БЮЛЛЕТЕНЬ
II МЕЖДУНАРОДНОЙ МОЛОДЕЖНОЙ КОНФЕРЕНЦИИ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

24 октября 2024 г.
(сборник тезисов)

Москва
2025

УДК 004, 327, 339, 341, 342
ББК 3, 65, 66, 67
ISBN-978-5-6052665-5-6

Научный руководитель:
Карпович Олег Геннадьевич
заслуженный деятель науки Российской Федерации, доктор юридических наук, доктор политических наук, профессор, и.о. проректора по экспертно-аналитической работе – руководитель Института актуальных международных проблем, заведующий кафедрой стратегических коммуникаций и государственного управления Дипломатической академии МИД России

Ответственные редакторы:
Мартиросян Аревик Жораевна *– кандидат юридических наук, мл.научный сотрудник Института актуальных международных проблем, старший преподаватель кафедры стратегических коммуникаций и государственного управления Дипломатической академии МИД России, член Российской Ассоциации международного права и Молодежного совета Координационного центра доменов.RU/.РФ*
Шангараев Руслан Насимович *– доктор политических наук, кандидат экономических наук, доцент, профессор кафедры стратегических коммуникаций и государственного управления Дипломатической академии МИД России, профессор Академии военных наук, главный редактор журнала «Вестник ученых-международников»*

Бюллетень II Международной молодежной конференции по информационной безопасности (сборник тезисов) / отв. ред. А.Ж. Мартиросян, Р.Н. Шангараев; Дипломатическая академия МИД России. – М., 2025. – 330 с.

Бюллетень отражает взгляды молодых ученых на проблематику информационно-коммуникационных технологий в контексте развития современных международных отношений, мировой экономики и международного права. Издание может использоваться в учебном процессе (в учебных организациях высшего образования, где изучают проблемы информационной безопасности), а также учеными, политиками, дипломатами, политологами и другими специалистами в их информационно-аналитической и иной работе.

Мнение авторов может не совпадать с мнением редакции. Редакция не несёт ответственности за высказанные авторами публикаций точки зрения на происходящие в России и в мире политические процессы, события, явления. При использовании материалов ссылка обязательна.

ISBN- 978-5-6052665-5-6

СОДЕРЖАНИЕ

[1] Организована совместно с Молодежным советом Координационного центра доменов .RU/.РФ

ПРОГРАММА
II МЕЖДУНАРОДНОЙ МОЛОДЕЖНОЙ КОНФЕРЕНЦИИ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

<table>
<tr><td colspan="2">9:30-10:00

РЕГИСТРАЦИЯ</td></tr>
<tr><td colspan="2">10:00 – 10:10 | Ауд.4

ОТКРЫТИЕ КОНФЕРЕНЦИИ</td></tr>
<tr><td colspan="2">10:10 – 11:10 | Ауд.4

Секция 1 «Цифровая дипломатия: от истории к практике»</td></tr>
<tr><td>11:10 – 13:30 | Ауд.4

Секция 2 «Технологии и методы обеспечения информационной безопасности»</td><td>11:10-13:30 | Ауд.5

Секция 3 «Актуальные проблемы информационной безопасности в контексте международного права»</td></tr>
<tr><td colspan="2">13:30-14:30 – кофе-брейк</td></tr>
<tr><td>14:30 –16:00 | Ауд.4

Секция 4 «Информационная безопасность и общество»</td><td rowspan="2">14:30 – 17:10 | Ауд.5

Секция 5 «Фактор искусственного интеллекта
в международных отношениях
и мировой экономике:
между мифом и реальностью»</td></tr>
<tr><td>16:00 – 17:40 | Ауд. 4

Секция 6 «Глобальные аспекты информационной безопасности»</td></tr>
<tr><td colspan="2">17:40 – 18:40 | Ауд. 4

Секция 7 «Цифровое пространство как точка пересечения политики и технологий» организована совместно с Молодежным советом Координационного центра доменов .RU/.РФ</td></tr>
<tr><td colspan="2">18:40 – фуршет</td></tr>
</table>

ПОРЯДОК РАБОТЫ СЕКЦИЙ

Аудитория 4

10:10 – 11:10
Секция 1
«Цифровая дипломатия: от истории к практике»

Модератор(ы) секции:

Мартиросян Аревик Жораевна, научный сотрудник ИАМП ДА МИД России, руководитель Школы МИБ;

Соловьев Никита Евгеньевич, член Исполнительной дирекции Школы МИБ ИАМП Дипломатической академии МИД России, член Молодёжного совета Координационного центра доменов .RU/.РФ,

1. Буканов Е.К. Цифровая дипломатия и информационно-коммуникационные технологии как движущая сила трансформации здравоохранения в рамках Евразийского экономического союза. ДонГМУ Минздрава России.
2. Голубева Т.Э. Публичная дипломатия Web 2.0 США. Генезис «Цифровой дипломатии»: опыт США. ДА МИД России.
3. Пьянникова Д.Е. Цифровая дипломатия как инструмент «мягкой силы» на примере Индии и России. Уральский федеральный университет.
4. Ракова Е.Д. Цифровая публичная дипломатия между Российской Федерацией и Исламской Республикой Иран. Международная академия бизнеса и управления.
5. Рудницкая В.А., Фадина Я.С. Цифровая дипломатия и трансформация международных отношений в условиях информационной конкуренции США и Китая. СПбГУ.
6. Чумаков В.А. Цифровая дипломатия против цифрового разрыва: вклад российского гражданского общества. ФКУ «Аппарат Общественной палаты России».

Аудитория 4

11:10 – 13:30

Секция 2

«Технологии и методы обеспечения информационной безопасности»

Модератор(ы) секции:

Мартиросян Аревик Жораевна, научный сотрудник ИАМП ДА МИД России, руководитель Школы МИБ.

1. Акчурина Д.Х. Актуальность оценки рисков информационной безопасности автоматизированных систем управления технологических процессов критически важных объектов. РГУ нефти и газа (НИУ) имени И.М. Губкина.
2. Близнякова С.С. К 75-летию российско-китайских дипломатических отношений. Российско-китайское сотрудничество по линии министерств внутренних дел в области обеспечения международной информационной безопасности. СПбГУ, Управление по борьбе с противоправным использованием информационно-коммуникационных технологий Главного управления Министерства внутренних дел Российской Федерации по г. Санкт-Петербургу и Ленинградской области.
3. Гараева А.Н. Технологии и методы обеспечения информационной безопасности в Российской Федерации. Нижегородский государственный лингвистический университет им. Н.А.Добролюбова.
4. Громова М.Б. Обеспечение справедливого доступа к программам информационной безопасности. ДА МИД России.
5. Коннова К.Д., Эпштейн В.А., Основные подходы к обеспечению информационной безопасности на примере США, ЕС, РФ и КНР. МГИМО (У) МИД России, ИБДА РАНХиГС при Президенте Российской Федерации.
6. Корних Е.М. Deepfakes как угроза информационной безопасности. РАНХиГС при Президенте Российской Федерации.
7. Крылов Д.С. Технологии рефлексивного управления в современных геополитических процессах на Ближнем Востоке. ИНИОН РАН.
8. Мельник С.В., Петрова Е.П. ИКТ в современном мире. Цифровая глобализация. Роль и значения МСЭ. Международная академия связи, ООО «НТЦ КОМТЕСТ». ООО «Испытательный центр документальной электросвязи».
9. Моисеева О.В. Сравнение основных тенденций в развитии систем обеспечения информационной безопасности в России и Китае. МГУ им. М.В. Ломоносова.

10. Ордин А.В. Программно-определяемые глобальные сети SD-WAN: элемент комплексной кибербезопасности для государств-членов ЕАЭС. ДА МИД России.

11. Оришак А.В. Цифровизация и диверсификация платежных инструментов как одна из опор экономической безопасности. ДА МИД России.

12. Пилюгина Д.А. Путь России к суверенному Интернету. ДА МИД России.

13. Пичугин Н.В. 6-уровневая партийно-государственная система управления обеспечения информационной безопасности КНР. ИКСА РАН, Исполнительная дирекция Школы МИБ.

14. Семедов С.А. Цифровые технологии в современных международных отношениях. РАНХиГС при Президенте Российской Федерации.

Аудитория 5

11:10 – 13:30

Секция 3
«Актуальные проблемы информационной безопасности в контексте международного права»

Модератор(ы) секции:

Анисимов Игорь Олегович, декан Юридического факультета, кандидат юридических наук, арбитр Арбитражного центра при РСПП, куратор Клуба международного права ДА МИД России.

1. Анисимов И.О., Ястребова А.Ю. Право на информацию в контексте осуществления международной миграции. ДА МИД России.
2. Волостных Д.Ю. Преследование (сталкинг) в сети Интернет: характеристика и проблемы противодействия. РАНХиГС при Президенте Российской Федерации.
3. Головач П.Н., Емельянович О.В. О правовом регулировании информационной безопасности Республики Беларусь в контексте обеспечения международной безопасности. Белорусский государственный университет.
4. Иванов Е.О. Подходы ведущих государств Латинской Америки к вопросу применимости международного гуманитарного права в цифровой среде. МГИМО (У) МИД России.
5. Клименко А.В. Правовые аспекты обеспечения информационной безопасности в Королевстве Таиланд.
6. Лопатёнков А.А. Искусственный интеллект и его роль в сохранении всемирного культурного и природного наследия. ГБУК г. Москвы «ГМЗ "Царицыно"».
7. Минаева Е.В. Полицентричный мир: реализация в медиапространстве социальных сетей принципа запрета осуществления прав и свобод человека вопреки правам и свободам других лиц. АНО ВО «Международная академия бизнеса и управления».
8. Насонова П.С. Правовое обеспечение международной информационной безопасности: проблемы и перспективы развития. Уральский государственный юридический университет им. В.Ф. Яковлева.
9. Нечаева Ю.С. Основные концепции определения правосубъектности искусственного интеллекта в отношении объектов интеллектуальной собственности. ДА МИД России.
10. Оганесян Т.Д. Национальная безопасность и защита данных: обновленные стандарты европейского правосудия. ДА МИД России.

11. Орешеч А.В. Особенности соблюдения и защиты цифровых прав граждан. Аппарат Уполномоченного по правам человека в Брянской области, Брянский филиал РАНХиГС при Президенте Российской Федерации.

12. Рустамов Ф.Ф. Краткий обзор международно-правового регулирования морских перевозок грузов. ДА МИД России.

13. Савельева Н.В. Возможности распространения положений Конвенции ООН против киберпреступности на системы космической связи и дистанционного зондирования земли из космоса. ИФЗ РАН.

14. Сигаури-Горский Е.Р. Политико-правовые проблемы сотрудничества государств АСЕАН в контексте территориального спора в Южно-Китайском море. Институт Китая и современной Азии РАН.

15. Сушков С.П. Вменение государству использования информационно-коммуникационных технологий частными лицами. НИУ ВШЭ.

16. Тян-Юшан Т.Л. Правовое регулирование беспилотных транспортных средств в России и в Зарубежных странах. ПФ РГУП.

17. Фролова Н.А. Вопросы кибербезопасности в контексте конвенционного механизма противодействия наркопреступности. Российский Новый университет.

18. Штанова А.А. Нейробезопасность как новое направление в международном праве. МГИМО (У) МИД России.

Аудитория 4

14:30 – 16:00

Секция 4
«Информационная безопасность и общество»

Модератор(ы) секции:
Мартиросян Аревик Жораевна, научный сотрудник ИАМП ДА МИД России, руководитель Школы МИБ.

1. Ветрова П.А. Обеспечение информационной безопасности коммерческой организации. ДА МИД России.
2. Дейкало С.С. О межгосударственных медиахолдингах в контексте информационной безопасности. Гродненский государственный университет им. Янки Купалы.
3. Зогранян Е.В. Латентные сетевые общности или колонизация будущего. РАНХиГС при Президенте Российской Федерации.
4. Красилова Е.П. Вербовка в экстремистские и террористические организации посредством социальных сетей и мессенджеров. РАНХиГС при Президенте Российской Федерации.
5. Минаева Е.В. Меры преодоления негативного влияния электронных средств массовой информации на правосознание молодежи. АНО ВО «Международная академия бизнеса и управления».
6. Ниточкин Ф.В. Фейки о выборах как угроза национальной безопасности. МГЮА, ФКУ «Аппарат Общественной палаты России».
7. Парфенова М.С. Деструктивные суицидальные сообщества в сети Интернет: характеристика и методы противодействия. РАНХиГС при Президенте Российской Федерации.
8. Чих И.Н. Роль некоммерческих организаций в обеспечении информационной безопасности Российской Федерации на примере Русского географического общества. НИУ ВШЭ.

Аудитория 5

14:30 – 17:10

Секция 5
«Фактор искусственного интеллекта в международных отношениях и мировой экономике: между мифом и реальностью»

Модератор(ы) секции:

Виноградова Екатерина Алексеевна, кандидат политических наук, директор Научно-исследовательского центра: технологии искусственного интеллекта в международных отношениях;

Соловьев Никита Евгеньевич, член Исполнительной дирекции Школы МИБ ИАМП Дипломатической академии МИД России, член Молодёжного совета Координационного центра доменов .RU/.РФ.

