таким образом, анализируя влияние информационных технологий на развитие подрастающего поколения необходимо отметить, что современные вызовы и риски технологического мира в первую очередь меняют будущее всего человечества. Эти риски отражаются на самом юном поколении, меняя его и подрывая основы устойчивого развития. Необходимо понимание этих рисков, своевременное реагирование на них и проведение превентивной

5 Открытый урок «Россия, устремленная в будущее» // Сайт Администрации Президента России, 01.09.2017 URL: http://kremlin/ ru/events/president/news/55493 (дата обращения: 08.05.2023).

6 Научно-технологический прогресс и современные международные отношения: В двух томах. Том 1: Учебник для вузов / Под общ. ред. А.В. Бирюкова; отв. ред. М.Б. Алборова, А.В. Крутских. — М.: Издательство «Аспект Пресс», 2023. — С. 167.



социальной политики по сохранению высокого уровня образования и нравственного капитала человечества.

Современные технологии в биоинженерии, когнитивных технологиях и иных инновациях коснулись самой сути человека, основ его развития, отразились на трансформации общества и государства. Понимание этих рисков и своевременная работа с ними позволят обеспечить стабильное развития общества.

Список литературы:

1. Бирюков А.В., Алборова М.Б. Социально-гуманитарное измерение международной информационной безопасности. М.: Аспект Пресс, 2019. — С. 34.
2. Крутских А., Бирюков А. Новая геополитика международных научно-технологических отношений // Международные процессы. 2017. № 2. — С. 6–26.
3. Ларина, Е.С. Человеческое мышление и искусственный интеллект. Российский аргумент в международном сотрудничестве / Е.С. Ларина // Международная информационная безопасность: Новая геополитическая реальность / Под ред. Е.С. Зиновьевой, М.Б. Алборовой. — Москва : Общество с ограниченной ответственностью Издательство «Аспект Пресс», 2021. — С. 79–85.
4. Научно-технологический прогресс и современные международные отношения: В двух томах. Том 1: Учебник для вузов / Под общ. ред. А.В. Бирюкова; отв. ред. М.Б. Алборова, А.В. Крутских. — М.: Издательство «Аспект Пресс», 2023.— С. 167.
5. Открытый урок «Россия, устремленная в будущее» // Сайт Администрации Президента России, 01.09.2017 URL: http://kremlin/ ru/events/president/news/55493 (дата обращения: 08.05.2023).
6. Социогуманитарные аспекты цифровых трансформаций и искусственного интеллекта/ Под ред. В.Е. Лепского, А.Н. Райкова. — М.: Когитто-Центр, 2022. — С. 5.

КРУГЛЫЙ СТОЛ № 6
РАЗВИТИЕ РЕГИОНАЛЬНОГО СОТРУДНИЧЕСТВА В СИСТЕМЕ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Ведущий:
Смирнов А.И., доктор исторических наук, профессор МГИМО МИД России, помощник президента Национальной Ассоциации международной информационной безопасности

А.И. Смирнов
Доктор исторических наук, профессор МГИМО МИД России, помощник президента Национальной Ассоциации международной информационной безопасности

ТЕНДЕНЦИИ ИЗМЕНЕНИЯ ПОДХОДОВ РЕГИОНАЛЬНЫХ ОРГАНИЗАЦИЙ К ПРОБЛЕМЕ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Уважаемые коллеги!

Наш круглый стол завершает работу Форума, в ходе которого состоялось заинтересованное обсуждение практически всех проблем и угроз использования ИКТ для МИБ. Очень приятно, что в дискуссии принимают участие представители стран-участников региональных организаций: Союзного государства, БРИКС, ШОС, Африканского союза, СВМДА и др.

В Основах государственной политики России в области МИБ (утверждены Указом Президента России от 12.04.2021 г. № 213) отмечено, что базовыми направлениями их реализации по противодействию угрозе использования ИКТ в целях подрыва (ущемления) суверенитета, нарушения территориальной целостности государств, осуществления в глобальном информационном пространстве иных действий, препятствующих поддержанию международного мира, безопасности и стабильности, являются, в том числе:

- **содействие развитию региональных систем обеспечения МИБ** и формированию соответствующей глобальной системы на основе общепризнанных принципов и норм международного права с учетом специфики ИКТ, а также на основе принципов и норм международного права, разработанных в целях предотвращения (урегулирования) межгосударственных конфликтов в глобальном информационном пространстве;
- выработка на глобальном, **региональном,** многостороннем и двустороннем уровнях мер укрепления доверия в области противодействия использованию ИКТ для осуществления в глобальном информационном пространстве действий, представляющих угрозу международному миру, безопасности и стабильности.

На региональных саммитах проблематика МИБ стала одной из ключевых.

Так, в **Нью-Делийской Декларации Совета глав государств-членов ШОС** от 4 июля 2023 года было отмечено:

- Государства-члены подчеркивают ключевую роль ООН в сфере противодействия угрозам в информационном пространстве, создания безопасного, справедливого и открытого информационного пространства, построенного на принципах уважения суверенитета и невмешательства во внутренние дела стран. Они считают важным обеспечивать равные для всех стран права на регулирование сети Интернет и суверенное право государств на управление ею в своем национальном сегменте.
- Государства-члены выступают категорически против милитаризации сферы ИКТ. Они поддерживают выработку универсальных правил, принципов и норм ответственного поведения государств в этой области, в т.ч. приветствуют запуск разработки под эгидой ООН всеобъемлющей международной конвенции о противодействии использованию ИКТ в преступных целях. Государства-члены продолжат сотруд-

ничать в рамках профильных переговорных механизмов в ООН и на других площадках.

Следует отметить, что к саммиту подключались представители ООН, СНГ, ОДКБ, ЕАЭС, СВМДА.

В Декларации второго саммита Россия—Африка (Санкт-Петербург, 28 июля 2023 г.) подчеркнуто:

«40. Объединять усилия на площадке ООН по формированию системы обеспечения МИБ в соответствии с принципами Устава ООН. Отстаивать центральную роль государств в решении вопросов безопасности ИКТ. Вести дело к выработке универсальных юридически обязывающих норм в этой сфере. Добиваться принятия в срок всеобъемлющей конвенции ООН о противодействии использованию ИКТ в преступных целях. Совместно выступать в пользу создания равноправной и прозрачной межгосударственной системы управления Интернетом при сохранении суверенного права государств регулировать национальные сегменты глобальной сети. Способствовать усилиям по преодолению цифрового разрыва.»

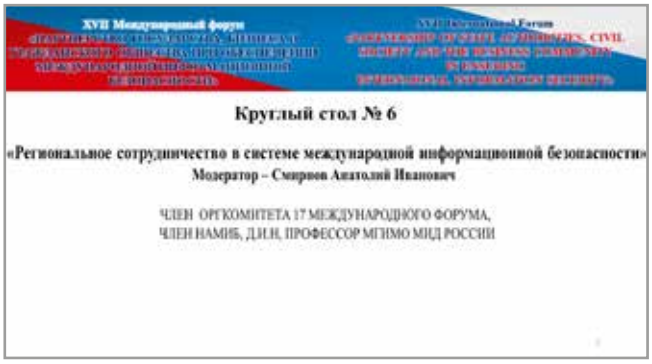
Кроме того, **на втором саммите была принята отдельная Декларация о сотрудничестве в области обеспечения МИБ.** В ней сказано:

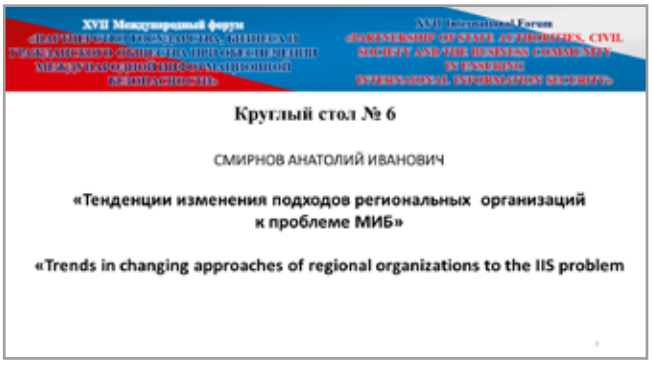
«1. Подтверждаем общность подходов РФ и африканских государств к обеспечению безопасности в сфере использования ИКТ. Заявляем, что использование ИКТ, сотрудничество в области обеспечения МИБ должны осуществляться в соответствии с принципами обеспечения прав и свобод человека и общепризнанными принципами и нормами международного права, закрепленными прежде всего в Уставе ООН.

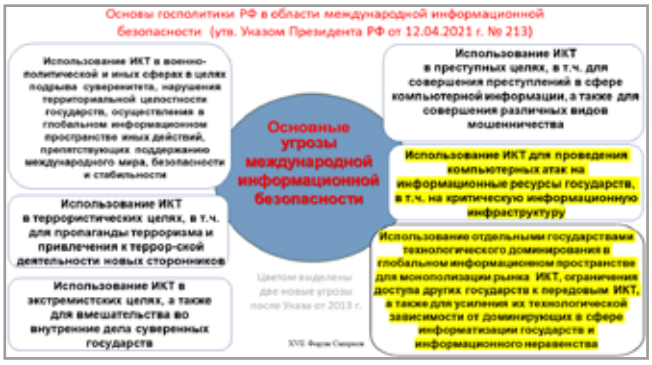
2. Выступаем за укрепление сотрудничества государств в интересах предотвращения и мирного урегулирования конфликтов, а также снижения рисков ошибочного восприятия, которые могут возникать в результате использования ИКТ. Подтверждаем ключевую роль ООН в дальнейшей выработке правил, норм и принципов ответственного поведения государств в сфере использования ИКТ, в т.ч. числе посредством формирования международных юридически обязывающих инструментов и их реализации государствами-членами ООН в согласованных рамках.

Признаем необходимость выработки под эгидой ООН эффективных и универсальных юридически обязывающих инструментов в сфере безопасности использования ИКТ и недопущения компьютерных атак на гражданскую инфраструктуру.

Призываем активизировать мероприятия по наращиванию потенциала в этой сфере и углублять взаимодействие между компетентными ведомствами и уполномоченными







организациями, в т.ч. в области реагирования на компьютерные инциденты.

3. Выступаем за международное сотрудничество в области обеспечения информационной безопасности путем активизации усилий на двустороннем и многостороннем уровнях. Подтверждаем готовность продолжить совместную работу и координацию усилий России и африканских государств под эгидой ООН.

4. Подчеркиваем важность наращивания потенциала для противодействия угрозам в информационном пространстве, а также мер укрепления международной безопасности, доверия, сотрудничества между государствами. Такие меры должны быть направлены на использование ИКТ в мирных целях, укрепление цифрового суверенитета развивающихся государств, учитывать их нужды и потребности, способствовать обмену … практиками, а также содействовать подготовке специалистов.

5. Подтверждаем приверженность развитию многостороннего сотрудничества по вопросам противодействия использованию ИКТ в террористических, экстремистских и других преступных целях. Призываем к завершению разработки под эгидой ООН всеобъемлющей международной конвенции о противодействии использованию ИКТ в преступных целях.

6. Признаем необходимость усиления координации деятельности России и африканских государств в организациях системы ООН в области электросвязи и почтовых услуг, обеспечения их работы в рамках уставных документов в целях развития ИКТ, а также недопущения различных форм дискриминации в отношении государств-участников этих организаций.

7. Исходим из важности реализации Тунисской программы для информационного общества, принятой в 2005 г. на Всемирной встрече на высшем уровне по вопросам информационного общества.

Поддерживаем создание сбалансированной международной системы управления Интернетом под эгидой ООН в целях исключения влияния на нее каких-либо односторонних политических ограничений или коммерческих интересов и обеспечения безопасности, целостности, стабильности критической инфраструктуры Всемирной сети.»

Особо просил бы обратить внимание на следующий пункт:

«8. В целях дальнейшего углубления сотрудничества России и африканских государств **договорились о проведении региональной встречи Россия—Африка по безопасности в сфере использования ИКТ**, которая заложит основы для практического взаимодействия органов государственной власти наших стран.»