1. Аствацатуров А.А. Как искусственный интеллект изменил стратегические наступательные вооружения в США (на примере развития интегрированной системы сдерживания). Южный федеральный университет.
2. Багаутдинова А.Р. Использование машинного обучения для идентификации фейковых новостей. Северо-Кавказский федеральный университет.
3. Васильева А.А. Международно-правовые аспекты развития и применения искусственного интеллекта. РАНХиГС при Президенте Российской Федерации.
4. Виноградова Е.А. Несанкционированное использование политических дипфейков в международной практике. Научно-исследовательский центр: технологии искусственного интеллекта в международных отношениях.
5. Вохминцев И.В. Государства БРИКС+: оценка возможностей в сфере ИИ. НИУ ВШЭ.
6. Гринченко А.Н. Влияние искусственного интеллекта на международно-правовую защиту культурных ценностей Российской Федерации в странах Балтии. Псковский государственный университет.
7. Де Апро С.В. Стандартизация в сфере ИИ как «кредит доверия» на международном уровне. МГУ им. М.В.Ломоносова.
8. Журих А.Н. Искусственный интеллект. Перспективы и угрозы в области международных отношений. РГСУ.
9. Власова К.В., Мухачева В.А. От мифа к манипуляции: искусственный интеллект и проблема распространения дезинформации в глобальной политике. Вятский государственный университет.

10. Мартиросян А.Ж. Международное регулирование ИИ: основные итоги и тенденции 2024 г. ДА МИД России.

11. Нечаева В.С. Искусственный интеллект сквозь призму теории международных отношений. Иркутский государственный университет.

12. Обидов М.М. Этические и правовые вызовы, связанные с искусственным интеллектом. ДА МИД России.

13. Олифиренко А.А. Data Poisoning: новые горизонты угроз для моделей машинного обучения и стратегии противодействия. СГТУ.

14. Прошина В.И. Искусственный интеллект в военной среде и разведке США. СПбГУ.

15. Степовая Д.А. Влияние ИИ на достижение ЦУР. МГУ им. М.В.Ломоносова.

16. Стучкайте М.В. Искусственный интеллект – будущий актор международных отношений? Северо-Кавказский федеральный университет.

17. Храповицкая Е.Д. Влияние искусственного интеллекта на экологический аспект мировой экономики. Донецкий государственный университет.

Аудитория 4

16:00 – 17:40

Секция 6
«Глобальные аспекты информационной безопасности»

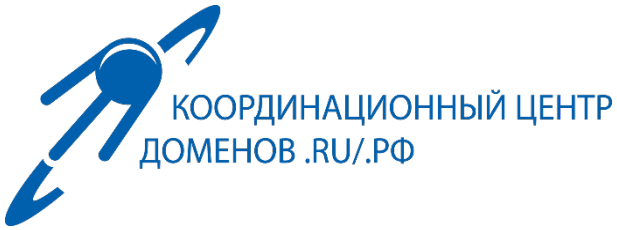
Модератор(ы) секции:

Мартиросян Аревик Жораевна, научный сотрудник ИАМП ДА МИД России, руководитель Школы МИБ;

Моисеева Марина Владиславовна, студент МГУ им. М.В. Ломоносова, член Исполнительной дирекции Школы МИБ ИАМП Дипломатической академии МИД России, член Молодёжного совета Координационного центра доменов .RU/.РФ.

1. Бурнакина А.В. Роль торговых переговоров в рамках ВТО в преодолении цифрового неравенства. НИУ ВШЭ.
2. Варламова А.Е. Сотрудничество России и АСЕАН в области информационной безопасности. Сравнение российского и китайского подходов. МГУ им. М.В. Ломоносова.
3. Гайнанов Р.Р. Международное измерение информационной безопасности. Ситуация в Турции и возможности России.
4. Гуляева Е.Е. Правовые основы обеспечения кибербезопасности в странах БРИКС. ДА МИД России.
5. Жбанов А.М. Тенденции политики ключевых акторов международной системы в области информационной безопасности и регулирования интернета. МГУ им. М.В. Ломоносова.
6. Жерлицына А.О. Кибербезопасность в повестке стран–участниц Организации Договора о коллективной безопасности. Сибирский федеральный университет.
7. Карасев П.А. Управление Интернетом в контексте Глобального цифрового договора. ИМЭМО РАН.
8. Кучина А.М. Цифровая солидарность и цифровой суверенитет в контексте развития международной информационной безопасности. ДА МИД России.
9. Меликсетян А.Г. Цифровизация рынка труда ЕАЭС. ДА МИД России.
10. Стрелкова М.В. Роль России в области международного сотрудничества по обеспечению информационной безопасности. Военный университет им. князя Александра Невского.
11. Щербань А.В. Формирование политики информационной безопасности в рамках ОДКБ. СПбГУ.

Аудитория 4



17:40 – 18:40

Секция 7
«Цифровое пространство как точка пересечения политики и технологий» организована совместно с Молодежным советом Координационного центра доменов .RU/.РФ

Модератор(ы) секции:

Алейников Андрей Алексеевич, председатель Молодёжного совета Координационного центра доменов .RU/.РФ, аспирант Российской государственной академии интеллектуальной собственности

1. Игнатов А.А. Политика управления данными новых стран-членов БРИКС и перспективы многостороннего сотрудничества в рамках объединения. ЦИМИ ИПЭИ РАНХиГС при Президенте Российской Федерации, Молодёжный совет Координационного центра доменов .RU/.РФ.
2. Мальцева Д.А., Стребкова К.Е. Практики использования нейросетей для анализа угроз и рисков для молодежи в цифровом пространстве: опыт США. СПбГУ, Молодёжный совет Координационного центра доменов .RU/.РФ.
3. Моисеева М.В. Информационная безопасность в современной повестке БРИКС. МГУ им. М.В. Ломоносова, Молодёжный совет Координационного центра доменов .RU/.РФ, Исполнительная дирекция Школы МИБ.
4. Соловьев Н.Е. Эксплуатация уязвимостей генеративных моделей искусственного интеллекта в контексте генерации вредоносного контента. Молодежный совет Координационного центр доменов .RU/.РФ, Исполнительная дирекция Школы МИБ.
5. Тюлякова С.А. Суверенитет данных как фактор формирования цифрового суверенитета государств. Молодёжный совет Координационного центра доменов .RU/.РФ.
6. Тюмин С.Г. Развитие онлайн-образования в российском интернет-сегменте. МТУСИ, Молодёжный совет Координационного центра доменов .RU/.РФ.

ТЕЗИСЫ ДОКЛАДОВ УЧАСТНИКОВ

II МЕЖДУНАРОДНОЙ МОЛОДЕЖНОЙ КОНФЕРЕНЦИИ

ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

24 ОКТЯБРЯ 2024 Г.

СЕКЦИЯ 1

«ЦИФРОВАЯ ДИПЛОМАТИЯ: ОТ ИСТОРИИ К ПРАКТИКЕ»

Евгений Кириллович Буканов,
Преподаватель, кафедра медицинской физики,
математики и информатики,
ДонГМУ Минздрава России,
E-mail: evgeni.bukaniv@yandex.ru

Evgeni K.Bukanov,
Lecturer, Department of Medical Physics,
Mathematics and Computer Science,
Donetsk State Medical University named after M. Gorky
of the Ministry of Health of the Russian Federation,
E-mail: evgeni.bukaniv@yandex.ru

ЦИФРОВАЯ ДИПЛОМАТИЯ И ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ КАК ДВИЖУЩАЯ СИЛА ТРАНСФОРМАЦИИ ЗДРАВООХРАНЕНИЯ В РАМКАХ ЕВРАЗИЙСКОГО ЭКОНОМИЧЕСКОГО СОЮЗА

DIGITAL DIPLOMACY AND INFORMATION AND COMMUNICATION TECHNOLOGIES AS A DRIVING FORCE OF HEALTHCARE TRANSFORMATION WITHIN THE EURASIAN ECONOMIC UNION

Аннотация. В работе исследуется значение цифровой дипломатии и информационно-коммуникационных технологий (ИКТ) для эффективной трансформации здравоохранения в Евразийском экономическом союзе (ЕАЭС). Цифровая дипломатия – это один из стратегических инструментов, благодаря которому осуществляется координация и стандартизация ключевых медицинских процессов, что в итоге приводит к улучшению качества медицинских услуг в странах-участницах ЕАЭС. Осуществление процессов по внедрению передовых ИКТ, таких как смарт-контракты, децентрализированные системы управления базами данных, дистанционный мониторинг, телемедицинские сервисы, системы обмена данными и удалённого взаимодействия, повышает эффективность медицинской помощи и ведёт к сокращению бюрократических процедур. В данной работе приведена статистика и успешные примеры внедрения ИКТ в рамках ЕАЭС, что

подтверждает актуальность и перспективность этих технологий для улучшения медицинского обслуживания и укрепления сотрудничества между странами.

Ключевые слова: ЕАЭС, здравоохранение, цифровая дипломатия, информационно-коммуникационные технологии.

Abstract. The paper explores the importance of digital diplomacy and information and communication technologies for effective transformation of healthcare in the Eurasian Economic Union (EAEU). Digital diplomacy is one of the strategic tools through which the coordination and standardization of key medical processes is carried out, which ultimately leads to the improvement of the quality of medical services in the EAEU member states. Implementation of advanced ICT processes, such as smart contracts, decentralized database management systems, remote monitoring, telemedicine services, data exchange and remote interaction systems, increases the efficiency of medical care and leads to the reduction of bureaucratic procedures. This paper presents statistics and successful examples of ICT implementation within the EAEU, which confirms the relevance and prospects of these technologies for improving medical care and strengthening cooperation between the countries.

Keywords: Eurasian Economic Union, healthcare, digital diplomacy, information and communication technologies.

Цифровая дипломатия и реализация инициатив по внедрению ИКТ представляют собой глобальные катализаторы для преобразования здравоохранения в странах-участницах ЕАЭС. В условиях интеграционных процессов цифровая дипломатия является ключевым инструментом для установления единых требований и стандартов, обмена накопленным опытом и создания единой интегрированной инфраструктуры здравоохранения. По данным Всемирной организации здравоохранения, переход к цифровой медицине оказывает значительное влияние на развитие здравоохранения в странах ЕАЭС [1]. Этому способствуют такие факторы, как повышение доступности ИКТ, государственная поддержка и программы модернизации,

а также интеграция цифровых решений [2]. Эти факторы формируют прочную основу для развития цифровых технологий в здравоохранении и стимулируют сотрудничество между государствами-членами, направленное на создание единого медицинского пространства [3].

В рамках этих изменений особое внимание стоит уделить развитию сервисов телемедицинских консультаций, которые с 2020 по 2023 год выросли на 82% [4]. Аналогичные процессы наблюдаются в Республике Казахстан, где 20% всех медицинских обращений проводилось в дистанционном формате, что значительно снизило нагрузку на клиники и улучшило доступ к медицинским услугам в отдалённых регионах [5].

По данным отчёта Евразийской экономической комиссии, к 2023 году 70% лечебных учреждений России и Белоруссии перешли на использование электронных медицинских сервисов. Это позволило сократить время на обработку медицинских данных внутри больниц, а также создать эффективные цифровые массивы для обмена данными и координации с министерствами и ведомствами. К 2025 году этот показатель должен достичь 90% на территории всех стран-участниц ЕАЭС [5-6].

Внедрение ИКТ и создание единого цифрового контура решают задачи, связанные с повышением квалификации медицинских работников, выработкой единых требований для аттестации и кооперации.

Заключение. Цифровая дипломатия и внедрение передовых ИКТ в здравоохранение стран-участниц ЕАЭС являются ключевыми направлениями, которые способствуют повышению эффективности медицинского обслуживания, улучшению взаимодействия между странами и созданию единого медицинского пространства. Эти процессы ускоряют внедрение инновационных решений, таких как телемедицина и электронные медицинские сервисы, что, в свою очередь, значительно повышает доступность и качество медицинской помощи.

Список источников и литературы:

1. WHO-ITU global standard for accessibility of telehealth services [Электронный ресурс] // Consolidated telemedicine implementation guide URL: https://www.who.int/publications/i/item/9789240059184 (дата обращения: 10.10.2024).

2. Еременко, М. Ю. Цифровизация как драйвер экономической интеграции стран Евразийского экономического союза / М. Ю. Еременко // Вестник университета. – 2021. – No 3. – С. 32-37. – DOI 10.26425/1816-4277-2021-3-32-37. – EDN JVAVAY.

3. Базлуцкая М.М., Зиновьева Е.С. Особенности цифровой публичной дипломатии международных организаций. Аналитический обзор коллективной монографии «Цифровая дипломатия международных организаций. Автономность, легитимность и конкуренция» под редакцией Р. Зайотти и К. Бйолы // Вестник международных организаций. 2022. Т. 17. No 1. С. 183–190 (на русском языке). doi:10.17323/1996-7845-2022-01-09.

4. Кобякова О.С., Кадыров Ф.Н. Проблемы развития телемедицинских технологий в России сквозь призму зарубежного опыта. Национальное здравоохранение. 2021;2(2):13-20. https://doi.org/10.47093/2713-069X.2021.2.2.13-20.

5. Основные приоритеты развития цифровой экономики в ЕАЭС [Электронный ресурс]. – Режим доступа: https://digital. ac.gov.ru/news/4254/?sphrase_id=4261 (дата обращения: 25.01.2021).

6. Основные направления реализации цифровой повестки Евразийского экономического союза до 2025 г., утверждены решением Высшего ЕЭС от 11.10.2017 No 12 [Электронный ресурс]. – Режим доступа: http://www.eurasiancommission.org/ru/act/dmi/workgroup/Pages/default.aspx (дата обращения: 25.01.2021).