Апофеозом **регионального взаимодействия в сфере МИБ можно считать Йохан-**


XVII Международный форум

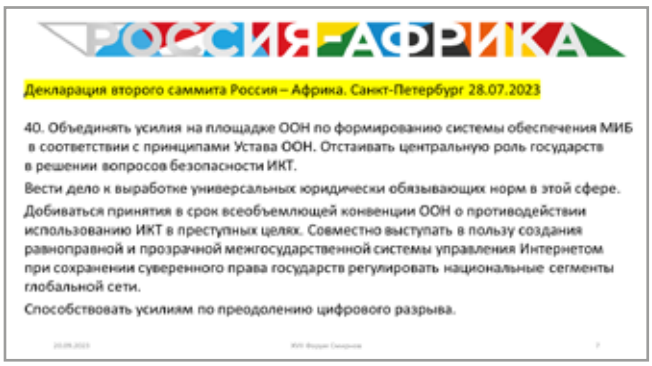
Из Основ государственной политики РФ в области МИБ:

- ✓ Основными направлениями реализации госполитики в области МИБ по противодействию угрозе использования ИКТ в целях подрыва (ущемления) суверенитета, нарушения территориальной целостности государств, осуществления в глобальном информационном пространстве иных действий, препятствующих поддержанию международного мира, безопасности и стабильности, являются в т.ч.:
- ✓ содействие развитию региональных систем обеспечения МИБ и формированию соответствующей глобальной системы на основе общепризнанных принципов и норм международного права с учетом специфики ИКТ, а также на основе новых принципов и норм международного права, разработанных в целях предотвращения (урегулирования) межгосударственных конфликтов в глобальном информационном пространстве;
- ✓ выработка на глобальном, региональном, многостороннем и двустороннем уровнях мер укрепления доверия в области противодействия использованию ИКТ для осуществления в глобальном информационном пространстве действий, представляющих угрозу международному миру, безопасности и стабильности.


XVII Международный форум

НЬЮ-ДЕЛИЙСКАЯ ДЕКЛАРАЦИЯ СОВЕТА ГЛАВ ГОСУДАРСТВ-ЧЛЕНОВ ШОС (4.7.2023)
NEW DELHI DECLARATION OF THE COUNCIL OF HEADS OF STATE OF SHANGHAI COOPERATION ORGANIZATION

- ✓ Государства-члены подчеркивают ключевую роль ООН в сфере противодействия угрозам в информационном пространстве, создания безопасного, справедливого и открытого информационного пространства, построенного на принципах уважения суверенитета и невмешательства во внутренние дела стран. Они считают важным обеспечивать равные для всех стран права на регулирование сети Интернет и суверенное право государств на управление ею в своем национальном сегменте.
- ✓ Государства-члены выступают категорически против милитаризации сферы ИКТ. Они поддерживают выработку универсальных правил, принципов и норм ответственного поведения государств в этой области, в т.ч. приветствуют запуск разработки под эгидой ООН всеобъемлющей международной конвенции о противодействии использованию ИКТ в преступных целях. Государства-члены продолжат сотрудничать в рамках профильных переговорных механизмов в ООН и на других площадках, к заседанию (подключались из ООН, СНГ, ОДКБ, ЕАЭС, СВМДА).


РОССИЯ-АФРИКА

Декларация второго саммита Россия – Африка. Санкт-Петербург 28.07.2023

40. Объединять усилия на площадке ООН по формированию системы обеспечения МИБ в соответствии с принципами Устава ООН. Отстаивать центральную роль государств в решении вопросов безопасности ИКТ.

Вести дело к выработке универсальных юридически обязывающих норм в этой сфере.

Добиваться принятия в срок всеобъемлющей конвенции ООН о противодействии использованию ИКТ в преступных целях. Совместно выступать в пользу создания равноправной и прозрачной межгосударственной системы управления Интернетом при сохранении суверенного права государств регулировать национальные сегменты глобальной сети.

Способствовать усилиям по преодолению цифрового разрыва.


РОССИЯ-АФРИКА

Декларация второго саммита РФ – Африка о сотрудничестве в области обеспечения МИБ
Declaration of the second Russia–Africa Summit on cooperation in the field of IIS 28.7. 2023.

несбургскую декларацию-II. БРИКС и Африка: партнерство в интересах совместного ускоренного роста, устойчивого развития и инклюзивной многосторонности (ЮАР, 23 августа 2023 г.). В ней, в частности, подчеркивается:

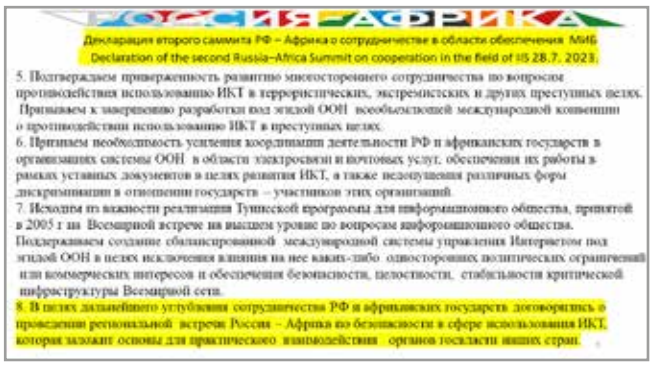
23. Подчеркивая огромный потенциал ИКТ для роста и развития, мы признаем связанные с ними существующие и новые возможности для преступной деятельности и угроз… Мы приветствуем работу, ведущуюся в Специальном комитете по разработке всеобъемлющей международной конвенции о противодействии использованию ИКТ в преступных целях, и подтверждаем свою приверженность сотрудничеству… по резолюции 75/282 ГА ООН.

24. …Мы поддерживаем центральную роль ООН в развитии конструктивного диалога по теме обеспечения безопасности ИКТ, в т.ч. в рамках Рабочей группы ООН открытого состава по вопросам безопасности в сфере использования ИКТ и самих ИКТ в 2021–2025 г, а также разработке общепризнанных нормативно-правовых рамок в этой области. Мы призываем к всеобъемлющему, сбалансированному и объективному подходу к разработке и обеспечению безопасности продуктов и систем ИКТ… Мы также признаем необходимость развития сотрудничества в рамках БРИКС посредством осуществления «дорожной карты» …БРИКС в обеспечении безопасности в сфере использования ИКТ и в рамках Рабочей группы БРИКС по вопросам безопасности в сфере использования ИКТ.

На саммите БРИКС была поддержана инициатива лидера КНР Си Цзиньпиня о создании рабочей группы по управлению искусственным интеллектом. Надеюсь, что проблематика ИИ будет рассмотрена и в ходе дискуссии на нашем круглом столе (как и на уже прошедших столах).

В Концепции внешней политики России (утверждена Президентом России В.В. Путиным 31 марта 2023 г.) отмечено, что человечество переживает эпоху революционных перемен, продолжается формирование более справедливого, многополярного мира. США и их сателлиты рассматривают укрепление России в качестве одной из угроз своей гегемонии. В силу этого в Концепции отмечено, что Россия намерена уделять приоритетное внимание сфере МИБ:

1) укреплению и совершенствованию международно-правового режима предотвращения и разрешения межгосударственных конфликтов и регулирования деятельности в глобальном информационном пространстве;
2) формированию и совершенствованию международно-правовых основ противодействия использованию ИКТ в преступных целях;

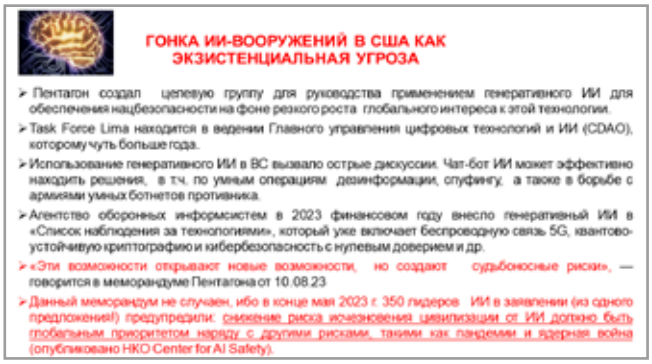

Декларация второго саммита РФ – Африка о сотрудничестве в области обеспечения МИБ
Declaration of the second Russia–Africa Summit on cooperation in the field of IIS 28.7. 2023.

5. Подтверждаем приверженность развитию многостороннего сотрудничества по вопросам противодействия использованию ИКТ в террористических, экстремистских и других преступных целях. Признаем к завершению разработки под эгидой ООН всеобъемлющей международной конвенции о противодействии использованию ИКТ в преступных целях.
6. Признаем необходимость усиления координации деятельности РФ и африканских государств в организациях системы ООН в области электросвязи и почтовых услуг, обеспечения их работы в рамках уставных документов в целях развития ИКТ, а также недопущения различных форм дискриминации в отношении государств – участников этих организаций.
7. Исходим из важности реализации Тунисской программы для информационного общества, принятой в 2005 г на Всемирной встрече на высшем уровне по вопросам информационного общества. Поддерживаем создание сбалансированной международной системы управления Интернетом под эгидой ООН в целях исключения влияния на нее каких-либо односторонних политических ограничений или коммерческих интересов и обеспечения безопасности, целостности, стабильности критической инфраструктуры Всемирной сети.
8. В целях дальнейшего углубления сотрудничества РФ и африканских государств договорились о проведении региональной встречи Россия – Африка по безопасности в сфере использования ИКТ, которая заложит основы для практического взаимодействия органов госвласти наших стран.


XVII Международный форум
Йоханнесбургская декларация-II. БРИКС и Африка: партнерство в интересах совместного ускоренного роста, устойчивого развития и инклюзивной многосторонности, ЮАР, 23.8.2023.
23. Подчеркивая огромный потенциал ИКТ для роста и развития, мы признаем связанные с ними существующие и новые возможности для преступной деятельности и угроз… Мы приветствуем работу, ведущуюся в Специальном комитете по разработке всеобъемлющей международной конвенции о противодействии использованию ИКТ в преступных целях, и подтверждаем свою приверженность сотрудничеству в реализации мандата по резолюции 75/282 ГА ООН.
24…Мы поддерживаем центральную роль ООН в развитии конструктивного диалога по теме обеспечения безопасности ИКТ, в т.ч. в рамках Рабочей группы ООН открытого состава по вопросам безопасности в сфере использования ИКТ и самих ИКТ в 2021-2025 г, а также разработке общепризнанных нормативно-правовых рамок в этой области. Мы призываем к всеобъемлющему, сбалансированному и объективному подходу к разработке и обеспечению безопасности продуктов и систем ИКТ… Мы также признаем необходимость развития сотрудничества в рамках БРИКС посредством осуществления «дорожной карты»…БРИКС в обеспечении безопасности в сфере использования ИКТ и в рамках Рабочей группы БРИКС по вопросам безопасности в сфере использования ИКТ.


XVII Международный форум
председатель КНР Си Цзиньпин на XV саммите БРИКС: РИСКИ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА (ИИ)

ИИ-область, которая может принести риски. Странам БРИКС необходимо сформировать структуру управления ИИ заявил Си Цзиньпин на саммите БРИКС.
По его словам, страны БРИКС уже договорились начать работу по исследованию ИИ.
"(Необходимо) продолжить расширять сотрудничество в области искусственного интеллекта, усилить обмен информацией и техническое сотрудничество, совместно работать по предотвращению рисков, на основе широкого консенсуса сформировать структуру управления искусственным интеллектом и стандартов", - сказал Си Цзиньпин.
Китайский лидер также отметил необходимость постоянно повышать безопасность и надежность ИИ.


ГОНКА ИИ-ВООРУЖЕНИЙ В США КАК ЭКЗИСТЕНЦИАЛЬНАЯ УГРОЗА

- Пентагон создал целевую группу для руководства применением генеративного ИИ для обеспечения нацбезопасности на фоне резкого роста глобального интереса к этой технологии.
- Task Force Lima находится в ведении Главного управления цифровых технологий и ИИ (CDAO), которому чуть больше года.
- Использование генеративного ИИ в ВС вызвало острые дискуссии. Чат-бот ИИ может эффективно находить решения, в т.ч. по умным операциям дезинформации, спуфингу, а также в борьбе с армиями умных ботнетов противника.
- Агентство оборонных информсистем в 2023 финансовом году внесло генеративный ИИ в «Список наблюдения за технологиями», который уже включает беспроводную связь 5G, квантово-устойчивую криптографию и кибербезопасность с нулевым доверием и др.
- «Эти возможности открывают новые возможности, но создают судьбоносные риски», — говорится в меморандуме Пентагона от 10.08.23
- Данный меморандум не случаен, ибо в конце мая 2023 г. 350 лидеров ИИ в заявлении (из одного предложения!) предупредили: снижение риска исчезновения цивилизации от ИИ должно быть глобальным приоритетом наряду с другими рисками, такими как пандемии и ядерная война (опубликовано HKO Center for AI Safety).

3) обеспечению безопасного и стабильного функционирования и развития информационно-телекоммуникационной сети «Интернет» на основе равноправного участия государств в управлении данной сетью и недопущению установления иностранного контроля над ее национальными сегментами;
4) принятию политико-дипломатических и иных мер, направленных на противодействие политике недружественных государств по милитаризации глобального информационного пространства, по использованию ИКТ для вмешательства во внутренние дела государств и в военных целях, а также по ограничению доступа других государств к передовым ИКТ и усилению их технологической зависимости.

Важно отметить, что все четыре пункта имеют и региональное измерение!

Спасибо за внимание!

А.Н. Курбацкий
Профессор, зав. кафедрой Белорусского государственного университета, профессор МГИМО МИД России

К.Е. Коктыш
Доктор политических наук, профессор Кафедры политической теории, старший научный сотрудник Центра евроазиатских исследований, старший научный сотрудник Института международных исследований

КАК ОБЕСПЕЧИТЬ СОБСТВЕННЫЙ ЦИФРОВОЙ СУВЕРЕНИТЕТ?

1. Образовательные системы в области подготовки IT-специалистов в России и Беларуси, равно как и в остальных странах ЕАЭС, ориентированы на рынок, и в массе своей готовят «IT-пролетариат» с ограниченными компетенциями, которые в ближайшие несколько лет будут успешно замещаться ИИ. При этом элитных специалистов, обладающих фундаментальными знаниями, и способными решать задачи на уровне системной архитектуры, крайне мало. Это создает понятную проблему в части полноценного обеспечения цифрового суверенитета.

2. Не менее важной проблемой, ограничивающей возможности выращивания специалистов высокого уровня, является «утечка мозгов»: IT-специалисты, воспринимающие себя «гражданами мира», легко перекупаются зарубежными корпорациями. Мировоззренческая причина понятна: пока Запад воспринимается как первичный источник технологического и любого иного ноу-хау, собственная страна будет восприниматься в качестве вторичной, и потому менее интересной.

3. Нелояльность технических специалистов, таким образом, имеет два основания. Первое вполне очевидно: в основе технического образования лежит позитивизм, в отношении неживой природы можно смело игнорировать такие измерения, как, например, способность к саморефлексии и свободу воли. В отношении социальных материй такое упрощение не проходит, но технический специалист, рассуждая о социальном, этих измерений просто не видит, результатом чего является эффект «Даннинга-Крюгера», когда состоявшийся специалист может демонстрировать одновременно удивительный уровень наивности, когда речь идет о вещах социально-политических, и склонность к принятию высокорисковых, по сути — упрощенческих решений, наиболее ярким примером чего является диссидентство академика Сахарова.

4. Второе основание менее очевидно, но едва ли не более существенно. Проблема в том, что в нашей истории, начиная с Петра I, технические инновации заимствовались вместе с западными политическими инсти-

тутами, по сути — в режиме «карго-культа», когда содержание не отделялось от упаковки. Это приводило к регулярным разрушительным конфликтам между «модернизаторами» и «охранителями», наиболее значительными из которых были конфликт державников и модернизаторов при Анне Иоанновне, восстание декабристов, и диссидентство советской научно-технической элиты в начале 60-х гг. XX века. Во всех случаях целью было заимствование технологических инноваций, но ни «охранительные элиты», ни «модернизаторы» были не в состоянии провести когнитивную деконструкцию заимствований и отделить содержание от институциональной «упаковки». При этом последнее не столь сложно, это сегодня легко и на регулярной основе делает Китай, продемонстрировав возможность успешной модернизации без вестернизации. Тем не менее, в отсутствие когнитивной деконструкции итог заимствований был всегда один: последние травматически внедрялись, приводя к технологическому рывку, затем начинался конфликт привнесенных вместе с инновациями протестантских культурных кодов с базовыми православными социокультурными кодами, в результате чего вместе с водой выплескивался и ребенок, и следовал травматический откат. В СССР проблема мировоззренческой нелояльности технических элит, кстати, тоже не была решена, в результате чего институтом производства инноваций стали «шарашки», ликвидация которых тут же вывела конфликт наружу.

Таким образом, речь идет о необходимости синтеза в рамках образовательного процесса технических и гуманитарных знаний. Последние, наряду с возможностью системного осмысления таких понятий, как цивилизационный уклад, и диктуемые им приоритеты, должны прививать и базовые навыки когнитивной деконструкции. Изложить эти сложные материи на понятном для «технарей» языке вполне возможно, в качестве одной из моделей вполне может подойти и «пентакль» Харичева: по сути, тот предложил пять интеграторов, на основании которых может быть описана цивилизационная разность, и на основе которых формируется язык описания политики. Эти интеграторы — индивид, семья, общество, государство и страна. Так, для протестантской цивилизации политический язык формируется на основе интеграторов «индивид» и «корпорация», заменившей общество, для нашей цивилизации значимы интеграторы «семья», «общество» и «государство», для Китая — общество и государство. Прямое следствие отсюда — смыслы экономического производства. В протестантском мире они завязаны на максимизацию индивидуального потребления, в Китае — на потребности общества, модерируемые партией. У нас они должны быть ориентированы на те же потребности общества, основанного на традиционной ценности семьи. Преподавание гуманитарной компоненты в терминах «цивилизационного кода» может быть достаточно эффективным в части формирования осознанных ценностей, становящихся частью картины мира, что подтверждает практика преподавания в МГИМО.

5. Синтез в рамках образовательного процесса гуманитарного и технического измерений позволяет не только решать эту проблему, но и подступиться к ликвидации еще одной уязвимости, тоже существующей в режиме «карго культа». Речь идет об алгоритмах, играющих все большую роль в повседневности: последние всегда являются результатом картины мира, продвигаемой разработчиком, и, по факту, в большинстве своем продвигают протестантские ценности, свойственные англосаксонскому миру. Китай эту опасность осознал еще два года назад, национализировав алгоритмы, и поставив их под этический контроль КПК. Нигде на постсоветском пространстве эта проблема пока не решается.

6. Соответственно, задача создания национальной IT-элиты требует создания отдельного учебного заведения, в рамках которого преподавалась бы высокая математика, наряду с гуманитарной когнитивной компонентой. В качестве стартовой площадки имеет смысл создание международной, лучше всего — евразийской магистратуры, на основе коллаборации ведущих вузов в области математики и гуманитарного измерения, начав с коллаборации ФПМ БГУ и МГИМО, и имея в виду последующее присоединение к проекту ведущих вузов стран ЕАЭС в рамках практической реализации предложенной президентом России В.В. Путиным пятой евразийской свободы, свободы знаний. Тогда это станет еще одним, и весьма весомым, интегрирующим фактором для евразийского пространства. Относитель-

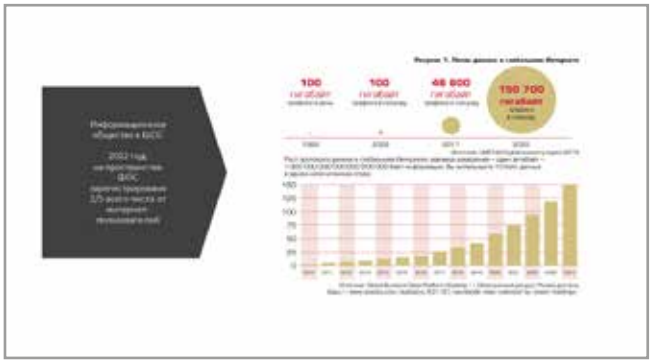
но малый стартовый формат позволит отработать учебный процесс и через какое-то время выйти на создание уже полноценного IT-университета.

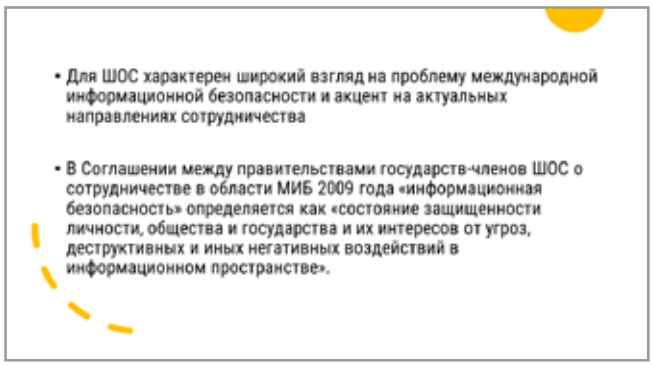
7. Представляется, что такой подход позволяет выйти на создание национальной IT-элиты, способной не только решать системные задачи, но и осознанно ориентированной на развитие и укрепление собственной цивилизации. Уместно отметить, что и в странах ШОС и БРИКС на сегодня нет специалистов, в картине мира которых успешно синтезированы технические и гуманитарные знания, а значит этот подход может стать нашим ноу-хау, продвигаемым и на внешние образовательные рынки.

8. Дополнительным и скорее иллюстративным аргументом о критической важности гуманитарного знания для осознания себя может служить британская практика: ***civil service,*** по сути — глубинное государство Британии, контролирующее все бюрократические процедуры в части чиновников категории «А», принимающих решения, состоит исключительно из гуманитариев. Эта реальность сложилась еще в колониальные времена, когда Британия контролировала большую часть мира, и с тех пор не претерпела существенных изменений. Включение в учебный процесс, скажем, когнитивной деконструкции алгоритмов британского владычества — а сегодня каждый шестой день года какая- либо страна мира празднует независимость от Британии, включая и США, автоматически позволяет оказаться «над ними», в положении субъекта, а не объекта. А это — лучшая мировоззренческая гарантия собственного суверенитета и лояльности специалистов собственным государствам.

Е.С. Зиновьева
Заместитель директора Центра международной информационной безопасности и научно-технологической политики, МГИМО МИД России

ПРОБЛЕМАТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ПОВЕСТКЕ ШОС






Глобальная цифровая трансформация в повестке ШОС
• 2019 год - на заседании СГГ ШОС в Бишкеке была утверждена Концепция сотрудничества государств-членов Шанхайской организации сотрудничества в сфере цифровизации и информационно-коммуникационных технологий.
• повышение глобальной конкурентоспособности и цифровое преобразование в национальных экономиках государств-членов ШОС путем внедрения инноваций и современных ИКТ;
• повышение инвестиционного потенциала, преодоление цифрового разрыва, повышение информационной безопасности для обеспечения равного и безопасного доступа к современным ИКТ


Глобальная цифровая трансформация в повестке ШОС
• 2020 году в Москве было принято Заявление о сотрудничестве в области цифровой экономики:
• важность развития сотрудничества в сфере цифровизации, информационно-коммуникационных технологий в промышленности, транспорта, сельского хозяйства, здравоохранения, образования, туризма, энергетики, торговли, финансов и таможни;
• изучения вопросов взаимодействия в сфере программ и научных разработок в области «сквозных» цифровых технологий, искусственного интеллекта, робототехники, Интернета вещей.


Глобальная цифровая трансформация в повестке ШОС
• 2022 год на саммите ШОС в Самарканде были приняты:
• Программа сотрудничества между уполномоченными органами государств-членов по развитию цифровой грамотности
• Программа сотрудничества между уполномоченными органами государств-членов по развитию искусственного интеллекта.