Дарья Евгеньевна Пьянникова,
студент 3-го курса обучения,
Уральский гуманитарный институт,
Уральский федеральный университет,
E-mail: pyannikova_daria@mail.ru

Daria Ev. Pyannikova,
3nd year student,
Ural Humanitarian Institute,
Ural Federal University,
E-mail: pyannikova_daria@mail.ru

ЦИФРОВАЯ ДИПЛОМАТИЯ КАК ИНСТРУМЕНТ «МЯГКОЙ СИЛЫ» НА ПРИМЕРЕ ИНДИИ И РОССИИ

DIGITAL DIPLOMACY AS A TOOL OF “SOFT POWER” ON THE EXAMPLE OF INDIA AND RUSSIA

Аннотация. Данное исследование посвящено использованию цифровой дипломатии в продвижении официальной политики государства и использовании данного вида дипломатии в качестве «мягкой силы». В нем проанализированы инструменты, которые используются для реализации цифровой дипломатии в Индии и России.

Ключевые слова: цифровая дипломатия, мягкая сила, Индия, Российская Федерация, социальные сети, Интернет, информация, коммуникация.

Abstract. This study is devoted to the use of digital diplomacy in promoting the official policy of the state and the use of this type of diplomacy as a “soft power". It analyzes the tools that are used to implement digital diplomacy in India and Russia.

Key words: digital diplomacy, soft power, India, Russian Federation, social networks, Internet, information, communication.

Введение. С развитием информационных технологий меняется модель коммуникации в международных отношениях. Цифровая дипломатия начала

активно развиваться с 2010-х гг., но мощным толчком послужила пандемия COVID-19, которая привела к необходимости выстраивать общение посредством онлайн-платформ, видеосвязи и социальных сетей. Цифровая дипломатия является неотъемлемым инструментом «мягкой силы» и направлена на решение стратегических задач, таких как создание групп государств с общими технологическими подходами к управлению социальными сетями, информационной безопасностью и цифровым суверенитетом [1]. Цифровая дипломатия формирует общественное восприятие в режиме реального времени и позволяет воздействовать на общественное мнение.

Развитие цифровой дипломатии в России. В Российской Федерации основным инструментом цифровой дипломатии являются социальные сети, это эффективный способ коммуникации с населением, т.к. это, во-первых, доступность информации, во-вторых, взаимодействие в режиме реального времени. Например, в социальной сети ВКонтакте есть официальная страница Министерства иностранных дел Российской Федерации, где публикуется информация по актуальным вопросам внешней политики России и международных отношений. Впервые упоминание цифровой дипломатии МИД России было отмечено еще в Концепции внешней политики Российской Федерации 2013 г. [2]. В целом, в современном мире информационное воздействие позволяет оказывать ненасильственное воздействие на другие субъекты международной политики. МИД РФ имеет достаточно небольшой охват в социальных сетях (около 486 тыс. подписчиков). Пользователи могут следить за публикуемым контентом, снабженном фото- и видеоматериалами, что позволяет быть осведомленным о внешней политике России. Стоит отметить, что в последние годы набирают популярность телеграм-паблики, где также публикуется официальная информация. Telegram является наиболее удобной площадкой, по сравнению с ВКонтакте.

Таким образом, новый формат цифровой дипломатии открывает двери для оперативного обмена свежими новостями. Министерства иностранных дел

различных стран также активно используют свои собственные страницы в социальных сетях, где делятся информационными сводками. Это помогает реализовывать открытую коммуникацию с гражданами, и препятствует распространению фейковой информации. Формирование благоприятного образа российской политики также связано с другими ресурсами цифровой дипломатии [3]. Важным инструментом также являются новостные каналы, например, Первый канал, а также блогосфера. На официальных порталах публикуются данные об их деятельности, что говорит о высоком уровне открытости и прозрачности. Важнейшим направлением цифровой дипломатии МИД России является противодействие фейкам и донесение достоверной информации о внешней политике России.

Развитие цифровой дипломатии в Индии. Индия использует аналогичные инструменты для продвижения цифровой дипломатии. Но есть одно существенное различие: если в России более популярным источником информации является официальная страница МИД России в социальных сетях, то в Индии − это конкретные политические деятели. Хотя в России тоже присутствуют каналы официальных представителей МИД РФ (например, канал Марии Захаровой), они не настолько эффективны, по мнению автора, как в Индии. Цифровая дипломатия − формирование личного бренда политического деятеля. Видеоконференции позволяли мировым лидерам общаться о международных отношениях и дипломатических связях. Например, в 2020 году состоялся XII саммит БРИКС в формате видеоконференции. Цифровая стратегия Индии включает использование мобильных приложений, видеоконференцсвязи и высокоскоростного Интернета для эффективной связи как с внутренней, так и с международной аудиторией. Премьер-министр Нарендра Моди выступает за развитие цифровой дипломатии. Более чем за половину срока председательства Индии в Группе двадцати (G20) стратегия цифровой дипломатии Индии стала центральным элементом её глобальной повестки [4]. Самыми популярными

социальными сетями в Индии являются Twitter и Facebook[2]. Министерство иностранных дел Индии (@MEAIndia) является одним из самых посещаемых в Twitter администраторов министерств иностранных дел во всем мире. Помимо управления социальными сетями Министерства иностранных дел Индии, управление индийской дипломатии (@IndianDiplomacy) также информирует граждан, публикуя пресс-релизы, совместные заявления, выступления, объявления о назначениях новых послов и т.д. [5] Сама концепция того, что Нарендра Моди ведет свои социальные сети, где публикует актуальную информацию, говорит об отсутствии проблемы обезличивания власти. Таким образом он пытается показать свою приверженность к населению и становится лидером при формировании общественного мнения.

Заключение. Таким образом, можно говорить о том, что цифровая дипломатия – это максимально удобная форма «мягкой силы» государства, т.к. информационное пространство позволяет охватить огромную аудиторию, как внутри, так и за пределами страны. Многие правительства, политические лидеры используют цифровую дипломатию для достижения собственных целей и национальных интересов. Цифровая дипломатия – это быстрота и лёгкость в коммуникации, а также экономия времени и ресурсов. Конечно, есть определённые риски, но многие страны активно занимаются разработкой специальных программ, работают над совершенствованием искусственного интеллекта и т.д.

Список источников и литературы:

1. «Цифра» и искусственный интеллект на службе дипломатии: аналитический доклад / Е.С. Зиновьева, Н.А. Цветкова, Э.Л. Сидоренко [и др.]; под редакцией Е.С. Зиновьевой; Московский государственный институт международных отношений (университет) Министерства иностранных дел

[2] Сервисы признаны судом экстремистскими и запрещены в России.

Российской Федерации, Кафедра мировых политических процессов. − Москва: МГИМО-Университет, 2024. − 68 с. ISBN 978-5-9228-2883-3

2. Указ Президента РФ от 12 февраля 2013 г. N Пр-251 "Об утверждении Концепции внешней политики Российской Федерации".

3. Алешкина Н.С. «Цифровая дипломатия»: новые инструменты «мягкой силы» // Вестник ПАГС. 2018. №1. URL: https://cyberleninka.ru/article/n/tsifrovaya-diplomatiya-novye-instrumenty-myagkoy-sily (Accessed: 15.10.2024)

4. Hussain N. India’s G20 Presidency: Towards a Digital Diplomacy Strategy // S. Rajaratnam school of international studies − 06.07.2023 URL: https://www.rsis.edu.sg/rsis-publication/rsis/indias-g20-presidency-towards-a-digital-diplomacy-strategy/ (Accessed: 15.10.2024)

5. Mohilay A. Social Media and India’s Digital Diplomacy: Lessons from Recent International Events // Indian Council of World Affairs Sapru House, New Delhi − 28.12.2023 URL: https://www.icwa.in/show_content.php?lang=1&level=3&ls_id=10333&lid=6588 (Accessed: 15.10.2024)

Екатерина Дмитриевна Ракова,
Студент, Департамент международных отношений,
Международная академия бизнеса и управления,
E-mail: volama@bk.ru

Ekaterina D. Rakova,
Student, Department of International Relations,
International Academy of Business and Management,
E-mail: volama@bk.ru

ЦИФРОВАЯ ПУБЛИЧНАЯ ДИПЛОМАТИЯ МЕЖДУ РОССИЕЙ И ИСЛАМСКОЙ РЕСПУБЛИКОЙ ИРАН

DIGITAL PUBLIC DIPLOMACY BETWEEN RUSSIA AND THE ISLAMIC REPUBLIC OF IRAN

Аннотация. В работе рассмотрены направления и методы цифровой публичной дипломатии России со странами Ближнего Востока на примере Ирана. На первый план выдвигается культурное цифровое взаимодействие стран с целью создания мягкого климата общения между нашими народами, а также применение этого метода дипломатии, как ответа на западные кибератаки и распространение ложной информации о России и Иране. Применение «мягкой силы» в этой сфере помогает доносить проверенную и исторически верную информацию до целевой аудитории и нивелировать ложную информацию «недружественных» стран.

Ключевые слова: Иран, Россия, цифровая публичная дипломатия, мягкая сила, Ближний Восток, цифровое просвещение, противодействие кибератакам, онлайн платформы, цифровые международные отношения, цифровизация востоковедения, киберпространство.

Abstract. The article examines the directions and methods of digital public diplomacy of Russia with the countries of the Middle East using Iran as an example. The focus is on the cultural digital interaction of countries with the aim of creating a soft climate of communication between our peoples, as well as the use of this method of diplomacy as a response to Western cyberattacks and the dissemination of false information about Russia and Iran. The use of "soft power" in this area helps

to convey verified and historically correct information to the target audience and neutralize false information from "unfriendly" countries.

Keywords: Iran, Russia, digital public diplomacy, soft power, Middle East, digital education, countering cyberattacks, online platforms, digital international relations, digitalization of oriental studies, cyberspace.

Цифровая публичная дипломатия как инструмент «мягкой силы». Определение «цифровая эпоха» в настоящее время на слуху у всего мирового сообщества, и мы постоянно слышим о развитии цифровизации в разных областях, об искусственном интеллекте и о кибербезопастности. И это не случайно, от методов и качества позиционирования себя в интернет-пространстве напрямую зависит не только ваш бизнес, но и мировая политика, и отношения между гражданами различных стран.

Цифровая дипломатия является частью публичной дипломатии, поскольку призвана оказывать влияние на зарубежное мнение и позицию народов в мире. Это один из методов мягкой силы. «Мягкая сила» проявляется в применении разных средств, таких как взаимодействие в культурной сфере, искусстве, образовании, дипломатии, сотрудничестве и пропаганде.

В целом по восточному направлению наблюдаются следующие тенденции: сделан значительный рывок в плане сотрудничества и укрепления позиций России в глобальном масштабе. Акцент делается как на Африканский континент, так и на страны Ближнего Востока. Хотелось бы обратить внимание на взаимоотношения Ирана и России в цифровом пространстве.

Такому плотному взаимодействию России и Ирана, конечно же, содействовали в том числе и санкции, введенные против России. И Россия, перенимая опыт Ирана жизни под санкциями в течение многих лет, обратила свой взгляд на улучшение отношений и наращивание взаимодействия в торгово-экономической и культурных сферах со своими партнерами в данном регионе.

Россия и Иран: взаимодействие в цифровом пространстве. Россия и Иран делают значительные шаги на государственном уровне в этом направлении: постоянно проводятся переговоры в части экономического и цифрового сотрудничества, в том числе и по информационной безопасности. Подписываются значимые договора и соглашения [8, 9]. Иран является одним из потенциально возможных наших партнеров по поставкам ИТ-технологий. Также немаловажным является фактор нашего сотрудничества в противодействии киберугрозам в мировом информационном пространстве [10, 11, стр. 4].

Цифровая публичная дипломатия Ирана становится одной из ведущих на мировой арене, она основана на концепции продвижения наследия персидской культуры, языка и религии, как инструмента противостояния западным ценностям, от однополярности и «навязывания своих правил» к многополярному мироустройству [12]. И эта концепция закреплена в Иране законодательно. Позиционируя себя в России, Иран старается содействовать сближению нашего населения в культурном плане прежде всего.

В цифровом пространстве это реализуется через онлайн обучение и персидскому языку, и проведение различных лекций и мероприятий на безвозмездной основе, так как Исламская Республика (ИР) Иран видит свою заинтересованность в проведении политики мягкой силы, как основного элемента достижения своих целей и смотрит далеко в будущее.

Позиционирование Ирана в России. В России продвижением Иранской культуры занимается Культурное представительство при посольстве ИР Иран, издательство Садра, Фонд Ибн Сина, Фонд наследия Ирана и другие. Проводятся как научные, культурно-познавательные лекции и конференции, так и онлайн лектории [16]. Мероприятия можно посетить как в очном формате, так и онлайн. Фонд Ибн Сина осуществляет несколько проектов, в том числе и издание электронного журнала «Ишрак» [4], и ранее YouTube канал, а теперь и развивает одноименный сайт «Изустная история» [3], проект «Исламология» [15].