Актуальные тенденции международного сотрудничества ШОС по МИБ
• 2020 год - в Москве Заявлении Совета глав государств-членов ШОС о противодействии распространению террористической, сепаратистской и экстремистской идеологии, в том числе в сети Интернет, была подтверждена важность коллективных подходов к борьбе с терроризмом и питающим его экстремизмом.
• 2021 год – на юбилейном заседании СГГ ШОС в Душанбе в прошлом году был принят План взаимодействия государств-членов ШОС по вопросам обеспечения международной информационной безопасности на 2022-2023 годы
• 2022 год - в составе Исполнительного комитета Региональной антитеррористической структуры ШОС был создан Департамент МИБ, который возглавил заместитель Директора Исполкома, гражданин Индии Ракеш Кумар.
• 2023 год - беспечение информационной безопасности и реагирование на вызовы и угрозы в интернете в 2023 году официально выделены в отдельное направление работы Региональной антитеррористической структуры Шанхайской организации сотрудничества (РАТС ШОС)

Бай Яцзе
Эксперт МГИМО МИД России (Китай)

ЭВОЛЮЦИЯ ПОДХОДОВ К ТЕМЕ МИБ В БРИКС — ВЗГЛЯД ИЗ КИТАЯ

Как мы все знаем, технология искусственного интеллекта — это технология, которая использует современные компьютеры и данные для имитации человеческого мышления и решения проблем. Это одна из важных движущих сил, ведущих новую волну технологий к четвертой промышленной революции. В последние годы развитие искусственного интеллекта ускорилось до предела: голосовые помощники, беспилотный автомобиль, «умные дома», «умные города» и т.д. — все это примеры использования искусственного интеллекта в повседневной жизни, охватывающие широкий спектр областей, таких как финансы, образование, здравоохранение и транспорт. Искусственный интеллект оказывает глубокое влияние на общество, экономику, и даже военно-политическую безопасность.

Этапы развития искусственного интеллекта в новую эпоху условно можно разделить на три стадии: машинное обучение, глубокое обучение и ИИ-сгенерированный контент (AI Generated Content). Первый — применение методов машинного обучения, возникшее в основном в первом десятилетии этого века, означает процесс анализа больших объемов данных с помощью алгоритмов, имитирующих поведение человека в процессе обучения. Второй — глубокое обучение (более углублённое обучение) преимущественно быстро развивалось во втором десятилетии этого века. Оно направлено на имитацию структуры человеческого мозга с его сложными многослойными нейронными сетями. В таких областях как, например, автомобили без водителя и превентивное здравоохранение, применяется более глубокое обучение, чем машинное обучение.

ИИ-сгенерированный контент рассматривается как будущая тенденция развития искусственного интеллекта. Получая большой объем данных, он имитирует метод расчёта нейронной сети человеческого мозга, понимает закономерности и правила в данных и генерирует новые данные, включая текст. картинки, музыку и другие формы. Например, ChatGPT, разработанный компанией OpenAI и запущенный в ноябре прошлого года, является типичным применением ИИ-сгенерированного контента. Он представляет собой интерактивный диалоговой робот, основанный на технологии ИИ-сгенерированного контента, способный решать проблемы взаимодействия людей. Он может не только генерировать вопросы и ответы, но и служить основой для широкого спектра сервисов, таких как распознавание речи, генерация текста и т.д., например, чат-ботов, систем вопросов и ответов, машинного перевода. Таким образом, достигается реальное ощущение взаимодействия между пользователями и программами. Технологии ИИ-сгенерированного контента имеют огромный потенциал развития и применения, позволяя создавать новые художественные произведения, генерировать текст и музыку, редактировать и улучшать изображения, создавать видео и т.д. Он также широко используется в дизайне и архитектуре, онлайн-играх, фармацевтических исследованиях и разработках, и других областях. Он может даже произвести прорыв в поисковых системах.

В последние годы китайская индустрия искусственного интеллекта высоко оценивается правительствами всех уровней и получила значительную поддержку со стороны промышленности. Государством был принят ряд мер, направленных на стимулирование развития и инноваций в области искусственного интеллекта. Начиная с 2013 г. был выпущен

ряд документов, посвященных искусственному интеллекту, таких как «Руководящие мнения Государственного совета по активному продвижению инициативы «Интернет плюс»», «План развития искусственного интеллекта нового поколения», «Уведомление о поддержке создания демонстрационных и прикладных сценариев искусственного интеллекта нового поколения», «Руководящие мнения по ускорению сценарных инноваций и содействию высококачественному экономическому развитию посредством высокоуровневого применения искусственного интеллекта» и «Трехлетний план действий по развитию новых центров обработки данных (2021–2023 гг.)».

Эти политические меры являются долгосрочной гарантией эффективного развития китайской индустрии искусственного интеллекта в долгосрочной перспективе.

2023 г. является важным для развития искусственного интеллекта, и Китай выпустил несколько соответствующих документов, направленных на его развитие. В частности, 13 июля Государственное управление интернет-информации Китая (Cyberspace Administration of China) совместно с шестью министерствами и ведомствами: Национальной комиссии по развитию и реформам (National Development and Reform Commission (NDRC)), Министерством образования (Ministry of Education (MOE), Министерством науки и технологий (Ministry of Science and Technology(MOST)), Министерством промышленности и информационных технологий (Ministry of Industry and Information Technology (MIIT)), Министерством общественной безопасности (MPS) и Национальным управлением радио и телевидения (National Radio and Television Administration) опубликовало «Временные меры по управлению ИИ-сгенерированным контентом» , которые вступили в силу с 15 августа 2023 г. Данный документ усиливает регулирование ИИ-сгенерированного контента и создает правовую основу для его более эффективного использования.

Сообщается, что проект закона об искусственном интеллекте включен в план законодательной работы Госсовета Китая на 2023 г.

Помимо национального правительства Китая, провинциальные и муниципальные власти, IT-гиганты также придают большое значение развитию искусственного интеллекта.

Согласно изученным нами статистическим данным, с 2023 г. 12 провинций и городов, включая Пекин, Шанхай, провинцию Цзянсу, Чжэцзян и т.д., в последних опубликованных программных документах прямо указали на поддержку планирования искусственного интеллекта, которая включает различные аспекты, такие как исследования и разработки, применение, привлечение проектов, производство и услуги.

Китайские ИТ-гиганты Хуавей (Huawei), Бэйду (Baidu), Тенсент (Tencent) и другие тех-

нологические компании увеличили объем инвестиций и научно-исследовательские работы в области искусственного интеллекта, пытаясь в полной мере использовать огромную коммерческую и прикладную ценность, заключенную в больших данных.

Например, в августе 2023 г. китайская технологическая компания Бэйду официально представила публике «китайскую версию ChatGPT» — Ernie.Bot. Будучи большой языковой моделью, укоренившейся на китайском рынке, Ernie.Bot обладает самыми передовыми возможностями обработки естественного китайского языка и не менее передовыми в области понимания и применения китайского языка и культуры.

3 февраля 2023 г. технологическая компания Тенсент объявила о получении патента на интерфейс «человек-машина», обеспечивающий свободное и плавное общение между машинами и пользователями.

В сентябре 2023 г. компания Хуавей выпустила мобильный телефон новой модели «Mate 60» с поддержкой сети 5G. Обновленный чип (Kirin 9000S) и система Хунмэн (Hongmeng) полностью разработаны в Китае, что привело к прорыву технологической блокады. Этот чип обладает мощными вычислительными возможностями в многозадачном режиме, способностью обрабатывать изображения и рассуждения с использованием искусственного интеллекта.

Акцент Китая на искусственный интеллект и его продвижение не ограничивается самой страной. Китай также активно продвигает искусственный интеллект и участвует в обменах и сотрудничестве с другими странами на международных платформах и в международных организациях. Особенно на платформе БРИКС поощряется сотрудничество между странами в целях энергичного развития искусственного интеллекта и обеспечения международной информационной безопасности.

Являясь самой динамичной и влиятельной развивающейся экономической системой в мире, БРИКС уже давно привержен поддержанию сотрудничества между странами-членами в ряде областей, таких как продовольственная безопасность, энергетическая безопасность, глобальное изменение климата, реформа финансовых институтов, валютная безопасность и информационная безопасность. На 15-й встрече лидеров БРИКС в августе 2023 г. было официально объявлено о расширении состава участников БРИКС: шесть стран — Аргентина, Египет, ОАЭ, Иран, Саудовская Аравия и Эфиопия приглашены присоединиться к механизму сотрудничества БРИКС. Это не только расширение числа членов, но и увеличение влияния развивающихся стран в мире.

В ходе встречи лидеры провели углубленный обмен мнениями по вопросам сотрудни-

чества БРИКС и основным международным проблемам, представляющим взаимный интерес. Достигли широкого консенсуса. Лидеры стран БРИКС совместно объявили, что искусственный интеллект — это новая область развития человечества, и договорились как можно скорее начать работу над созданием исследовательской группы по искусственному интеллекту.

Председатель КНР Си Цзиньпин, выступая на встрече, заявил, что все должны и дальше расширять сотрудничество в области искусственного интеллекта, укреплять обмен информацией и технологиями, совместно работать над предотвращением рисков, способствовать созданию универсального международного механизма информационной безопасности, формировать структуру управления, стандарты и нормы искусственного интеллекта на основе широкого консенсуса, постоянно повышать безопасность, надежность, контролируемость и справедливость технологий искусственного интеллекта. Кроме того, Китай и БРИКС обязались создать совместный научно-инновационный инкубатор для того, чтобы ускорить сотрудничество в области искусственного интеллекта между странами-членами БРИКС.

Актуальность продвижения сотрудничества в области искусственного интеллекта обсуждалась еще на предыдущих встречах. На 14-ом саммите лидеров БРИКС в 2022 г. было предложено использовать новые возможности экономического развития, такие как большие данные и искусственный интеллект. Их использование означает идти в ногу со временем; на 13-ом саммите лидеров в 2021 г. БРИКС определила «цифровые технологии для достижения целей устойчивого развития (ЦУР)» одним из приоритетных направлений сотрудничества на тот год.

Кроме того, в рамках БРИКС действуют такие механизмы, как встреча министров иностранных дел и встреча высоких представителей по вопросам безопасности, которые используются для углубления сотрудничества в области борьбы с терроризмом и кибербезопасности, а также для укрепления координации во многосторонних структурах, таких как ООН.

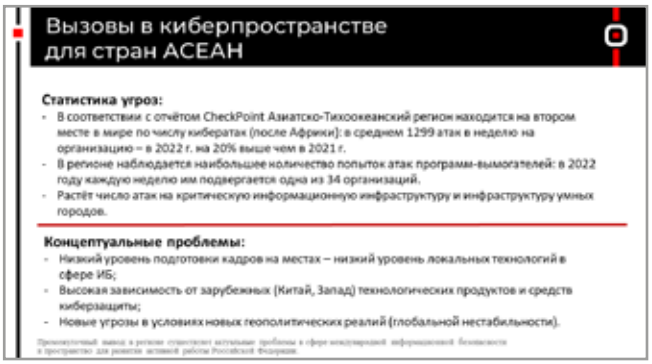
Остальные формы сотрудничества между странами-членами БРИКС показаны в виде таблицы.