Фонд Ибн Сина предоставляет доступ для учебных и научных организаций на безвозмездной основе к электронной системе «Нур» (араб. نور – «свет») − это сайт с двадцатью восьмью платформами, куда входят базы данных с научными статьями иранских ученых [5,13, 14]. «Нурлиб» − база данных по книгам арабской культуры. На этих ресурсах находится в цифровом виде вся литература, выходящая на персидском языке, платформа поиска хадисов [1], (хадис (от араб. حديث −«новость» ,«рассказ» (− рассказ очевидцев и современников о поступках и словах пророка Мухаммада, затрагивающий различные религиозно-правовые стороны жизни мусульман), историческая платформа[6], где собраны материалы о важнейших вехах развития исламского мира и проведения параллелей с другими историческими событиями Ближнего Востока, все события интерактивны и, при желании, можно перейти по ссылке и более подробно ознакомиться с событиями.

Деятельность России в ИР Иран. Подобная работа проводится и российской стороной в Тегеране. Продвижением русской культуры там занимаются в основном российская общественная организация «Русский мир», Российское общество культурных связей с Ираном и Россотрудничество. Но, к сожалению, это, как правило, не электронные ресурсы, способные охватывать большую аудиторию, а тематические выставки, праздничные мероприятия и реклама, и содействие обучению в России. Иран занимает более активную позицию в этом вопросе.

Развивая связи с Ираном, Россия делает ставки в пользу сотрудничества в экономической сфере, оставляя «культурные связи» почти без внимания [7]. Что уж говорить о цифровом пространстве. Так же и в диалоге религий: в Иране есть серьезная нехватка теологов-преподавателей по православным наукам, в то время как в России есть исламские университеты, в том числе функционирующие и онлайн. Между тем культурное наследие России и достижения ее в искусстве и науке, туристический потенциал [2] могли бы стать отличным подспорьем в представлении политики Российской Федерации на Ближнем и Среднем Востоке, базой для формирования

положительного имиджа страны в глазах иранцев и, в следствие этого продвижения взаимовыгодных экономических проектов, в том числе и взаимодействие в киберсфере, что повлекло бы за собой большую представленность России на интернет платформах Ирана и возможность доступа к ресурсам обычных граждан, а следовательно к формированию имиджа России и устранению ложных стереотипов, присущих населению из-за недостаточного владения информацией. Имеет место недооценка роли культурного сотрудничества и так называемой «мягкой силы» для наращивания влияния России в регионе.

Заключение. Вышеуказанные организации и цифровые платформы целесообразно будет использовать для изучения и дальнейшего применения студентам, и научному сообществу. Для систематизации знаний и углубления сотрудничества международным государственным структурам, для улучшения взаимоотношений между Россией и странами Ближнего Востока, в первую очередь с Исламской Республикой Иран. Данное исследование позволяет акцентировать внимание на недостаточности представленности России в цифровом пространстве Ирана и показывает перевес активной деятельности с Иранской стороны. Конечно, Российской Федерации следует начать с малого, например, открытия культурного представительства в Иране и предоставления в учебные организации докторов – теологов по православным наукам, параллельно налаживая и цифровое взаимодействие на территории Исламской Республики.

Список источников и литературы:

1. «Абре-е-Нур» − платформа поиска хадисов / https://abrenoor.ir/en (дата обращения: 18.12.2024).

2. Единая межведомственная информационно-статистическая система. Число въездных туристских поездок иностранных граждан в Российскую Федерацию. / https://www.fedstat.ru/indicator/59466 (дата обращения: 18.12.2024).

3. Изустная история − цикл передач об истории отечественного исламоведения в лицах Фонда исследований исламской культуры имени Ибн Сины / https://www.youtube.com/playlist?list=PLLF3IzoNdauaPCuHqi9toew1r48TAqykh (дата обращения: 18.12.2024).

4. Ишрак. Журнал исламской философии / https://j.iphras.ru/index.php/ishraq/index (дата обращения: 18.12.2024).

5. Крупнейший банк статей по исламским и гуманитарным наукам / https://www.noormags.ir/view/en/default (дата обращения: 18.12.2024).

6. Обширная база данных истории на графике Ганта / https://tarikh.inoor.ir/ (дата обращения: 18.12.2024).

7. Ракова Е.Д. Цифровая публичная дипломатия между Россией и Ираном // Цифровое востоковедение / ИВ РАН, ГАУГН. / Т. 3, № 3–4. 2023. − с.15−25 / https://www.ivran.ru/f/DO-2023-Vol-3--No-3-4.pdf?ysclid=m13xhmx7yf932044674 (дата обращения: 18.12.2024).

8. Сетевое издание «Коммерсантъ» // Тегеранская преференция. Технологический сектор России предложил Ирану партнерство / https://www.kommersant.ru/doc/6084928?ysclid=ltprrotwrn817378390 (дата обращения: 18.12.2024).

9. Соглашение между Правительством Российской Федерации и Правительством Исламской Республики Иран о сотрудничестве в области обеспечения информационной безопасности. Двусторонние договоры – Министерство иностранных дел Российской Федерации / https://www.mid.ru/ru/foreign_policy/international_contracts/international_contracts/2_contract/59914/ (дата обращения: 18.12.2024).

10. США провели хакерские атаки на Россию, чтобы предотвратить вмешательство в выборы / https://www.ferra.ru/news/techlife/ssha-proveli-khakerskie-ataki-na-rossiyu-chtoby-predotvratit-vmeshatelstvo-v-vybory-04-11-2020.htm (дата обращения: 18.12.2024).

11. Цветкова Н.А., Сытник А.Н., Гришанина Т.А. Цифровая дипломатия и digital international relations: вызовы и новые возможности // Вестник Санкт-Петербургского университета. Международные отношения. 2022. Т. 15. Вып. 2. С. 174–196. https://cyberleninka.ru/article/n/tsifrovaya-diplomatiya-i-digital-international-relations-vyzovy-i-novye-vozmozhnosti (дата обращения: 18.12.2024).

12. Цветкова Н.А., Ярыгин Г.О. Политизация «цифровой дипломатии»: публичная дипломатия Германии, Ирана, США и России в социальных сетях// Вестник СПбГУ. Сер. 6. 2013. Вып., 1, С.3 (121). Политизация «Цифровой дипломатии»: публичная дипломатия Германии, Ирана, США и России в социальных сетях / https://cyberleninka.ru/article/n/politizatsiya-tsifrovoy-diplomatii-publichnaya-diplomatiya-germanii-irana-ssha-i-rossii-v-sotsialnyh-setyah (дата обращения: 18.12.2024).

13. Центр компьютерных исследований исламских наук / https://alphapedia.ru/w/Computer_Research_Center_of_Islamic_Sciences (дата обращения: 18.12.2024).

14. Цифровая библиотека «Нур» − «Нурлиб» / https://noorlib.ir/en (дата обращения: 18.12.2024).

15. Энциклопедия ислама «Исламология» / https://islamology.ru (дата обращения: 18.12.2024).

LectOrient (Образовательный онлайн проект) / https://lectorient.ru (дата обращения: 18.12.2024).

Виктория Андреевна Рудницкая,
Магистрант 1 курса, факультет международных отношений,
Санкт-Петербургский государственный университет,
E-mail: rudnitskaya.vika862@mail.ru

Яна Сергеевна Фадина,
Магистрант 1 курса, факультет международных отношений,
Санкт-Петербургский государственный университет,
E-mail: fadina.iana@mail.ru

Victoria A. Rudnitskaya,
Master's Degree Student, Faculty of International Relations,
Saint Petersburg State University,
E-mail: rudnitskaya.vika862@mail.ru

Iana S. Fadina,
Master's Degree Student, Faculty of International Relations,
Saint Petersburg State University,
E-mail: fadina.iana@mail.ru

ЦИФРОВАЯ ДИПЛОМАТИЯ И ТРАНСФОРМАЦИЯ МЕЖДУНАРОДНЫХ ОТНОШЕНИЙ В УСЛОВИЯХ ИНФОРМАЦИОННОЙ КОНКУРЕНЦИИ США И КИТАЯ

DIGITAL DIPLOMACY AND TRANSFORMATION OF INTERNATIONAL RELATIONS IN THE CONDITIONS OF INFORMATIONAL COMPETITION OF THE USA AND CHINA

Аннотация. Стремительно развивающийся мир и эпоха цифровизации повлияли на формирование нового информационного пространства. Рассматривается трансформация традиционной публичной дипломатии, которая столкнулась с новыми вызовами. Исследование направлено на сравнение подходов к цифровой дипломатии двух ключевых акторов современной мировой политики − США и КНР, проанализировать как официальные документы и практические шаги, так и дискуссии в научном сообществе двух стран.

Ключевые слова: дипломатия данных, цифровая дипломатия, США, Китай, цифровая трансформация, искусственный интеллект.

Abstract. The rapidly developing world and the digital era have influenced the formation of a new information space. There is considered the transformation of traditional public diplomacy, which has faced new challenges. The study aims to compare the approaches to digital diplomacy of two key actors in modern world politics − the United States and China, to analyze both official documents and practical steps, as well as discussions in the scientific community of the two countries.

Keywords: data diplomacy, digital diplomacy, USA, China, digital transformation, artificial intelligence.

Датафикация в мировой политике. Цифровая дипломатия в эпоху глобальной датафикации становится важнейшим инструментом международных отношений, позволяя государствам управлять информационными потоками и влиять на восприятие мировой политики через цифровые каналы. Датафикация, подразумевающая превращение данных в ключевой политический и экономический ресурс, трансформирует дипломатические методы и стратегии, делая акцент на использовании больших данных и искусственного интеллекта для решения внешнеполитических задач [4]. Цифровая дипломатия, которая в начале 2010-х годов ограничивалась распространением информации через социальные сети, сегодня включает более сложные механизмы работы с данными, такие как алгоритмы, направленные на фильтрацию аудитории, идентификацию целевых групп, создание таргетированных информационных кампаний и прочее [2].

Актуальность исследования состоит в том, что в настоящее время наблюдается становления абсолютно иной цифровой реальности, которая, в свою очередь, имеет отражение не только на прогрессивном развитии востребованных социальных сетей, но и на ведущих акторах сложившейся системы международных отношений.

Цифровая трансформация на современном этапе. В рамках этого процесса дипломатия данных – новый этап развития цифровой дипломатии, основанный на аналитике больших данных и использовании технологий искусственного интеллекта для управления информацией. Дипломатия данных предоставляет возможность оперативного реагирования на информационные вызовы, включая опровержения в ответ на враждебную пропаганду, и становится мощным инструментом противостояния между государствами в условиях фрагментации цифрового пространства [5].

Современные международные отношения демонстрируют, как цифровизация трансформирует взаимодействие государств, делая информационные войны неотъемлемой частью дипломатической практики. Цифровая дипломатия в 2020-е годы становится механизмом, через который такие государства, как США и Китай управляют общественным мнением, формируют международные альянсы и защищают свои интересы на глобальной арене.

С увеличением числа участников информационной арены – от неправительственных организаций до блогеров и активистов – цифровая дипломатия сталкивается с новыми вызовами. Государственные ведомства теряют монополию на информационные потоки, а конкуренция за внимание аудитории становится более острой. Процессы датификации усиливают эту тенденцию, предоставляя неограниченные возможности для манипуляции информацией и распространения фейковых новостей. Появление феномена «цифровой силы» меняет традиционное распределение ролей в международных отношениях, усиливая влияние государств через использование цифровых технологий [1].

Научный дискурс. Изучение теоретических подходов неотделимо от анализа современного состояния всех мирополитических аспектов. Так и идейно-теоретические течения в отношениях цифровой дипломатии выступают базисом к обоснованию уместности применения механизмов публичной дипломатии с целью укрепления внешнеполитического имиджа

страны для ее конкурентноспособности. Цифровая дипломатия проявляется как инструмент цифровых международных отношений и всесторонне рассматривается в научном пособии «Цифровые международные отношения» (Москва, 2023) под редакцией Е.С. Зиновьевой и С.В. Шитькова [1]. Проблемы международной информационной безопасности заставляют сконцентрироваться на рисках, возникающих в процессе информационной борьбы. Внимание многих экспертов направлено на влияние информационных технологий и инноваций на мировую политику, что непосредственно находит отражение и в специфике организации ведомственных государственных структур. С.В. Кривохиж и М.П. Теленьга [3] обращают особое внимание на стратегии крупнейших акторов мирового сообщества – США и Китая, осуществляют разбор актуальных концептуальных дискуссий экспертов в сфере цифровой дипломатии. Большое внимание также уделяется практической стороне столкновения их интересов на внешнеполитической арене. Теоретическая основа исследования состоит из трудов Торкунова А.В.[6], Кривохиж С.В. и Теленьга М.П. [3], Кузнецова Н.М. и Цветковой Н.А. [4], Сытник А.Н. и Гришаниной Т.А. [5] и др.

Стратегические соперники. Цифровая дипломатия США и Китая иллюстрирует две разные стратегии работы в цифровом пространстве. Если США делают ставку на продвижение универсальных демократических ценностей через социальные сети и алгоритмические решения, то Китай, начиная с 2013 года, использует более агрессивные подходы, включая вирусные видео и активное присутствие в международных цифровых средах, таких как YouTube и Twitter[1] [3]. Несмотря на эти различия, в условиях датафикации и цифровизации границы между подходами этих двух держав стираются, вынуждая страны использовать новые, ранее непривычные форматы и инструменты, а также активно реагировать на действия оппонентов и постоянно корректировать свою политику. В условиях неопределенности,

[1] Twitter является запрещённой организацией на территории Российской Федерации.

жесткой конкуренции и манипуляций информацией различия между стратегиями цифровой дипломатии США и Китая постепенно стираются.