Конференции/ мероприятия	**Время**	**Организатор/Участники**	**Содержание**
Сетевой инновационный форум будущего БРИКС 2023 года	04.09.2023	Министерство промышленности и информационных технологий Китая, муниципальное правительство Шэньчжэня (Китай)	Под лозунгом «Сетевые инновации способствуют высококачественному развитию», страны БРИКС расширяют сотрудничество в области искусственного интеллекта и совместно проводят технологические исследования и разработки в новых областях.
Глобальный диалог по вопросам развития на высоком уровне	06.2022	В ходе 14-го саммита БРИКС	БРИКС обсуждает вопросы глобального развития, представляющие взаимный интерес
«Рамочная программа партнерства БРИКС в области цифровой экономики»	06.2022	В ходе 14-го саммита БРИКС	В рамках этой структуры обсуждаются и принимаются меры для текущих передовых областей цифровой экономики, соглашается сотрудничать в области новых технологий, таких как искусственный интеллект.
Форум БРИКС по развитию промышленного Интернета и цифрового производства	05.2022	При поддержке Министерства промышленности и информационных технологий Китая, Народного правительства провинции Фуцзянь (Китай) и Народного правительства муниципалитета Сямэнь (Китай).	Создание Сямыньской инновационной базы Партнерства БРИКС по новой промышленной революции. Обнародована «Инициатива сотрудничества стран БРИКС в области цифровой трансформации производства». Фокус на тему «Инновационное развитие промышленного Интернета и содействие цифровой трансформации обрабатывающей промышленности».
8 заседание Рабочей группы БРИКС по кибербезопасности	24.05.2022	Встречу принимал Китай, во встрече и обсуждении приняли участие функциональные подразделения кибербезопасности стран БРИКС.	БРИКС обменялись углубленными мнениями по политическим и законодательным обменам, наращиванию потенциала, укреплению многостороннего сотрудничества и другим вопросам вокруг итогового документа «Дорожная карта практического сотрудничества БРИКС в области кибербезопасности», принятого 4.09.2017.

Конференции/ мероприятия	Время	Организатор/Участники	Содержание
Форум больших данных по устойчивому развитию БРИКС	26.04.2022	Академии наук стран-членов БРИКС	БРИКС инициировали сотрудничество в научных исследованиях в области больших данных для устойчивого развития и использования технологических инновации и технологии больших данных в рамках процесса ЦУР ООН 2030 г.
Платформа цифровых общественных благ БРИКС		Индия — инициатор	Платформа может служить хранилищем технологий, созданных странами БРИКС для достижения Целей устойчивого развития, принося пользу странам БРИКС и другим развивающимся странам.
Социальная инфраструктура: финансирование и технический отчет о применении цифровых технологий		Рабочая группа БРИКС по сотрудничеству в области инфраструктуры и государственного и социального капитала.	В отчете отражены коллективные усилия стран БРИКС по продвижению цифровых платформ и технологических приложений.
Глобальная инициатива по безопасности данных	2020	В ходе 12-го саммита лидеров БРИКС	Китай предлагает углублять диалог и сотрудничество и совместно строить сообщество-киберпространства с общим будущим мира, безопасности, открытости, сотрудничества и сообщества.

В.А. Педанов
Генеральный директор ООО «Технологии Безопасности Транспорта», представитель Группы Компаний «Инжиниринговые Технологии в АСЕАН»

ОСОБЕННОСТИ ОБЕСПЕЧЕНИЯ МИБ В АСЕАН В НОВЫХ ГЕОПОЛИТИЧЕСКИХ РЕАЛИЯХ




JICA
Japan International Cooperation Agency
Opening Ceremony for the First Training Session at the ASEAN-Japan Cybersecurity Capacity Building Centre in Thailand Contributing to the cultivation of cybersecurity experts in ASEAN member states


Заключение
Выводы:
- страны АСЕАН нуждаются в поддержке развития безопасности ИКТ, благоприятный момент для России оказать такую поддержку.
- страны АСЕАН наращивают взаимодействие с другими глобальными игроками в сфере МИБ. Для того, чтобы не остаться за бортом этого процесса, Россия должна наращивать работу в этом направлении.
- перспективы сотрудничества стран АСЕАН с Россией открывают широкий потенциал безопасного и устойчивого развития и выработки мер доверия в области ответственного поведения государств.
Предложения:
1. Создать в департаменте МИБ МИД России отдел (направление) по работе со странами АСЕАН;
2. Активизировать работу по линии обмена информацией по актуальным инцидентам информационной безопасности, которое может выражаться в обмене данными между ГосСОПКА и CERT-командами стран АСЕАН;
3. Изучить опыт The CyberGreen Institute (Британия), а также опыт AJCC BC (Япония), рассмотреть возможность создать аналогичную организацию вместе с государствами АСЕАН (со всем АСЕНА или с отдельными странами);
4. Рассмотреть возможности финансирования совместных программ в сфере МИБ и кибербезопасности в частности.

И.В. Сурма
Кандидат экономических наук, доцент кафедры Международной и национальной безопасности Дипломатической академии МИД России, член-корреспондент РАЕН, вице-президент НИИГлоб

ПОЛЯРИЗАЦИЯ КИБЕРПРОСТРАНСТВА И РОЛЬ ОДКБ В РАЗВИТИИ МЕЖГОСУДАРСТВЕННОГО СОТРУДНИЧЕСТВА В СИСТЕМЕ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Современные ИКТ являются универсальным инструментом политико-социально-экономической трансформации, под воздействием которого изменяется социум, что приведёт, в конечном счёте, к тому, что информационное общество, скорее всего, будет трансформироваться в сверхинтеллектуальное общество, основанное на эффективной оптимизации ресурсов не только отдельного человека, а общества в целом через интеграцию физического (реального) уровня и киберпространства (виртуального уровня). Важным аспектом этого процесса является создание равных возможностей для всех, а также обеспечение среды для реализации потенциала каждого человека. В процессе производства вся собранная в физическом пространстве информация будет накапливаться в киберпространстве и, благодаря технологии искусственного интеллекта (ИИ), появляется возможность анализировать эти данные, находить оптимальные решения для организационно-производственных и финансовых процессов, которые затем использовать для управления конкретными объектами и процессами в реальном физическом пространстве. По прогнозам RAND Corporation, в мире к 2025 году будет насчитываться более 41 млрд активных устройств, которые будут ежедневно генерировать 2,5 квинтиллиона байтов данных об окружающей среде, геолокациях, транспорте, питании, упражнениях, биометрии, социальном взаимодействии людей и повседневной жизни человека и целого государства. В связи с этим существуют кибер-риски, относящиеся к потенциальной вероятности взлома этой системы и риски утечки конфиденциальных данных и данных о так называемых критических инфраструктурах.

Количество скомпрометированных записей персональных данных и платежной информации в мире за 2022 год превысило 20 млрд, в то время как в «рекордном» за предыдущие 5 лет 2019 году утекло 15,23 млрд записей. На долю персональных данных пришлось 82,3% утечек, а на долю коммерческой тайны — 14,6%.

Сегодня анализируя 2022 год, можно с уверенностью сказать, что напряженность в международных отношениях между государствами растет и это всё больше сказывается на том, как развиваются попытки регулировать киберпространство и сферу кибербезопасности, включая военную. Сложившаяся в 2022 году картина утечек отражает сильную зависимость состояния информационной безопасности от мировой политики. Геополитические изменения в мире привели к росту количества кибер-инцидентов практически во всех странах, что также спровоцировало резкое увеличение количества зафиксированных утечек персональных данных. Причём высокий рост утечек данных был зафиксирован не только в ряде стран Евросоюза (Франция, Испания, Германия), но также в Юго-Восточной Азии (Индонезия), Центральной Америке (Мексика), Ближнем Востоке (ОАЭ), Китае и ряде других регионов. Недавно эксперты по кибербезопасности зафиксировали крупнейшую утечку конфиденциальной информации в истории Китая. В руки злоумышленников

попали персональные данные миллиарда жителей. Предположительно, такой огромный массив информации был получен в результате взлома информационных систем полиции Шанхая.

Растущая поляризация киберпространства создает риски безопасности для многих, ведь киберугрозы и инциденты не знают границ. Даже если злоумышленники изначально планируют атаковать одну или несколько конкретных организаций, атака может выйти далеко за пределы первой цели и распространиться на все цепочки поставок ИКТ. Способны ли будут организации, относящиеся к разным юрисдикциям, обмениваться информацией об угрозах и смогут ли они сотрудничать глобально по реагированию на угрозы? Некоторые — да, но возникает все больше и больше вопросов и даже барьеров и вместе с ними — рисков безопасности.

Происходит фрагментация киберпространства, но теперь разделение происходит по принципу схожести убеждений — не только среди государств, но и среди негосударственных структур. Последние геополитические события усугубили поляризацию между разными группами государств и сообществ. Так традиционно сплоченное IT-сообщество, которое, как предполагается, должно занимать нейтральную позицию и помогать бороться с киберугрозами, также разбивается на отдельные закрытые группы. Например, международные организации *Forum of Incident Response and Security Teams* (FIRST) или *Computer Emergency Response Team* (CERT) могут вообще не включить или приостановить членство ряда организаций, учрежденных в определенных юрисдикциях, что противоречит фундаментальному принципу доверия в области кибербезопасности. Сегодня не существует системной защиты личности в современном мире, а организации уровня FIRST или CERT, скорее всего будут мотивироваться либо чисто коммерческими интересами («кто заплатил, того и защитили»), либо политическими, что ставит под сомнение защиту частных лиц и организаций независимо от их географического положения, государственной и национальной принадлежности. Это приведёт к тому, что организации начнут обсуждение возможности инициации собственных альтернативных сообществ. Подобные объединения априори не могут обеспечить равноправное и справедливое участие всех стран в работе по реагированию на кибератаки из-за их существенной политизации и нежелания реализовывать открытое и прагматичное взаимодействие с уполномоченными специалистами отдельных стран. Это, в свою очередь, не способствует стабильности и развитию международной архитектуры кибербезопасности для снижения рисков и обеспечения международного мира в цифровую эпоху.

При этом, одним и единственным авторитетным международным органом, который способен выступить объединяющим началом всех международных усилий в области противодействия киберугрозам и обеспечения кибербезопасности, является ООН, но страны по-разному смотрят на регулирование киберпространства и кибербезопасности. Лишь некоторые успели принять правила, нормы и законодательства с экстерриториальным действием (например, GDPR — Общий регламент защиты данных Европейского Союза, устанавливающий требования к различным организациям за пределами ЕС), сделав это, они расширили свое влияние далеко за пределы национальных границ.

Таким образом, сегодня требуется объединить усилия на уровне всех стран в рамках ООН, создав, например, профильный комитет при ООН по вопросам международной информационной безопасности (как предложение, это может быть, например, подкомитет по вопросам международной информационной безопасности или кибербезопасности при Первом комитете Генассамблеи (С1)), в который войдет только одна официальная структура от каждого государства-члена ООН и, которая будет представлять свою страну и нести ответственность за вопросы обеспечения международной кибербезопасности и урегулирование международных киберинцидентов. При этом международные организации подобные CERT и FIRST будут находиться в своих национальных юрисдикциях и смогут выступать вспомогательным элементом, обеспечивающим деятельность и экспертное сопровождение официальной структуры от своей страны при таком подкомитете ООН.

Однако в сложившихся современных геополитических условиях при усиленном лоббировании и влиянии США внутри ООН и по-

пытках принизить или вообще «заиграть» ряд важных и актуальных инициатив России, особую значимость приобретают решения и практика, реализуемые на региональном и субрегиональном уровнях. В этой связи интересен опыт ОДКБ, которая разрабатывает правовые основы скоординированной информационной политики. С 2008 г. ОДКБ реализует Программу совместных действий по созданию системы информационной безопасности ее государств-членов. Важным элементом реализации этой Программы стало принятие Советом коллективной безопасности ОДКБ Положения о сотрудничестве государств в сфере информационной безопасности, которое предусматривает формирование организационно-координирующей структуры и регулярное проведение оперативно-профилактических мероприятий, направленных на борьбу с киберпреступлениями.

К первому успешному опыту скоординированных мероприятий ОДКБ по противодействию преступлениям в информационной сфере можно отнести проведение в 2009 году специальной операции под условным названием «ПРОКСИ» («Противодействие криминалу в сфере информации»). В этой операции приняли участие специальные подразделения органов безопасности и внутренних дел всех государств-членов ОДКБ. В результате скоординированных совместных действий стран-участниц за достаточно короткий промежуток времени в национальных сегментах Интернета были выявлены более сотни информационных ресурсов, используемых для распространения сведений, наносящих политический ущерб государственным интересам странам-участницам ОДКБ, разжигающих национальную и религиозную рознь, содержащих информацию, предназначенную для организаций террористической и экстремистской направленности и др. После проведения соответствующих оперативных и следственных мероприятий, было возбуждено более 530 уголовных дел. Непосредственно в России была приостановлена деятельность 216 информационных ресурсов и выявлено 208 преступлений, по которым возбуждены уголовные дела.

Еще одним примером успешного опыта ОДКБ стало создание в 2014 году Консультационного координационного центра по вопросам реагирования на компьютерные инциденты (ККЦ ОДКБ) с целью координации взаимодействия уполномоченных органов по вопросам, связанным с компьютерными инцидентами, несущими угрозы функционированию информационно-телекоммуникационных сетей и информационных систем любого из государств-членов ОДКБ.

Следует отметить, что проблема международной информационной безопасности также постоянно находится в сфере внимания Парламентской Ассамблеи ОДКБ (ПА ОДКБ). В рамках Программы деятельности ПА ОДКБ на 2016–2020 годы была разработана «Концепция плана действий и инструментария в вопросах противодействия кибервызовам и угрозам» (принята 30 ноября 2020 года), а 13 октября 2017 года — «Рекомендации по совершенствованию уголовного законодательства государств-членов ОДКБ по вопросам борьбы с правонарушениями в информационной сфере» и 30 октября 2018 года — Модельный закон «Об информационном противоборстве терроризму и экстремизму».

В развитие Соглашения о сотрудничестве государств-членов ОДКБ в области обеспечения информационной безопасности, которое было подписано 30 ноября 2017 года и вступило в силу в апреле 2019 года, МИДом России подготовлен проект решения Совета министров иностранных дел и Комитета секретарей советов безопасности ОДКБ о перечне дополнительных мер, направленных на обеспечение информационной безопасности в Организации. В сентябре 2022 года этот документ был одобрен на заседании Постоянного совета ОДКБ и направлен в страны-члены на внутригосударственные согласования.

Подчеркнём, что Программой деятельности ПА ОДКБ на 2021–2025 годы предусмотрена разработка целого ряда модельных законов и рекомендаций в области обеспечения международной информационной безопасности:

- модельного закона ОДКБ «Об обеспечении защиты критически важных объектов информационной инфраструктуры»;
- модельного закона ОДКБ «О защите информации и кибербезопасности»;
- модельного закона ОДКБ «Об информационной безопасности»;

- рекомендаций для государств-членов ОДКБ по выработке общих принципов развития национального законодательства по формированию и использованию больших данных в целях обеспечения национальной безопасности;
- рекомендаций для государств-членов ОДКБ по выработке общих принципов развития национального законодательства в области создания искусственного интеллекта и робототехники в целях обеспечения национальной безопасности;
- рекомендаций по гармонизации законодательства государств-членов ОДКБ о цифровых подписях в целях обеспечения информационной безопасности;
- рекомендаций для государств-членов ОДКБ по выработке общих принципов государственного регулирования сети Интернет в целях обеспечения национальной безопасности;
- рекомендации по регулированию оборота виртуальных валют (противодействию распространению криптовалют и иных электронных суррогатов платежных средств, подрывающих (разрушающих) национальные финансовые системы).

Кроме того, Советом министров иностранных дел ОДКБ и Комитетом секретарей советов безопасности ОДКБ было принято решение о проведении профильных межведомственных консультаций по тематике международной информационной безопасности начиная с 2022 года, сроком на три года, что позволит на регулярной основе координировать позиции стран-участниц по наиболее актуальным вопросам.

Таким образом, можно заключить, что Организация Договора о коллективной безопасности и Парламентская Ассамблея ОДКБ в настоящее время являются одной из важных международных площадок для реализации справедливого международно-правового режима в сфере предотвращения и урегулирования межгосударственных конфликтов в глобальном информационном пространстве.

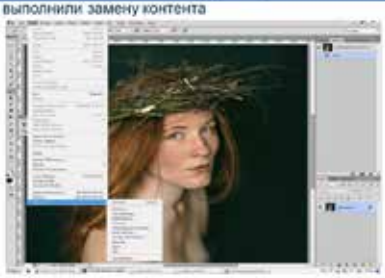
Видится, что такой положительный опыт ОДКБ, независимо от реализации российских инициатив в рамках РГОС на международных площадках ООН, следует транслировать и на страны БРИКС и другие региональные объединения. И одним из основных направлений реализации такой политики в области информационной безопасности должно быть проведение на двусторонней и многосторонней основе экспертных консультаций, а также согласование ключевых позиций и основных направлений сотрудничества в области обеспечения международной информационной безопасности со странами-участницами СНГ и государствами БРИКС.

Д.Б. Фролов
Советник Департамента информационной безопасности Российской телевизионной и радиовещательной сети

НОВЫЕ ВЫЗОВЫ И УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СФЕРЕ ТЕЛЕРАДИОВЕЩАНИЯ В МЕЖДУНАРОДНОМ И РЕГИОНАЛЬНЫХ ИЗМЕРЕНИЯХ

Пусть ИИ выполнил подмену контента…

Нейросети выполнили замену контента



МТУСИ

Но всегда остаются артефакты…

Глубокое обучение для изменений проекции в пространстве

МТУСИ

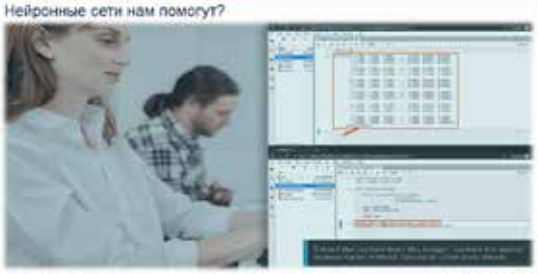
А иногда и «ляпы» работы ИИ…

Случаются казусы при общем автоматизированном подходе (в т.ч. при анализе – когда заведомо «хорошее» изображение менее убедительно «плохого»…

МТУСИ

Как с этим бороться?

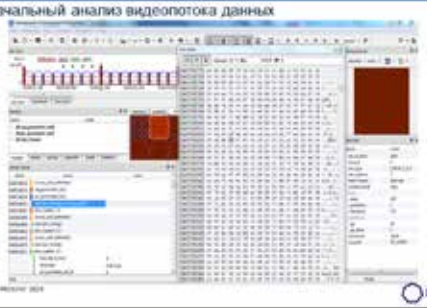
Нейронные сети нам помогут?



МТУСИ

Всегда остаются артефакты…

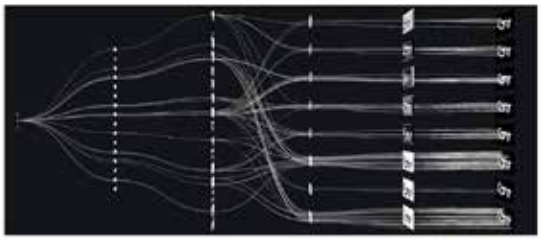
Первоначальный анализ видеопотока данных



МТУСИ

Как с этим бороться?

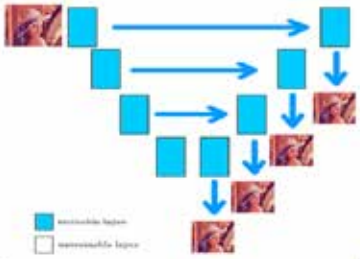
Детальное разложение элементов изображения. Поиск артефактов.



МТУСИ

Как с этим бороться?

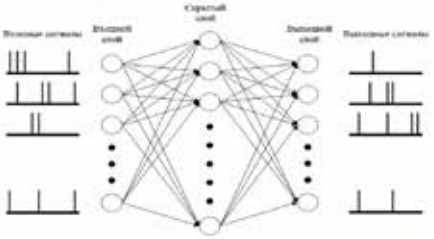
Обратная тренировка нейросети на поиск артефактов.



МТУСИ

Как с этим бороться?

Возможное использование импульсных нейросетей для анализа дискретного потока данных.



МТУСИ

Как этому противостоять?

Использование технологии блокчейн дает некоторую уверенность, что контент не был изменен. Хотя есть сложности в реализации – многие оконечные устройства обладают слабыми CPU и могут не обработать необходимые проверки

Осуществление мониторинга источников видеопотока, аутентификация с помощью цифровых водяных знаков

Разработка технологий анализа видеопотока «на лету» с целью детектирования изменений, определение нарушения целостности и, при необходимости, оперативного блокирования негативного контента (аналог IDS / IPS систем)

МТУСИ

Что ждет в дальнейшем?

МТУСИ

П.А. Карасев
Старший научный сотрудник Центра ИПИБ МГУ им. М.В. Ломоносова, эксперт Национальной Ассоциации международной информационной безопасности

Р.А. Шаряпов
Ведущий научный сотрудник Центра ИПИБ МГУ им. М.В. Ломоносова

МЕЖДУНАРОДНАЯ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В БРИКС: ОБЩЕЕ ПОНИМАНИЕ И СИНЕРГИЯ УСИЛИЙ

Непрерывно возрастающие угрозы, исходящие из ИКТ-среды, носят трансграничный и глобальный характер. Эффективно бороться с ними возможно только на международном уровне — при взаимовыгодном, взаимоуважительном диалоге стран, с учетом законных национальных интересов и при соблюдении соответствующих норм международного права. Это должно быть не общение гегемона с вассалами, а равных с равными. У государств может быть разный уровень развития в сфере ИКТ, к тому же до сих пор не преодолена проблема цифрового разрыва, сохраняется разделение на «богатый Север» и «бедный Юг», но помощь в наращивании потенциала не должна перерождаться в навязывание догм кибербезопасности «сверху», без учета национальных интересов. Это приведет к технико-политическому закабалению менее развитых стран, а не к решению их проблем информационной безопасности.

Международное сотрудничество по проблематике информационной безопасности поступательно развивается уже не первый год. Так, в сентябре этого года исполнилось 25 лет как Россия первой озвучила проблему безопасности ИКТ-среды на площадке Организации Объединенных Наций. В письме Министра иностранных дел России И.С. Иванова на имя Генсекретаря ООН Кофи Аннана было сказано, что есть серьёзная «опасность использования достижений в информационной сфере в целях, не совместимых с задачами поддержания мировой стабильности и безопасности»[1]. Речь также шла о «создании информационного оружия и опасности возникновения информационных войн,... как действий одной страны, направленных на нанесение ущерба информационным ресурсам и системам другой»[2]. Кроме того, было отмечено, что «возникает реальная угроза воздействия

1 ГА ООН, «Письмо Постоянного представителя Российской Федерации при Организации Объединенных Наций от 23 сентября 1998 года на имя Генерального секретаря», С. 2. URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N98/284/60/PDF/N9828460.pdf?OpenElement

2 Там же.

на информационные ресурсы в террористических и криминальных целях, последствия которого также могут иметь катастрофический характер». Таким образом, была обозначена триада угроз информационной безопасности, которая в конце 1999 г. была закреплена в резолюции «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» :

«Генеральная Ассамблея... выражая озабоченность тем, что эти технологии могут быть использованы в целях, несовместимых с задачами обеспечения международной стабильности и безопасности, и могут негативно воздействовать на безопасность государств, применительно как к гражданской, так и к военной сфере, считая необходимым предотвратить неправомерное использование информационных ресурсов или технологий в преступных или террористических целях»[3].

На уровне ООН одним из инструментов создания основ системы международной информационной безопасности (МИБ) стали заседания Группы правительственных экспертов ООН по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности (ГПЭ). Сегодня можно подвести некоторые итоги уже проведенной и продолжающейся работы. В положительный актив ГПЭ можно записать, среди прочего, согласование в 2015 г. норм, правил и принципов ответственного поведения государств в ИКТ-среде — это та основа, которая учитывается в большинстве международных инициатив. Одновременно, реализуемые в ООН инициативы показали политико-идеологические расхождения относительно того, как именно обеспечивать безопасность ИКТ-среды — и это стало причиной непринятия консенсусом докладов нескольких ГПЭ.