Изучение информационных стратегий стран, абсолютно противоположных в своих взглядах, интересно еще и с той точки зрения, что дальнейшее направление их деятельности может определить будущее, а также своевременно предотвратить информационную напряженность и стать предметом для исследований.

Список источников и литературы:

1. Цифровые международные отношения: В двух томах. Том 1: Учебное пособие для вузов / Под ред. Е. С. Зиновьевой, С. В. Шитькова. − Москва: Издательство «Аспект Пресс», 2023. − 354 с.

2. Зиновьева Е.С. Кибердипломатия в условиях обострения великодержавной конкуренции // Вестник МГИМО-Университета. 2024. 17(4). С. 27–47.

3. Кривохиж С. В., Теленьга М. П. Трансформация цифровой дипломатии в условиях новых вызовов: взгляд из Вашингтона и Пекина// Вестник Санкт-Петербургского университета. Международные отношения. 2024. Т. 17. Вып. 2. С. 143–163.

4. Кузнецов Н.М., Цветкова Н.А. Дипломатия данных России: цели, тенденции, прогнозы // Вестник РГГУ. Серия «Политология. История. Международные отношения». 2022. №1. С. 26–40.

5. Цветкова Н.А., Сытник А.Н., Гришанина Т.А. Цифровая дипломатия и digital international relations: вызовы и новые возможности // Вестник Санкт-Петербургского университета. Международные отношения. 2022. Т. 15. Вып. 2. С. 174–196. https://doi.org/10.21638/spbu06.2022.204

6. МГИМО – Университет: Традиции и современность. 1944 – 2004 / Под общ. ред. А.В. Торкунова. – М.: ОАО «Московские учебники и Картолитография», 2004. – 336 с.

СЕКЦИЯ 2

«ТЕХНОЛОГИИ И МЕТОДЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

Диляра Хусяиновна Акчурина,
Ассистент, кафедра безопасности информационных технологий,
РГУ нефти и газа (НИУ) имени И.М. Губкина,
E-mail: dilyara-akchurina@mail.ru

Dilyara K.Akchurina,
Assistant, Department of Information Technology Security,
National University of Oil and Gas «Gubkin University»,
E-mail: dilyara-akchurina@mail.ru

АКТУАЛЬНОСТЬ ОЦЕНКИ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ ТЕХНОЛОГИЧЕСКИХ ПРОЦЕССОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

RELEVANCE OF INFORMATION RISK ASSESSMENT SAFETY OF AUTOMATED CONTROL SYSTEMS TECHNOLOGICAL PROCESSES OF CRITICAL INFORMATION INFRASTRUCTURE

Аннотация. Обоснована необходимость анализа рисков информационной безопасности объектов ТЭК как объектов критической информационной инфраструктуры. Выделена проблема отсутствия отечественного программного инструментария для количественной оценки рисков, отвечающего ключевым требованиям. Рассмотрены основные программные инструменты для анализа рисков информационной безопасности, проведен их сравнительный анализ.

Abstract. The necessity of analyzing the risks of information security of fuel and energy complex facilities as objects of critical information infrastructure is substantiated. The problem of the lack of domestic software tools for quantitative risk assessment that meets key requirements is highlighted. The main software tools for analyzing information security risks are considered and their comparative analysis is carried out.

Ключевые слова: управление рисками, риски информационной безопасности, КИИ, АСУ ТП.

Keywords: risk management, information security risks, critical information infrastructure, APCS.

Современные автоматизированные системы управления технологическими процессами (АСУ ТП) характеризуются возрастающей сложностью и постоянной модернизацией, основанной на передовых технологиях, что делает невозможным обеспечение безопасности только за счет контроля физического доступа к компонентам АСУ ТП. По мере ускорения цифровизации и все большей взаимосвязанности информационных систем расширяется поверхность атак, что приводит к появлению сложных угроз информационной безопасности, бросающих вызов традиционным парадигмам безопасности.

В соответствии с Федеральным законом от 26.07.2017 г. № 187-ФЗ «О безопасности критический информационной инфраструктуры РФ» информационные системы, сети, АСУ ТП топливно-энергетического комплекс выступают объектами критический информационной инфраструктуры [1].

Необходимость обеспечения информационной безопасности (ИБ) АСУ ТП как объектов критической информационной инфраструктуры (КИИ) обусловлена также требованиями приказов ФСТЭК России № 239 и 31. Данные приказы содержат требования к применяемым мерам защиты информации АСУ ТП КИИ в соответствии с присвоенной категорией значимости объекта КИИ и классом защищенности АСУ.

Противодействовать угрозам и пресекать нарушения ИБ на объектах КИИ невозможно без грамотной организации процесса управления рисками ИБ. Эффективный риск-менеджмент основывается на выборе оптимальный методики и инструмента для оценки рисков в зависимости от специфики и потребностей предприятия.

Кроме того, внедрение новых технологий в АСУ ТП, как интернет-вещей, облачные вычисления, большие данные, виртуализация приводят к

возникновению дополнительных, не учтенных ранее рисков реализации угроз безопасности информации. Так, согласно данным Национального координационного центра по компьютерным инцидентам, число кибератак на объекты КИИ России за 2023 год выросло на 16% относительно предыдущего 2022 года [4].

Анализ исследований в области управления рисками ИБ показал, что, по мнению многих специалистов, при оценке рисков приоритет отдается качественным методам оценки рисков [3]. Готовых решения для количественной оценки рисков ИБ на данный момент ограниченное количество. При этом большинство из них являются разработками международных компаний. Одним из аналогов зарубежных инструментальных средств анализа рисков нарушения ИБ выступает отечественная русскоязычная программа ГРИФ, разработчиком которой является одна из ведущих российских консалтинговых компаний Digital Security.

Проведен сравнительный анализ существующего программного инструментария для управления рисками ИБ. Критериями для сравнения выступили: возможность управления, методы оценки, предлагаемые способы снижения рисков, использование элементов рисков, способы измерения величин, мониторинг рисков, стоимость использования, наличие поддержки. В качестве сравниваемых программных комплексов выступили CRAMM, Risk Watch, CORAS, MSAT, ГРИФ и ряд других.

Универсальным и допустимым инструментом для анализа рисков ИБ соответствующим потребностям российских пользователей выступает отечественное решение ГРИФ. Данное программное обеспечение позволяет проводить мониторинг динамики бизнес-процессов, оценивать риски как качественно, так и количественно, а также проводить анализ политики безопасности в соответствии с архитектурой информационной системы [2]. Преимуществом также выступает невысокая цена и возможность

использования без наличия специализированных компетенций у пользователей.

Для повышения защищенности АСУ ТП критической информационной инфраструктуры необходима организация грамотной системы управления рисками, согласованной с существующей практикой обеспечения ИБ, методами управления рисками и требованиями приказов ФСТЭК России.

Список источников и литературы:

1. Федеральный закон от 26 июля 2017 г. N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации" // Справочно-правовая система КонсультантПлюс (дата обращения 14.09.2024).

2. Баранова Е. К., Чернова М. В. Сравнительный анализ программного инструментария для анализа и оценки рисков информационной безопасности Проблемы информационной безопасности. Компьютерные системы. 2014. № 4. С. 160-168.

3. Минаков А. В. Оценка модели рисков информационной безопасности: характеристика, проблемы и перспективы // Экономика и бизнес: теория и практика. 2023. № 10–2 (104). С. 63–69.

4. Review Цифровая инфраструктура. Приложение №85/П от 20.05.2024, стр. 1. URL: https://www.kommersant.ru/doc/6679041 (дата обращения: 14.09.2024)

Софья Сергеевна Близнякова,
Управление по борьбе с противоправным использованием
информационно-коммуникационных технологий,
Главное Управления МВД России
по г. Санкт-Петербургу и Ленинградской области
E-mail: sofia.bliznyakova@yandex.ru

Sofya S.Bliznyakova,
Department for Combating the Illegal Use of Information
and Communication Technologies,
Main Directorate of the Ministry of Internal Affairs
of the Russian Federation for St. Petersburg and the Leningrad Region
E-mail: sofia.bliznyakova@yandex.ru

К 75-ЛЕТИЮ РОССИЙСКО-КИТАЙСКИХ ДИПЛОМАТИЧЕСКИХ ОТНОШЕНИЙ. РОССИЙСКО-КИТАЙСКОЕ СОТРУДНИЧЕСТВО ПО ЛИНИИ МИНИСТЕРСТВ ВНУТРЕННИХ ДЕЛ В ОБЛАСТИ ОБЕСПЕЧЕНИЯ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

TO THE 75TH ANNIVERSARY OF RUSSIAN-CHINESE DIPLOMATIC RELATIONS. RUSSIAN-CHINESE COOPERATION THROUGH THE MINISTRIES OF INTERNAL AFFAIRS IN THE REGION ENSURING INTERNATIONAL INFORMATION SECURITY

Аннотация. В работе представлен анализ сотрудничества России и Китая в области международной информационной безопасности (МИБ) в контексте 75-летия дипломатических отношений. Рассматриваются ключевые документы, роль министерств внутренних дел в обеспечении кибербезопасности и противодействии киберпреступности, а также примеры совместных проектов в 2024 году. Подчеркивается важность российско-китайского взаимодействия в укреплении глобальной безопасности ИКТ-среды.

Ключевые слова: МВД, кибербезопасность, киберпреступность, международное сотрудничество, российско-китайское сотрудничество.

Abstract. The paper presents an analysis of cooperation between Russia and China in the field of international information security (IIS) in the context of the 75th anniversary of diplomatic relations. Key documents, the role of the ministries of internal affairs in ensuring cybersecurity and combating cybercrime, as well as examples of joint projects in 2024 are considered. The importance of Russian-Chinese interaction in strengthening global cybersecurity is emphasized.

Key words: Ministry of Internal Affairs, cybersecurity, cybercrime, international cooperation, Russian-Chinese cooperation.

Введение. Международная информационная безопасность (МИБ) представляет собой состояние глобального информационного пространства, при котором поддерживаются мир, стабильность и безопасность на основе международного права и равноправного партнёрства [5]. Основными угрозами в этой сфере являются кибератаки на критическую инфраструктуру, пропаганда терроризма через информационные технологии, вмешательство во внутренние дела государств и киберпреступления.

Россия и Китай: сотрудничество в области МИБ. Россия и Китай сталкиваются с общими вызовами в защите ИКТ-среды и противодействии киберпреступности. Их партнёрство развивается на фоне многолетних дипломатических связей [1, 2, 8, 9, 10, 13, 14]. Основой двустороннего сотрудничества являются два основополагающих документа: Соглашение о сотрудничестве в области МИБ (2015) и Совместное заявление о развитии информационного пространства (2017). Эти документы подчеркивают важность взаимодействия в международных организациях, таких как ООН, ШОС, БРИКС (+) и ставят целью создание всеобъемлющего международного соглашения по МИБ.

Роль МВД в обеспечении МИБ. Министерства внутренних дел России и Китая занимают лидирующее место в борьбе с киберпреступностью. В России это Управление «К» [7], которое координирует действия с зарубежными партнёрами для противодействия киберпреступлениям, обмена

информацией и поддержания устойчивости международной кибербезопасности. В Китае аналогичную функцию выполняет Бюро №11 Министерства общественной безопасности [20]. Одним из крупнейших проектов Китая в этой сфере является проект «Золотой Щит», направленный на улучшение кибербезопасности и защиту граждан [22].

Совместные проекты и инициативы России и Китая в области МИБ в юбилейном 2024 году. По словам заместителя директора Информационно-исследовательского центра прокурорских технологий Верховной народной прокуратуры Чжао Сяньвэя, после создания государств-членов ШОС в Шанхае в 2001 году, в 2002 году в системе прокуратуры ШОС была создана Конференция генеральных прокуроров высокого уровня [23, 25]. Орган прокуратуры ШОС проводит собрание раз в год, а в 2024 году оно состоялось [25] уже в двадцать второй раз. Участники обменялись опытом цифрового реформирования органов прокуратуры в различных странах, реагирования на новые угрозы и вызовы, защиты прав человека и обеспечение устойчивого состояния МИБ. Страны договорились, что следующая встреча генеральных прокуроров государств-членов ШОС пройдет в Пакистане в 2025 году.

Ещё одним мероприятием в рамках российско-китайского сотрудничества по линии МВД по вопросам МИБ стала XII Международная встреча высоких представителей, курирующих вопросы безопасности, прошедшая в г. Санкт-Петербурге 26 апреля 2024 года. На встрече присутствовали представители 114 стран и международных организаций, в их числе был и член Политбюро ЦК КПК, секретарь Центральной политико-правовой комиссии, Чэнь Вэньцин, выступивший с программной речью [26]. Он заявил о готовности КНР сотрудничать по МИБ с региональными державами, также обратил внимание на необходимость бороться с киберпреступностью в соответствии с законом, способствовать разработке международных правил для ИКТ-среды и достигать устойчивости в нём [26]. Чэнь Вэньцин также присутствовал на обеде глав делегаций стран БРИКС и

провел двусторонние переговоры и встречи с главами делегаций многих стран, в том числе с секретарем Совета Безопасности РФ Н.П. Патрушевым [26].

Значимой инициативой Китая стало предложение, высказанное Ли Цзинцзином, директором Бюро №11 Министерства общественной безопасности, о создании комплекса мер трансграничного предотвращения и контроля киберпреступности в рамках ШОС [24]. Полагается, что по мере развития подходов к обеспечению МИБ, инициатива будет способствовать унификации подходов к определению киберпреступлений и мер по борьбе с ними.