Во-вторых, сотрудничество эволюционирует как по формату, так и по тематике. Так, в 2018 г. было положено начало процессу в рамках Рабочей группы ООН открытого состава (РГОС) по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности. К участию были приглашены представители всех государств- членов ООН, а также были предусмотрены механизмы, обеспечивающие инклюзивность других, негосударственных, акторов. Сейчас идёт работа уже второй РГОС, продолжается разработка универсальной Конвенции ООН по противодействию использованию ИКТ в преступных целях. Активизировался диалог по преодолению вызовов, создаваемых развитием искусственного интеллекта.

На фоне существующих расхождений в подходах к решению многих вопросов информационной и кибербезопасности и, одновременно, наличия запроса на преодоление новых вызовов и угроз при использовании и развитии ИКТ-средств, новую актуальность приобретает взаимодействие на региональном и межрегиональном уровне. БРИКС — международное объединение пяти государств (Бразилии, России, Индии, Китая и Южно-Африканской Республики) — обладает значительным потенциалом эффективного решения многих проблем от пандемии до финансовых кризисов, и повестка международной информационной безопасности не является исключением.

История обсуждения тематики МИБ в БРИКС насчитывает не один год. Впервые она была затронута в итоговом документе III Саммита БРИКС (Санья, КНР, 13–14 апреля 2011 г.), где страны выразили «приверженность сотрудничеству в укреплении международной информационной безопасности», а также высказали намерение уделить «особое внимание борьбе с киберпреступностью»[4]. По итогам V Саммита БРИКС (Дурбан, ЮАР, 26–27 марта 2013 г.) страны-участники объединения отметили, среди прочего, «исключительно важную позитивную роль, которую играет интернет в мире в плане содействия экономическому, социальному и культурному развитию», а также подчеркнули, что «безопасность при использовании информационных и коммуникационных технологий с применением универсально признанных норм, стандартов и практик имеет первостепенную важность»[5].

3 Там же.

4 Национальный Комитет по исследованию БРИКС, «Декларация, принятая по итогам саммита БРИКС (г.Санья, о.Хайнань, Китай, 14 апреля 2011 года)», URL: https://nkibrics.ru/system/asset_docs/data/53fd/b5d2/6272/6907/2b09/0000/original/III_саммит Брик -_Саньянская декларация (г.Санья _о.Хайнань _Китай _14_апреля 2011_года)(1).docx?1409136082 п. 11.

5 Национальный Комитет по исследованию БРИКС, «Этеквинская декларация и Этеквинский план действий, 27 марта 2013 года», URL: https://nkibrics.ru/system/asset_docs/data/53da/1fa2/676c/761f/8d13/0000/original/V_саммит БРИКС -_Этеквинская декларация (г._Дурбан _ЮАР _27_марта 2013_года).docx?1406803874, п. 34.

На рубеже 2013-2014 гг. произошел качественный скачок в обсуждении тематики МИБ в БРИКС, и итоговые декларации объединения стали гораздо более субстантивными на этом направлении. Стоит вспомнить, что именно летом 2013 г. в публичном дискурсе стали доступны секретные материалы о тотальной слежке спецслужб США с использованием ИКТ, раскрытые Эдвардом Сноуденом — бывшим сотрудником американской разведки. Эта информация подтвердила точку зрения, что США используют своё технологическое доминирование и глобальную сеть интернет для продвижения собственных национальных интересов, не считаясь с интересами других государств, даже собственных союзников. В итоговой декларации VI Саммита БРИКС (Форталеза и Бразилиа, Бразилия, 15–16 июля 2014 г.) страны решительно осудили «акты массовой электронной слежки и сбора данных о частных лицах по всему миру, а также нарушение суверенитета государств и прав человека, в частности права на неприкосновенность частной жизни»[6]. Принципиально важной стала выработка общего видения стран БРИКС по вопросам развития ИКТ и обеспечения безопасности ИКТ-среды. В Декларации VI Саммита было отмечено, что, во-первых, ИКТ «должны служить инструментом поощрения устойчивого экономического прогресса и социальной интеграции». Во-вторых, «использование и развитие ИКТ на основе международного сотрудничества и общепризнанных норм и принципов международного права имеют первостепенное значение для обеспечения мирного, безопасного и открытого цифрового и интернет-пространства». В-третьих, «необходимо сохранять ИКТ, и, в частности, Интернет, как инструмент мира и развития и не допускать их использования в качестве оружия». Кроме того, в практическом плане страны обязались «сотрудничать друг с другом в выявлении возможностей для осуществления совместных действий по решению общих проблем безопасности в сфере использования ИКТ»[7]. Также было заявлено о создании группы экспертов стран БРИКС, которая будет заниматься выработкой практических предложений, касающихся основных областей сотрудничества, и будет координировать позиции на международных форумах. Направления работы группы более подробно раскрыты в итоговой декларации VII Саммита БРИКС (Уфа, Российская Федерация, 8–10 июля 2015 г.): «обмен информацией и передовой практикой в вопросах безопасности в сфере использования ИКТ; эффективная координация мер противодействия киберпреступности; выделение уполномоченных по связям в государствах-участниках; сотрудничество между странами БРИКС с использованием существующих групп реагирования на компьютерные инциденты в области компьютерной безопасности (CSIRT); совместные проекты в области НИОКР; укрепление потенциала; а также разработка международных норм, принципов и стандартов»[8]. Ввиду осуществлявшихся в тот момент активных попыток интернационализации управления интернетом, этим вопросам также было уделено особое внимание, и выработано общее понимание, что «интернет является международным ресурсом и что государства должны в равной степени участвовать в ее развитии и функционировании, принимая во внимание необходимость привлечения соответствующих заинтересованных сторон в определенном качестве и с определенными обязательствами». Страны БРИКС поддержали «развитие механизма управления интернетом… на основе открытого и демократического процесса, не подверженного влиянию решений, принятых в одностороннем порядке»[9].

2016 г. ознаменовался активными действиями против ИГИЛ[10] как на земле, так и в информационном пространстве, и Декларация VIII саммита БРИКС (Гоа, Индия, 15–16 октября 2016 г.) («Декларация Гоа») призвала все стра-

6 Национальный Комитет по исследованию БРИКС, «Форталезская декларация (принята по итогам шестого саммита БРИКС), г. Форталеза, Бразилия, 15 июля 2014 года», URL: https://nkibrics.ru/system/asset_docs/data/5486/a918/6272/6941/3e24/0000/original/VI_саммит БРИКС -_Форталезская декларация (г.Форталеза _Бразилия _15_июля 2014_года).doc?1418111256, п. 49.

7 Там же.

8 Национальный Комитет по исследованию БРИКС, VII саммит БРИКС, «Уфимская декларация (Уфа, Российская Федерация, 9 июля 2015 года)», URL: https://nkibrics.ru/system/asset_docs/data/559e/7a9a/6272/6943/081f/0000/original/VII_саммит БРИКС -_Уфимская декларация (г.Уфа _Россия _9_июля 2015_года).pdf?1436449434 С. 23.

9 Там. же, С. 21.

10 Прежнее название «Исламского государства», террористической группировки, запрещённой в России.

ны придерживаться всеобъемлющего подхода в борьбе с терроризмом, который должен включать «противодействие злоупотреблению террористическими структурами Интернетом, включая социальные сети, используя последние разработки в области ИКТ»[11].

С 2017 г. наметились значимые подвижки в плане развития практического сотрудничества. Так, в итоговой Декларации IX Саммита БРИКС (Сямэнь, КНР, 4–5 сентября 2017 г.) был отмечен прогресс, достигнутый Рабочей группой экспертов государств БРИКС по вопросам безопасности в сфере использования ИКТ; принято решение «развивать сотрудничество в соответствии с Дорожной картой практического сотрудничества БРИКС в обеспечении безопасности в сфере использования ИКТ и любыми другими согласованными механизмами»; подтверждено, что страны БРИКС «продолжат совместную работу при помощи существующего механизма в целях обеспечения безопасного, открытого, мирного и совместного использования ИКТ на основе равноправного участия международного сообщества в управлении им», а также отмечена инициатива Российской Федерации «о межправительственном соглашении БРИКС по сотрудничеству в вопросах безопасности в сфере использования ИКТ»[12].

В Йоханнесбургской декларации X Саммита БРИКС (Йоханнесбург, ЮАР, 25–27 июля 2018 г.) была подтверждена «важность разработки под эгидой ООН правил, норм и принципов ответственного поведения государств в информационном пространстве для обеспечения безопасности в сфере использования ИКТ»; подтверждена «важность международного сотрудничества в борьбе с использованием ИКТ в террористических и преступных целях» и «необходимость выработки под эгидой ООН универсального, юридически обязывающего нормативно-правового документа по противодействию использованию ИКТ в преступных целях»; признана «значимость создания правовых рамок для сотрудничества между участниками БРИКС в области обеспечения безопасности в сфере использования ИКТ». В этой связи государства объединения договорились продолжить работу по рассмотрению и разработке соответствующего межправительственного соглашения[13].

В Московской Декларации XII Саммита БРИКС[14] (состоялся 17 ноября 2020 г. в режиме видеоконференции) вновь содержались решения, способствующие укреплению МИБ. В Декларации акцентирована необходимость всеобъемлющего и сбалансированного подхода к развитию и обеспечению безопасности в сфере использования ИКТ, в том числе в контексте технического прогресса и развития бизнеса, обеспечения безопасности государств и защиты их интересов, а также уважения права на неприкосновенность частной жизни; была подчеркнута ведущая роль ООН в развитии диалога — без ущерба для деятельности других международных площадок — по достижению общего понимания в отношении безопасности ИКТ и их использования и разработки под эгидой ООН общепризнанных норм, правил и принципов ответственного поведения государств в сфере использования ИКТ; особо была отмечена важность международного права и принципов, применяемых в данной сфере, и приветствовалась деятельность Рабочей группы ООН открытого состава и Группы правительственных экспертов (ГПЭ) ООН по международной информационной безопасности. В Московской Декларации была также подчеркнута «важность формирования нормативно-правовой базы для сотрудничества стран БРИКС в обеспечении безопасности в сфере использования ИКТ»[15]

11 Национальный Комитет по исследованию БРИКС, «Декларация Гоа, 16 октября 2016 года», URL: https://nkibrics.ru/system/asset_docs/data/580f/3a55/6272/696e/9142/0000/original/VIII_саммит БРИКС -_Декларация Гоа (Гоа _Индия _16_октября 2016_года).docx?1477392981, п. 59.

12 Национальный Комитет по исследованию БРИКС, «Сямэньская декларация руководителей стран БРИКС, Сямэнь, Китай, 4 сентября 2017 года», URL: https://nkibrics.ru/system/asset_docs/data/5a4f/6bcb/6272/695d/471c/0000/original/IX саммит БРИКС -_Сямэньская декларация (г.Сямэнь _Китай _4_сентября 2017_года).doc?1515154379, пп. 54, 55.

13 Национальный Комитет по исследованию БРИКС, «Йоханнесбургская декларация Десятого саммита БРИКС, Йоханнесбург, ЮАР, 26 июля 2018 года», URL: https://nkibrics.ru/system/asset_docs/data/5b59/f0d6/6272/6905/341e/0000/original/X саммит БРИКС -_Йоханнесбургская декларация (г.Йоханнесбург _ЮАР _26_июля 2018_года).docx?1532621014, пп. 37, 38.

14 Национальный Комитет по исследованию БРИКС, «Московская декларация XII саммита БРИКС», URL: https://nkibrics.ru/system/asset_docs/data/6052/2d9c/6272/697e/b441/0000/original/XII_саммит БРИКС -_Московская декларация (г.Москва _Россия _17_ноября 2020_года).pdf?1615998364, п. 40.

15 Там же.

и отмечены усилия Рабочей группы экспертов (РГЭ) БРИКС по вопросам безопасности в сфере использования ИКТ»[16]. Также приветствовалось» создание центральными банками стран БРИКС специального Канала по информационной безопасности для осуществления обмена данными и опытом государств объединения в области противодействия киберугрозам в финансовой сфере»[17].

В Декларации XIII саммита БРИКС (9 сентября 2021 г., Нью-Дели[18]) вновь было подтверждена приверженность созданию открытой, безопасной, стабильной, доступной и мирной среды для использования ИКТ; отмечена необходимость всеобъемлющего и сбалансированного подхода к развитию и обеспечению безопасности в сфере использования ИКТ, в том числе в контексте технического прогресса и развития бизнеса, обеспечения безопасности государств и защиты их интересов, а также уважения права на неприкосновенность частной жизни.; подчеркнута ведущую роль ООН в развитии диалога — без ущерба для деятельности других профильных международных площадок — по достижению общего понимания в отношении безопасности ИКТ и их использования и разработки под эгидой ООН общепризнанных норм, правил и принципов ответственного поведения государств в сфере использования ИКТ. В Декларации приветствовалось успешное завершение работы Рабочей группы ООН открытого состава (РГОС) и Группы правительственных экспертов (ГПЭ) по международной информационной безопасности, а также запуск новой РГОС по вопросам безопасности в сфере использования ИКТ и самих ИКТ 2021–2025. Среди прочего, в этом документе отмечена публикация «Электронного справочника регуляторных актов стран БРИКС в сфере информационной безопасности и Сборника лучших практик по надзору и контролю за рисками информационной безопасности, рассматривая их в качестве комплексных документов, содержащих правила и передовые практики, используемые в рамках специального Канала БРИКС по информационной безопасности»[19].

Сегодня проблематика МИБ неизменно стоит в повестке дня заседаний с участием глав государств-членов БРИКС и регулярно находит отражение в итоговых документах саммитов объединения. Также успешно продолжается формирование общих позиций и по новым вопросам, связанным с использованием ИКТ. Так, XIV Саммит БРИКС (Пекин, КНР, 23–24 июня 2022 г.) сформировал позицию по вопросам, связанным с искусственным интеллектом (ИИ). В Пекинской декларации было отмечено, что «прорывы в применении цифровых технологий таких как, например, большие данные и искусственный интеллект, могут играть важную роль в обеспечении устойчивого развития»[20]. В декларации подчеркнута «необходимость сотрудничества в интересах укрепления доверия и безопасности, а также прозрачности и подотчетности в развитии надежного ИИ, чтобы максимально использовать его потенциал во благо общества и человечества в целом, с особым акцентом на маргинализированные и уязвимые группы населения»[21]. Отмечено, что нужно работать над устранением озабоченностей, связанных с рисками и этическими дилеммами, «обмениваться передовым опытом, проводить сравнительные исследования по этому вопросу для разработки общего подхода к управлению, которое будет служить руководством для стран БРИКС в отношении этического и ответственного использования искусственного интеллекта, способствуя развитию технологий ИИ»[22].

В 2023 г., на XV саммите БРИКС (Йоханнесбург, ЮАР, 22–24 августа 2023 г.) Председатель КНР Си Цзиньпин заявил, что «Искусственный интеллект — это новая область человеческого развития, которая может при-

16 Там же.

17 Там же, п. 63.

18 Национальный Комитет по исследованию БРИКС, «Декларация XIII саммита БРИКС — Нью-Дели», URL: https://nkibrics.ru/system/asset_docs/data/6148/6c7a/6272/6906/7842/0000/original/Декларация_Нью-Дели.pdf?1632136314.

19 Там же, п. 60.

20 Национальный Комитет по исследованию БРИКС, «Декларация XIV саммита БРИКС — Пекин», URL: https://nkibrics.ru/system/asset_docs/data/635a/6df2/6272/6945/fa54/0000/original/XIV_саммит БРИКС -_Пекинская декларация (г._Пекин _Китай _23_июня 2022_года).pdf?1666870770, п. 57.

21 Там же.

22 Там же.

нести большие возможности, но и риски и вызовы»[23]. Он также сказал, что «[необходимо] продолжить расширять сотрудничество в области искусственного интеллекта, усилить обмен информацией и техническое сотрудничество, совместно работать по предотвращению рисков, на основе широкого консенсуса сформировать структуру управления искусственным интеллектом и стандартов»[24].

В декларации саммита[25] вновь была подтверждена приверженность созданию открытой, безопасной, стабильной, доступной и мирной среды, подчеркнута важность достижения общего понимания и активизации сотрудничества в использовании ИКТ и Интернета. Саммит поддержал ведущую роль ООН в развитии конструктивного диалога по теме обеспечения безопасности ИКТ, в том числе в рамках Рабочей группы ООН открытого состава по вопросам безопасности в сфере использования ИКТ и самих ИКТ в 2021–2025 гг., а также разработке общепризнанных нормативно-правовых рамок в этой области. Положения Декларации подтверждают последовательность БРИКС в стремлении к всеобъемлющему, сбалансированному и объективному подходу к разработке и обеспечению безопасности продуктов и систем ИКТ. XV саммит вновь обозначил необходимость развития практического сотрудничества в рамках БРИКС посредством осуществления «дорожной карты» практического сотрудничества БРИКС в обеспечении безопасности в сфере использования ИКТ и в рамках деятельности Рабочей группы БРИКС по вопросам безопасности в сфере использования ИКТ»[26].

Положения Декларации в части, касающейся использования ИКТ (как и декларации предыдущих саммитов БРИКС), показывают общность подходов государств-участников объединения к выбору механизмов и средств противодействия глобальным вызовам и угрозам, возникающих при использовании ИКТ, обеспечению безопасности и стабильности глобальной цифровой среды, и это способствует формированию и укреплению системы МИБ.

Объединение БРИКС растет и развивается, организация готова к расширению и принятию новых постоянных стран-участников. В Декларацию XV саммита 2023 г. включено положение пригласить Аргентинскую Республику, Арабскую Республику Египет, Исламскую Республику Иран, Объединенные Арабские Эмираты, Королевство Саудовская Аравия и Федеративную Демократическую Республику Эфиопия стать полноформатными членами БРИКС с 1 января 2024 г.

Мир стоит на пороге перемен, и выработка общей позиции на основе инклюзивности, уважения суверенитета и национальных особенностей государств очень важна. В отличие от ГПЭ, в работе РГОС принимает участие гораздо большее число государств, в том числе тех, для которых проблематика МИБ становится актуальной. Вероятно, что эти страны изучат множество мнений и точек зрения и примут решения, способствующие объективному решению проблем информационной/кибербезопасности как на региональном, так и глобальном уровнях. Чем более четко и осмысленно будет звучать позиция БРИКС — как альтернатива гегемонии, тем большее число стран присоединятся к ней.

БРИКС — это больше, чем простая сумма частей. И каждому члену объединения есть что предложить. Синергия научно-образовательного, финансового и промышленного потенциала стран-участников БРИКС, при сохранении общих подходов к решению вопросов по МИБ, может в значительной степени стать драйвером преодоления существующих и новых вызовов — от проблем цифрового разрыва и достижения и поддержания технологического суверенитета до рисков, сопровождающих внедрение технологий искусственного интеллекта.

23 РИА Новости, «Си Цзиньпин призвал БРИКС сформировать общую структуру управления ИИ», URL: https://ria.ru/20230823/tszinpin-1891759909.html.

24 Там же.

25 Президент России, «XV саммит БРИКС, Йоханнесбургская декларация-II, БРИКС и Африка: партнерство в интересах совместного ускоренного роста, устойчивого развития и инклюзивной многосторонности, Сэндтон, Гаутенг, ЮАР, 23 августа 2023 года», URL: http://static.kremlin.ru/media/events/files/ru/ls471x8ogLBhjRQx05ufVB2uzMFo1kWs.pdf.

26 Там же, п. 24.

В.А. Романовский
Главный советник управления внешней политики БИСИ

О НАПРАВЛЕНИЯХ РЕГИОНАЛЬНОГО СОТРУДНИЧЕСТВА ПО ОБЕСПЕЧЕНИЮ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1. В условиях возрастания глобальной военно-политической напряженности и углубления кризисных явлений в мировой экономике повышается значимость заинтересованного межгосударственного взаимодействия, которое становится одним из ключевых условий для обеспечения собственной безопасности любого государства.
2. На сегодняшний день ИКТ-среда является международным пространством, в котором государства взаимодействуют друг с другом напрямую. Особенную актуальность приобретают направления сотрудничества по обеспечению безопасности и интересов личности, общества и государства в ИКТ-среде, в частности, региональное межгосударственное взаимодействие в целях выработки общего понимания масштабов угроз в ИКТ-среде в отношении отдельного региона и возможных методов противодействия им со стороны соответствующих сил обеспечения информационной безопасности.
3. Безусловно, важным направлением регионального сотрудничества являются вопросы применения норм ответственного поведения государств в ИКТ-среде. Так, проблематика делимитации и демаркации границ зон ответственного поведения государств в ИКТ-среде приобретает особую значимость в условиях продолжающегося осмысления теоретико-правовой природы концепции «технологический суверенитет».
4. Существенно повысилась значимость измерения информационной безопасности в профильных направлениях деятельности региональных межгосударственных объединений. Представляется, что развитие взаимодействия государств в сфере информационной безопасности в рамках межгосударственных объединений в среднесрочной перспективе будет в большей степени зависеть от направления и характера трансформации самих объединений. Вместе тем необходимо обратить внимание, что эффективность реализации стратегий по обеспечению экономической безопасности и технологического развития в рамках региональных международных организаций и интеграционных структур будет, в том числе, зависеть от динамики межгосударственного взаимодействия в сфере информационной безопасности.
5. Представляется своевременным обратить внимание на вопрос правового обеспечения управления трансграничными потоками данных. В рамках региональных интеграционных объединений необходимостью становится правовое регулирование доступа к хранилищам данных, использование которых в национальном сегменте ИКТ напрямую связано с проблематикой защиты персональных данных.
6. Цифровизация изменяет формы и направления своего развития в географических и политических регионах, что проявляется в возможности появления региональных цифровых платформ. Вместе с тем их широкое распространение приводит к размыванию границ между ними и социальными инфраструктурами. Платформы становятся новой социальной инфраструктурой и одновременно обретают черты регулятора общественных отношений. Этот фактор необходимо учитывать при развитии правового регулирования цифровых платформенных решений в рамках региональных интеграционных объединений.
7. В условиях стратегического характера вопроса обеспечения технологического суверенитета закономерно повышается значимость стандартов и других технических нормативных правовых актов. С учетом перспекти-

вы формирования и развития региональных межгосударственных цифровых платформ открытым остается вопрос о процедурах составления и внедрения актов, которые относятся к области технического нормирования и стандартизации и соотношения этих процедур с законодательством в сфере информационной безопасности.

8. В условиях, когда стратегическим приоритетом для государства является внедрение передовых информационно-коммуникационных и производственных технологий в отрасли национальной экономики и сферы общественной жизни, важным направлением сотрудничества профильных государственных структур и научного сообщества стран отдельного региона становится развитие и применение технологий искусственного интеллекта. Представляется, что большая юридическая определенность сферы развития и применения технологий искусственного интеллекта в рамках региональных межгосударственных объединений создаст условия как для эффективной реализации задач технологической политики, так и разработки комплекса мер, направленных на противодействие широкому спектру угроз безопасности, в том числе информационно-психологического характера.

Таким образом, совершенствование механизма участия представителей научного и экспертного сообщества в научно-исследовательском и аналитическом обеспечении подготовки и продвижения совместных инициатив по формированию системы обеспечения международной информационной безопасности видится особенно актуальным с учетом **закономерного повышения значимости регионального сотрудничества** в сфере информационной безопасности.

СБОРНИК ДОКЛАДОВ УЧАСТНИКОВ XVII МЕЖДУНАРОДНОГО ФОРУМА «ПАРТНЕРСТВО ГОСУДАРСТВА, БИЗНЕСА И ГРАЖДАНСКОГО ОБЩЕСТВА ПРИ ОБЕСПЕЧЕНИИ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

Подписано в печать 28.11.2023. Гарнитура Helios.
Формат 60x84/8. Объем 28,37 усл. печ. л.
Тираж 200 экз.

www.namib.online
info@namib.online