Полагаем, что партнёрство правоохранительных органов России и Китая в рамках реализации данной инициативы представляется наиболее эффективным, поскольку проводимые регулярные совместные мероприятия и достигнутые соглашения значительно улучшают взаимодействие между правоохранительными органами обеих стран, географическое соседство стран способствует более быстрому и эффективному реагированию на угрозы, а также упрощает логистику совместных операций в области обеспечения МИБ, и, наконец, общие стратегические интересы в регионе и на мировой арене являются весомым аргументом в пользу налаживания партнёрства правоохранительных органов для обеспечения МИБ именно между Россией и Китаем.

Перспективы сотрудничества. В 2024 году отмечается 75-летие установления дипломатических отношений между Россией и Китаем. Страны активно развивают сотрудничество в сфере информационной безопасности и планируют расширять взаимодействие в рамках международных организаций, таких как ООН, БРИКС и ШОС [19]. Это сотрудничество включает как защиту от в ИКТ-среде, так и реализацию совместных инициатив по обеспечению правопорядка в информационном пространстве.

Заключение. Российско-китайское сотрудничество в области МИБ продолжает углубляться. Благодаря обмену опытом и совместной борьбе с киберпреступностью, страны обеспечивают стабильность и безопасность в

информационном пространстве. В условиях современных вызовов это партнёрство играет важную роль в поддержании глобального мира и безопасности.

Список источников и литературы:

1. Заявление глав государств-членов ШОС по международной информационной безопасности, 15 июня 2006 года. URL: http://infoshos.ru/ru/?id=94 (дата обращения: 10.09.2024).

2. Китай и Россия опубликовали Совместное заявление о дальнейшем углублении отношений всеобъемлющего партнерства и стратегического взаимодействия // Новостной ресурс. URL: https://russian.news.cn/2017-07/05/c_136419741.htm (дата обращения: 10.09.2024).

3. Министерство внутренних дел России Владимир Колокольцев находится с рабочим визитом в Китае // Новостной ресурс. URL: https://www.1tv.ru/news/2023-12-05/466472-ministr_vnutrennih_del_rossii_vladimir_kolokoltsev_nahoditsya_s_rabochim_vizitom_v_kitae (дата обращения: 10.09.2024).

4. МИД оценил сотрудничество с Китаем в области информбезопасности // Новостной ресурс. URL: https://ria.ru/20240105/kitay-1919778402.html (дата обращения: 10.09.2024).

5. Основы государственной политики Российской Федерации в области международной информационной безопасности (Утверждены Указом Президента Российской Федерации от 12 апреля 2021 г. № 213).

6. О российско-китайских консультациях по международной информационной безопасности (МИБ) // Пресс-релиз. URL: https://mid.ru/ru/foreign_policy/international_safety/1864294/ (дата обращения: 10.09.2024).

7. Приказ МВД России от 29.12.2022 N 1110 "Об утверждении Положения об Управлении по организации борьбы с противоправным использованием информационно-коммуникационных технологий

Министерства внутренних дел Российской Федерации" СЗ РФ. 2011. № 7, ст. 900.

8. Путин и Си Цзиньпин подписали заявление об углублении отношений // Новостной ресурс. URL: https://tass.ru/politika/20813413 (дата обращения: 10.09.2024).

9. Соглашение между правительствами государств—членов Шанхайской Организации Сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности, 16 июня 2009 года. URL: https://ccdcoe.org/uploads/2018/11/SCO-090616-IISAgreementRussian-1.pdf (дата обращения: 10.09.2024).

10. Соглашение между Правительством Российской Федерации и Правительством Китайской Народной Республики о сотрудничестве в области обеспечения международной информационной безопасности от 8 мая 2015 года. URL: http://publication.pravo.gov.ru/Document/View/0001201608100001?rangeSize=1 (дата обращения: 10.09.2024).

11. Сообщение МИД России от 14 июня 2011 года «О вступлении в силу Соглашения между правительствами государств-членов ШОС о сотрудничестве в области обеспечения международной информационной безопасности». URL: https://base.garant.ru/2571125/ (дата обращения: 10.09.2024).

12. Совместное заявление Российской Федерации и Китайской Народной Республики об углублении отношений всеобъемлющего партнерства и стратегического взаимодействия, вступающих в новую эпоху, в контексте 75-летия установления дипломатических отношений между двумя странами, 16 мая 2024 года. URL: http://www.kremlin.ru/supplement/6132 (дата обращения: 10.09.2024).

13. Ташкентская декларация 15-летия Шанхайской организации сотрудничества, 24 июня 2016 года. URL: http://special.kremlin.ru/supplement/5094 (дата обращения: 10.09.2024).

14. Циндаоская декларация Совета глав государств – членов Шанхайской организации сотрудничества, 10 июня 2018 года. URL: http://www.kremlin.ru/supplement/5315 (дата обращения: 10.09.2024).

15. Федеральный закон «О полиции» от 7 февраля 2011 года № 3-ФЗ: в ред. Федерального закона от 3 августа 2018 года № 322-ФЗ СЗ РФ, 2016, N 52, ст. 7614; 2022, N 40, ст. 6787.

16. United Nations: Member States finalize a new cybercrime convention, 9 August 2024 // Пресс-релиз. URL: https://www.unodc.org/unodc/frontpage/2024/August/united-nations_-member-states-finalize-a-new-cybercrime-convention.html (дата обращения: 10.09.2024).

17. 中华人民共和国和俄罗斯联邦关于《中俄睦邻友好合作条约》签署 20 周年 的联合声 (Совместное заявление Китайской Народной Республики и Российской Федерации по случаю 20-летия подписания Договора о добрососедстве, дружбе и сотрудничестве между Китаем и Россией). URL: https://www.mfa.gov.cn/web//gjhdq_676201/gj_676203/oz_678770/1206_679110/1207_679122/202106/t20210628_9182899.shtml (дата обращения: 10.09.2024).

18. 中国公安部与俄罗斯等国执法机构保持有效合作 (Министерство общественной безопасности Китая поддерживает эффективное сотрудничество с правоохранительными органами России и других стран) // Новостной ресурс. URL: https://sputniknews.cn/20240527/1059355713.html (дата обращения: 10.09.2024).

19. 中华人民共和国网络安全法 (Закон Китайской Народной Республики о кибербезопасности). URL: https://www.gov.cn/xinwen/2016-11/07/content_5129723.htm (дата обращения: 10.09.2024).

20. 金 盾 ("Золотой щит"). URL: http://www.goldencis.com/ (дата обращения: 10.09.2024).

21. 开展国际合作打击网络犯罪已成共识 (Международное сотрудничество в борьбе с киберпреступностью стало всеобщим консенсусом) // Новостной ресурс. URL: https://sh.12348.gov.cn/sites/12348/news-detail.jsp?entityid=0965479ef5e54fc4a04698809fc31d6e&category=lpa.Dynamic (дата обращения: 10.09.2024).

22. 网络犯罪黑色产业链趋向无国界 (Черный рынок киберпреступности становится трансграничным) // Новостной ресурс. URL: http://money.people.com.cn/n1/2016/0817/c392426-28642834.html (дата обращения: 10.09.2024).

23. 上海合作组织成员国举行总检察长会议 (Заседание генеральных прокуроров государств-членов Шанхайской организации сотрудничества). URL: https://chn.sectsco.org/20240726/1469569.html (дата обращения: 10.09.2024).

24. 陈文清在俄出席第十二届安全事务高级代表国际会议 (Чэнь Вэньцин принял участие в 12-й Международной конференции высокопоставленных представителей по вопросам безопасности в России) // Новостной ресурс. URL: http://www.news.cn/politics/leaders/20240424/243a7f6accee443e852f694954f80551/c.html (дата обращения: 10.09.2024).

Ксения Денисовна Коннова,
Магистрант, факультет международных отношений
МГИМО МИД России,
E-mail: ks.konnova@mail.ru

Виталий Анатольевич Эпштейн,
зав. каф. мировой экономики и международных отношений,
ИБДА РАНХиГС, к. социолог. н., доцент,
E-mail: epshteinv@gmail.com

Ksenia D. Konnova,
Master's Degree Student, Faculty of International Relations,
MGIMO University,
E-mail: ks.konnova@mail.ru

Vitaliy A.Epstein,
Head of Department of World Economy and International Relations,
IBS RANEPA, Ph.D. in Sociology, Associate Professor,
E-mail: epshteinv@gmail.com

ОСНОВНЫЕ ПОДХОДЫ К ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ПРИМЕРЕ США, ЕС, РФ И КНР

THE MAIN APPROACHES TO ENSURING INFORMATION SECURITY ON THE EXAMPLE OF THE USA, THE EU, THE RUSSIAN FEDERATION AND THE PEOPLE'S REPUBLIC OF CHINA

Аннотация. Статья посвящена проблематике обеспечения информационной безопасности (ИБ) как критически важного элемента защиты личности, общества и государства от внутренних и внешних угроз. Актуальность исследования определяется ростом информационно-коммуникационных технологий в экономике, политике и обеспечении безопасности как в отдельно взятых странах, так и в мире в целом и роста количества военных и террористических угроз с их использованием. В работе проведен анализ подходов к ИБ со стороны четырех ключевых международных игроков: Российской Федерации, Соединенных Штатов Америки, Европейского Союза, Китайской Народной Республики.

В рамках исследования представлена эволюция подходов к ИБ, основные нормативно-правовые документы, а также специфика и ключевые особенности каждого актора. Статья строится на теоретическом анализе законодательных актов, научной литературы и публикаций экспертов. В заключение подчеркивается необходимость глобального сотрудничества для разработки универсальных норм и подходов к ИБ, в условиях нарастающих киберугроз, что должно способствовать обеспечению стабильности в международных отношениях и обеспечению мирного сосуществования в цифровом пространстве.

Ключевые слова: информационная безопасность, защита данных, безопасность данных, нормативно-правовая основа, США, ЕС, КНР, РФ, особенности подходов.

Abstract. The article addresses the issues of ensuring information security as a fundamental element of protecting individuals, society and the state from internal and external threats. The relevance of the study is determined by the growth of information and communication technologies in the economy, politics and security both in individual countries and in the world as a whole and the increasing number of military and terrorist threats using them. The paper analyses the approaches to IS by four key international players: the Russian Federation, the United States of America, the European Union, the People's Republic of China.

The study presents the evolution of approaches to IS, the main legal and regulatory documents, as well as the specifics and key features of each actor. The article is based on a theoretical analysis of legislative acts, scientific literature and expert publications. It concludes by emphasizing the need for global cooperation to develop universal norms and approaches to IS in the context of growing cyber threats, which should contribute to ensuring stability in international relations and peaceful coexistence in the digital space.

Keywords: information security, data protection, data security, regulations, USA, EU, China, Russian Federation, features of approaches.

Развитие информационной безопасности является требованием времени ввиду роста количества информационно-коммуникационных технологий (ИКТ) и их модернизации. В эру общедоступности информации, скорости ее распространения и возможностей ее интерпретации, общество сталкивается с новыми вызовами и угрозами: использованием ИКТ в военно-политических, пропагандистских (с целью подрыва суверенитета государства, нарушения территориальной целостности), террористических, экстремистских и преступных целях.

Автор осуществил анализ нормативно-правовых актов США [6;11;12;13;14], ЕС [10;15], РФ [1;2;3;4;5] и КНР [7;8;9], сравнение и обобщение точек зрения, представленных в научной литературе [16;20], посвящённой данной проблематике на русском и английском языках.

Выявлено, что каждый актор находится в процессе разработки собственной нормативно-правовой базы для обеспечения функционирования системы ИБ. На основе проведенного анализа нормативно-правовых актов можно утверждать, что подходы у стран по многим вопросам противоречивы: США и ЕС рассматривают систему ИБ и ее особенности в рамках существующей западноцентричной системы, Китай проводит более обособленную, закрытую политику, в то время как РФ пытается наращивать информационно-технологические возможности, чтобы обеспечить свой цифровой суверенитет.

Подход к обеспечению ИБ определяется каждым актором в соответствии с техническими, геополитическими и технологическими условиями.

Подходу Российской Федерации характерны следующие особенности:

1) ИБ является неотъемлемой составляющей политики национальной безопасности.

2) Страна стремится усилить компоненты ИБ.

3) Блокировка ряда зарубежных интернет-ресурсов (ввиду нарушения данными ресурсами российского законодательства) и создание отечественных аналогов.

4) Высокий уровень использования информационных технологий для оказания услуг и недостаточный уровень развития для осуществления производства.

Подход США отличают следующие аспекты:

1) Разобщенность системы кибербезопасности: ответственность распределена между многими агентствами и федеральными департаментами, но никто не наделен должными полномочиями для проведения решительных мер и разрешения конфликтных ситуаций.

2) Распространено частно-государственное партнерство (сотрудничество с частным сектором) в обеспечении кибербезопасности.

3) По ряду причин существует открытая враждебность к непосредственному государственному регулированию, т.к. оно, в некоторой степени, препятствует развитию.

4) Применение новых передовых технологий и ИИ для обеспечения ИБ.

Подходу Европейского союза характерны следующие особенности:

1) Несмотря на попытки проведения последовательной политики в области ИБ, каждое государство пытается самостоятельно регулировать сферу ИБ, что свидетельствует о проблемах взаимодействия.

2) Различия в экономическом развитии стран-членов ЕС способствуют дисбалансу в уровне обеспечения ИБ.

3) Особенность системы ЕС – последовательная и целенаправленная политика по нахождению баланса между национальной и наднациональной компетенциями.

Подход КНР отличают аспекты:

1) Особый режим автономности информационно-телекоммуникационной сети «Интернет».

2) Блокировка большого количества зарубежных интернет-ресурсов и создание отечественных аналогов.

3) Сбор и использование конфиденциальной личной информации возможен только при получении явного разрешения от субъекта данных.

4) Обеспечение ИБ при помощи новой модели государственного управления с использованием достижений цифровизации – «умное управление».

5) Рост сотрудничества с частными ИТ-компаниями.

Каждый из рассмотренных подходов формируется не только на технологической основе, но также на исторических, культурных и политических особенностей стран и регионов, что делает информационную безопасность не просто технической задачей, но и важным элементом геополитических стратегий. В условиях, как глобализации, так и регионализации продолжает увеличиваться количество и изменяться качество киберугроз со стороны антисистемных акторов (террористических организаций, экстремистских группировок и др.), что требует продолжения сотрудничества между государствами по выработке новых меры по защите от информационных угроз ради обеспечения стабильности международных отношениях.

Список источников и литературы:

1. Российская Федерация. Законы. Об информации, информационных технологиях и защите информации: Федеральный закон № 149-ФЗ: [принят Государственной думой 8 июля 2006 года: одобрен Советом Федерации 14 июля 2006 года] – Текст: электронный. – URL: http://www.kremlin.ru/acts/bank/24157 (дата обращения: 13.10.2024).

2. Российская Федерация. Законы. О персональных данных: Федеральный закон № 152-ФЗ: [принят Государственной думой 8 июля 2006 года: одобрен Советом Федерации 14 июля 2006 года] – Текст: электронный. – URL: http://www.kremlin.ru/acts/bank/24154 (дата обращения: 13.10.2024).

3. Российская Федерация. Министерство иностранных дел. Внешняя политика. Основополагающие документы. Стратегия национальной безопасности Российской Федерации от 2 июля 2021 г. – Текст: электронный. – URL: https://www.mid.ru/ru/foreign_policy/official_documents/1784948/ (дата обращения: 13.10.2024).

4. Российская Федерация. Указы. Об утверждении Доктрины информационной безопасности Российской Федерации: Указ Президента Российской Федерации от 05.12.2016 г. № 646: [утвержден Президентом Российской Федерации 5 декабря 2016 года] – Текст: электронный. − URL: http://www.kremlin.ru/acts/bank/41460 (дата обращения: 12.10.2024).

5. Российская Федерация. Указы. О дополнительных мерах по обеспечению информационной безопасности Российской Федерации: Указ Президента Российской Федерации от 01.05.2022 г. №250: [утвержден Президентом Российской Федерации 1мая 2022 года] – Текст: электронный. − URL: http://www.kremlin.ru/acts/bank/47796 (дата обращения: 13.10.2024).

6. The Alliance for the Future of the Internet – Text: online // Non-Paper. − Discussion Purposes Only. − Politico, 2021. − URL: https://www.politico.com/f/?id=0000017c-e71b-d8e1-a57c-efffa3810004 (дата обращения: 12.10.2024).

7. China Cybersecurity Law, 2016 – Text: online. – URL: https://d-russia.ru/wp-content/uploads/2017/04/China-Cybersecurity-Law.pdf (дата обращения: 12.10.2024).

8. China National Informatization Development Strategy 2006-2020 – Text: online. − URL: https://digichina.stanford.edu/work/2006-2020-national-informatization-development-strategy/ (дата обращения: 12.10.2024)

9. Data Security Law of the People’s Republic of China, 2021: Translation – Text: online. – URL: https://digichina.stanford.edu/work/translation-data-security-law-of-the-peoples-republic-of-china/ (дата обращения: 13.10.2024).

10. The EU Cyber Solidarity Act, 2023 – Text: online. – URL: https://digital-strategy.ec.europa.eu/en/policies/cyber-solidarity (дата обращения: 12.10.2024).

11. The Federal Information Security Management Act of 2002 – Text: online. – URL: https://www.govinfo.gov/content/pkg/STATUTE-116/pdf/STATUTE-116-Pg2899.pdf (дата обращения 12.10.2024).

12. The Federal Information Security Modernization Act of 2014 – Text: online. − URL: https://www.congress.gov/bill/113th-congress/senate-bill/2521 (дата обращения 12.10.2024).

13. The Homeland Security Act. Version 2023 – Text: online. – URL: https://www.dhs.gov/sites/default/files/2023-11/23_0930_HSA-2002-updated.pdf (дата обращения 12.10.2024).

14. The National Cybersecurity Strategy, 2023 – Text: online. – URL: https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf (дата обращения: 17.03.2024).

15. Network and Information security: Proposal for A European Policy Approach – Text: online. – URL: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2001:0298:FIN:EN:PDF (дата обращения: 20.03.2024).

16. Балакин, Д.А. Особенности Закона о кибербезопасности Китайской Народной Республики 2017 г. и международная реакция на его принятие / Д.А. Балакин, А.Р. Аликберова – Текст: электронный // Современные Востоковедческие исследования. – 2023. − № 5. − URL: https://cyberleninka.ru/article/n/osobennosti-zakona-o-kiberbezopasnosti-kitayskoy-narodnoy-respubliki-2017-g-i-mezhdunarodnaya-reaktsiya-na-ego-prinyatie (дата обращения: 13.10.2024).

17. В Сеть утекли почти 3 млрд записей с личными данными жителей США, Канады и Великобритании – Текст: электронный // CNews, 2024. − URL: https://www.cnews.ru/news/top/2024-08-20_podtverzhdena_utechka_pochti (дата обращения: 14.10.2024).

18. Зиновьева, Е.С. Цифровые международные отношения. Том 2. Сборник документов / Е.С. Зиновьева, С.В. Шитьков. – Москва: Аспект Пресс, 2023. – С.430-431.

19. Коньков, С. Кибератака мирового масштаба: вирус WannaCry и как от него защититься / С. Коньков – Текст: электронный // ТАСС, 2017. − URL: https://tass.ru/proisshestviya/4248806 (дата обращения: 14.10.2024).

20. Чекменева, Т.Г. Стратегия Китая по обеспечению информационной безопасности: политический и технический аспекты / Т. Г. Чекменева, Б.А. Ершов, С.Д. Трубицын, А.А. Остапенко – Текст: электронный // «Bulletin Social-Economic and Humanitarian Research». – 2020. − № 7. – URL: https://cyberleninka.ru/article/n/strategiya-kitaya-po-obespecheniyu-informatsionnoy-bezopasnosti-politicheskiy-i-tehnicheskiy-aspekty (дата обращения: 12.10.2024).

21. Dutta, S. Global Innovation Index 2023. Innovation in the face of uncertainty. 16 Edition / S. Dutta, B. Lanvin, L. R. León, S. Wunsch-Vincent – Text: online. − URL: https://www.wipo.int/edocs/pubdocs/en/wipo-pub-2000-2023-en-main-report-global-innovation-index-2023-16th-edition.pdf (дата обращения: 12.10.2024).

22. Swansan, A. U.S. Tightens China’s Access to Advanced Chips for Artificial Intelligence / A. Swansan – Text: online // The New York Times, 2023. − URL: https://www.nytimes.com/2023/10/17/business/economy/ai-chips-china-restrictions.html (дата обращения: 14.10.2024).

Елизавета Максимовна Корних,
студентка 4-го курса, Юридический факультет,
Институт права и национальной безопасности,
РАНХиГС при Президенте РФ,
E-mail: Lizoki7956@mail.ru

Elizaveta M. Kornikh,
fourth-year Student, Faculty of Law,
Institute of Law and National Security,
RANEPA under the President of the Russian Federation,
E-mail: Lizoki7956@mail.ru

DEEPFAKES КАК УГРОЗА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
DEEPFAKES AS A THREAT TO INFORMATION SECURITY

Аннотация. Изучен вопрос совершенствования механизма правового регулирования дипфейков в России как новой угрозы правам человека в условиях цифровизации и беспрецедентного роста вызовов и угроз в информационном пространстве. Эта тема представляет собой несомненную актуальность на данном этапе современного развития общества в эпоху бурного прогресса в области цифровых технологий с точки зрения обеспечения информационной безопасности, в частности защиты прав человека от угрожающего деструктивного воздействия дипфейков.

Ключевые слова: дипфейки, искусственный интеллект, дипфейк-технологии, права человека, киберпространство, нейросети, угроза информационной безопасности, виды дипфейков, нормативное регулирование дипфейков, ответственность за дипфейки, меры.

Abstract. The purpose of the study was to study the issue of improving the mechanism of legal regulation of diplomatic posts in Russia as a new threat to human rights in the context of digitalization and an unprecedented increase in challenges and threats in the information space. This topic is undoubtedly relevant at this stage of modern development of society in an era of rapid progress in the field of digital technologies from the point of view of ensuring information security, in particular, protecting human rights from the threatening destructive effects of deepfakes.

Keywords: deepfakes, artificial intelligence, deepfake technologies, human rights, cyberspace, neural networks, threat to information security, types of deepfakes, regulatory regulation of deepfakes, responsibility for deepfakes, measures.

Определение понятия «дипфейк» как нового явления в киберпространстве. В английском языке есть термин «deep learning», под которым обычно подразумевается глубокий метод машинного обучения, основанный на использовании нейросетей [3, 14]. Под термином «fake», в свою очередь, обычно подразумевается подделка или фальшивка. Таким образом, под дипфейком можно рассматривать некоторое соединение изображений, видео и звука, которое генерируется благодаря возможностям искусственного интеллекта с целью искажения исходной информации.

В конце 2017 года впервые данный термин появился в достаточно широком цифровом пространстве, тогда он стал производным он никнейма «Deepfakes», принадлежавшего одному из пользователей известного по всему миру онлайн-форума Reddit. Данный пользователь использовал различные возможности кодинга и машинного обучения для формирования порнографических роликов с лицами звезд шоу-бизнеса [5]. На современном этапе данный термин пока еще не получил какого-либо определения с технической точки зрения, которое использовалось бы во всем мире. Более того, искомое понятие в реалиях современной России не прописано в действующем на сегодняшний день законодательстве, т.е. оно не имеет юридического оформления [2, 75].

Виды дипфейков в зависимости от методов их создания. На сегодняшний день можно выделить несколько следующих видов дипфейков: смена лица («face swaps»), синхронизация губ («lip-syncing»), клонирование голоса («voice cloning»), синтез изображений, генерация текста и подрисовывание («inpainting») [5].

Анализ российского законодательства, регламентирующего дипфейк-технологии. В реалиях современной России на законодательном уровне

определен порядок ограничения доступа к информации, которая ранее была распространена с нарушением тех или иных правил, что регламентировано статьей 15.3 ФЗ № 149 «Об информации, информационных технологиях и о защите информации» [1, 3-4].

Более того, при распространении в публичном поле заведомо ложной информации, которая при определенных обстоятельствах может представлять угрозу и повлечь тяжкие последствия для жизни и безопасности граждан, а также обществу в целом, виновные понесут наказание по ст. 207.1 и 207.2 УК РФ. Распространение фейковых новостей, в свою очередь, в качестве ответственности имеет установленное наказание по ст. 13.15 КоАП РФ.

Несмотря на всю серьезность рассматриваемой проблемы, особенно в ИКТ-среде, по закону с распространением дипфейков можно бороться на основе ч. 1 ст. 152.1 ГК РФ, регламентирующей охрану изображения граждан Российской Федерации. Однако простые фото или видео в значительной степени не сопоставимы с дипфейками, поскольку вторые позволяют подорвать репутацию граждан.

По мнению кандидата юридических наук А. Киселева, возможностей для порочения чести и достоинства, и незаконного обогащения на современном этапе в РФ достаточно много в силу того, что данная область законом почти не регулируется [4, 5, 6]. Именно поэтому в Государственную Думу РФ 16 сентября 2024 года был внесен законопроект, предусматривающий наложение уголовной ответственности за создание и использование дипфейков. В соответствии с данным законопроектом, в УК РФ вводятся изменения в ряд статей: «Клевета», «Мошенничество», «Кража», «Вымогательство» и «Мошенничество в сфере компьютерной информации». Также законопроект вносит новый квалифицирующий признак «Причинение имущественного ущерба путем обмана или злоупотребления доверием».

Дипфейки как угроза информационной безопасности. Потенциально дипфейки действительно могут стать крупнейшей угрозой в области информационной безопасности по всему миру [6]:

1. Прежде всего, использование подобных технологий позволяет генерировать контент с якобы реальными событиями, по результатам создания которого злоумышленники могут распространять фейки и вводить широкую общественность в заблуждение.

2. Экономические гиганты, вроде крупных компаний, потенциально могут понести значительные убытки в рамках своей репутации в случаях, когда подотчетные им лица станут жертвами дипфейков.

3. Равным образом доверие к власти может упасть в самой серьезной степени, поскольку дипфейки позволяют генерировать контент с политиками, в частности первого звена, на которых они будут совершать противоправные, либо иные порочащие честь и достоинство личности действия.

Меры по противодействию вредоносным дипфейк-технологиям. Следовательно, на современном этапе существует необходимость по противодействию созданию и распространению дипфейков, прежде всего, в правоприменительной практике. Рассмотрим некоторые возможные меры:

1. Нормативное закрепление «дипфейка» со всеми сопутствующими данному явлению деталями. Например, термин «дипфейк» в российском законодательстве можно рассматривать в качестве ложного материала, который ранее был сформирован на основе использования ИИ-технологии с совокупности с машинным обучением и иными инструментами соответствующего характера.

2. Законодательство в административном, а также в уголовном направлении также необходимо будет подкрепить определенного рода дополнениями, которые будут касаться рассматриваемых материалов ложного характера. В УК РФ, в частности, есть ст. 207.1, в которую можно включить дополнительные сведения о дипфейках.

3. Дополнение ст. 152 и 152.1 ГК РФ, в рамках которого будет регламентировано, что в случае искусственного создания дипфейков с целью порочения чести и достоинства тех или иных лиц, виновные будут привлекаться к соответствующей ответственности. Также предлагается

дополнить ГК РФ полноценной статьей, регламентирующей процесс наследования цифрового образа личности.

4. Верификация материалов, которые размещаются в сети, на предмет нахождения в них дипфейков, также является одним из возможных решений. Разработка и тестирование определенного механизма с целью создания алгоритма, который будет отслеживать и верифицировать контент, сформированный при использовании дипфейк-технологий.

5. Подготовка норм профильного законодательства, которые в дальнейшем позволят регулировать системы искусственного интеллекта, робототехники и виртуальной реальности. В результате такие нормы позволят регламентировать возможности использования ИИ-технологий в тех или иных общественных отношениях. Так, например, можно считать вполне уместным принятие Цифрового кодекса РФ.

Заключение. Таким образом, можно сделать вывод, что необходимо совершенствование механизма правового регулирования дипфейков в России – как новой угрозы правам человека в условиях цифровизации и беспрецедентного роста вызовов и угроз в мировом информационном пространстве. Разработка законодательства, включающего в себя понятийный аппарат и меры ответственности за недобросовестное и противоправное поведение с ИИ позволит минимизировать угрозу деструктивного воздействия дипфейков и возможность нарушения прав граждан, повысить уровень обеспечения информационной безопасности.

Список источников и литературы:

1. Ващенко Д.Г. К вопросу о правовом регулировании дипфейков / Д.Г. Ващенко, Э.А. Оруспай, О.Г. Степаненко // Вопросы науки и образования. – 2023. – № 7 (172). – С. 1-6.

2. Игнатенков Г.К. Технология дипфейк как угроза информационной безопасности / Г.К. Игнатенков // Наука. Исследования. Практика: сборник избранных статей по материалам Международной научной конференции,

Санкт-Петербург, 25 июня 2022 года. – Санкт-Петербург: Издательство Гуманитарного национального исследовательского института «Нацразвитие», 2022. – С. 74-77.

3. Игнатьев А.Г. Дипфейки в цифровом пространстве: основные международные подходы к исследованию и регулированию / А.Г. Игнатьев, Т.А. Курбатова. – Москва: АНО «Центр компетенций по глобальной ИТ-кооперации», 2023. – 54 с.

4. Киселев А.С. О необходимости правового регулирования в сфере искусственного интеллекта: дипфейк как угроза национальной безопасности / А.С. Киселев // Вестник Московского государственного областного университета. Серия: Юриспруденция. – 2021. – № 3. – С. 54-64.

5. Аферы с дипфейками: какие угрозы скрываются за искусственными лицами? [Электронный ресурс]. – URL: https://www.security-lab.ru/blog/company/PandaSecurityRus/351217.php. (дата обращения: 30.09.2024).

6. Мошенник подделал голос CEO и украл $243 тыс. при помощи технологии «deepfake» [Электронный ресурс]. – URL: https://incrussia.ru/news/deepfake-moshennik-ukral-243-tys/. (дата обращения: 30.09.2024).

Ольга Владимировна Моисеева,
Студент, Институт стран Азии и Африки,
МГУ имени М.В. Ломоносова,
E-mail: moiseevao04@mail.ru

Olga V. Moiseeva,
Undergraduate student, Institute of Asian and African Studies,
Moscow State University,
E-mail: moiseevao04@mail.ru

СРАВНЕНИЕ ОСНОВНЫХ ТЕНДЕНЦИЙ В РАЗВИТИИ СИСТЕМ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РОССИИ И КИТАЕ

COMPARISON OF THE MAIN TRENDS IN THE DEVELOPMENT OF INFORMATION SECURITY SYSTEMS IN RUSSIA AND CHINA

Аннотация. Настоящее исследование направлено на проведение сравнительного анализа тенденций развития информационной безопасности в России и Китае. Рассмотрены стратегии двух стран по данному аспекту, а также проанализированы выступления глав государств, касающиеся вопросов информационной безопасности и международного сотрудничества в этой сфере.

Ключевые слова: информационная безопасность, кибератака, кибербезопасность, международное сотрудничество, Китай, Россия, развитие информационных технологий, тенденции развития систем информационной безопасности.

Abstract. This study is aimed at conducting a comparative analysis of information security trends in Russia and China. The strategies of the two countries on this issue are considered, as well as the speeches of the heads of state on information security issues and international cooperation in this area are analyzed.

Keywords: information security, cyber attacks, cybersecurity, international cooperation, China, Russia, information technology development, trends in the development of information security systems.

Перспективы развития информационной безопасности в России. На 2024 год Россия и Китай входят в тройку наиболее зараженных кибератаками стран по данным «Лаборатории Касперского» [2]. В связи с этим обеспечение кибербезопасности и информационной безопасности является одним из приоритетных направлений внутренней и внешней политики в обеих странах.

О дальнейшем планировании развития системы информационной безопасности можно говорить на основе стратегий, публикуемых правительствами стран. В 2017 году в РФ был принят Указ Президента №203 «О Стратегии развития информационного общества в Российской Федерации на 2017 − 2030 годы» [6]. В стратегии признается, что в России отсутствуют отечественные разработки технологий анализа больших объемов данных. К основным целям стратегии относятся: создание и применение российских технологий в информационной и коммуникационных сферах; обеспечение перехода государственных органов к использованию инфраструктуры электронного правительства; обеспечение использования российских «средств шифрования при электронном взаимодействии» госорганов между собой, гражданами и организациями; замена импортного оборудования и программного обеспечения российскими аналогами [5]. Также планируется усовершенствовать безопасность Рунета (русскоязычный сегмент Интернета) путем отслеживания страновой принадлежности всех сетей и отключения аудитории от ресурса в случае возникшей атаки [3]. При этом в рамках Рунета создаются аналоги иностранных сервисов (например, онлайн-кинотеатры Кинопоиск, Okko и др. заменили недоступный на территории РФ онлайн-кинотеатр Netflix).

Число кибератак на российские структуры увеличилось после начала специальной военной операции. На заседании Совета Безопасности в 2022 году Президент РФ В.В. Путин отметил, что против России «развязана война в информационном пространстве» [4]. В том числе по этой причине с 1 января 2025 использование зарубежного программного обеспечения

государственными органами и госзаказчиками на критической инфраструктуре будет полностью запрещено [7].

Основные тенденции в области обеспечения информационной безопасности в Китае. По сообщению агентства Синьхуа, Председатель КНР Си Цзиньпин в июле 2023 года на Национальной конференции по кибербезопасности отметил необходимость руководствоваться концепцией построения социализма с китайской спецификой в новую эпоху при наращивании «киберсилы». В речи члена Постоянного комитета Политического бюро ЦК КПК Цай Ци на конференции несколько раз говорится о необходимости выстраивания барьера безопасности в киберпространстве Китая, что, вероятно, относится к укреплению Великого китайского файрвола [9]. Стоит отметить, что в рамках проекта Великого китайского файрвола в Китае уже созданы аналоги большинства иностранных сервисов, таких как поисковая система Baidu (аналог Google), мессенджер WeChat (аналог WhatsApp [3]), платформа онлайн-продаж TaoBao (аналог Amazon[4] и Ebay).

В феврале 2024 года был опубликован трехлетний план по усилению защиты данных промышленных предприятий [10]. К концу 2026 года планируется повысить осведомленность о защите данных, усовершенствовать систему предотвращения рисков кибератак и контроля за ними, тем самым значительно повысить уровень защиты предприятий.

Международному сотрудничеству в сфере информационной безопасности китайское правительство также уделяет большое внимание. В 2022 году была опубликована Белая книга «Совместное создание сообщества единой судьбы в киберпространстве» [1]. В документе отмечается, что развитие интернета и кибербезопасность являются неотъемлемой частью формирования сообщества единой судьбы человечества.

[3] Принадлежит организации Meta, которая признана в РФ экстремистской и запрещена.
[4] Заблокирован Роскомнадзором в связи с отказом выполнить требования закона о «приземлении», который требует от крупных зарубежных IT-компаний создать представительства в РФ.

Сходства и различия в политике России и Китая. В связи с постоянным ростом киберугроз в обеих странах особое внимание уделяется развитию отечественных технологий: разрабатываются отечественные программные обеспечения, технологии искусственного интеллекта и суперкомпьютеров. В России новые технологии находятся на этапе разработки, однако появление отечественных ПО необходимо в силу запрета на использование некоторых иностранных ПО государственными структурами и задачи развивать технологический суверенитет страны. Наблюдается технологическая отсталость по сравнению с другими крупными государствами (КНР, США). Китай же является одним из мировых лидеров по компьютерным технологиям, будучи практически полностью технологическим независимым от других государств.

В вопросах международного сотрудничества Россия и Китай призывают мировое сообщество соблюдать нормы международного права в ИКТ-среде, придерживаться принципа суверенитета страны в ней. При этом и Россия, и КНР не согласны с некоторыми подходами иностранных государств в данной сфере (обе страны не присоединились к Будапештской конвенции о киберпреступности 2001 года [8]), развивают координацию усилий в международных организациях (ООН, БРИКС, ШОС). Концепция конвенции по международной информационной безопасности ООН 2023 года была составлена Россией в соавторстве с некоторыми другими странами [3]. Китай же видит целью создать сообщество единой судьбы в киберпространстве.

Заключение. Перспективы развития информационной безопасности как в России, так и в Китае, связаны с ростом киберугроз и стремлением к технологическому суверенитету. Общей чертой политики обеих стран является фокус на совершенствование национальных технологий. Сотрудничество между странами в данной сфере открывает новые возможности как на двустороннем, так и на многостороннем уровнях, в том числе в рамках различных международных организаций.

Список источников и литературы:

1. В Китае опубликована Белая книга о сообществе единой судьбы в киберпространстве // Синьхуа [Электронный ресурс] − URL: http://russian.news.cn/20221107/9577cd5da3e7418b8d16019933a28df3/c.html (Дата обращения: 10.10.2024)

2. Интерактивная карта киберугроз Лаборатории Касперского // Лаборатория Касперского [Электронный ресурс] − URL: https://cybermap.kaspersky.com/ru/stats (Дата обращения: (10.10.2024)

3. Обновленная концепция Конвенции ООН об обеспечении международной информационной безопасности от 15.05.2023.

4. «Против России развязана настоящая война». Как она будет защищаться // Газета.ru [Электронный ресурс] − URL: https://www.gazeta.ru/politics/2022/05/20/14882558.shtml (Дата обращения: 10.10.2024)

5. Распоряжение Правительства РФ от 24.11.2023 N 3339-р «Об утверждении Стратегии развития отрасли связи Российской Федерации на период до 2035 года».

6. Указ Президента РФ от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017 − 2030 годы».

7. Указ Президента Российской Федерации от 30.03.2022 № 166 "О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации».

8. The Convention on Cybercrime (Budapest Convention, ETS No. 185) 2001 yr. // Council of Europe. Available at: https://www.coe.int/en/web/cybercrime/the-budapest-convention (Accessed: 14.10.2024)

9. Xi stresses advancing high-quality development of internet and information technology sector. Available at: http://english.www.gov.cn/news/202307/16/content_WS64b3f805c6d0868f4e8ddd2e.html (Accessed: 14.10.2024)

10. 四举措提升工业企业数据保护能力 = Четыре меры по повышению уровня защиты данных промышленных предприятий // Центральное народное правительство КНР [Электронный ресурс] − URL: https://www.gov.cn/lianbo/bumen/202402/content_6934376.htm (Дата обращения: 13.10.2024).

Алексей Вячеславович Ордин,
к.т.н., эксперт в области кибербезопасности,
ассистент, кафедра «Инженерная графика»,
Московский авиационный институт,
E-mail: alexey_ordin@mail.ru

Alexey V. Ordin,
Ph.D. in Engineering, Expert in Cybersecurity,
Assistant Professor, Department of Engineering Graphics,
Moscow Aviation Institute,
E-mail: alexey_ordin@mail.ru

SD-WAN КАК КЛЮЧЕВОЙ ФАКТОР ПОСТРОЕНИЯ КОМПЛЕКСНОЙ КИБЕРБЕЗОПАСНОСТИ В ГОСУДАРСТВАХ-ЧЛЕНАХ ЕАЭС
SD-WAN AS A KEY FACTOR IN BUILDING COMPREHENSIVE CYBERSECURITY IN THE EAEU MEMBER STATES

Аннотация. Статья посвящена роли программно определяемых сетей (SD-WAN) как ключевого инструмента в построении комплексной кибербезопасности в государствах-членах Евразийского экономического союза (ЕАЭС). В условиях увеличения киберугроз, SD-WAN предлагает возможность оптимизации сетевого трафика и интеграции различных систем безопасности. Рассматриваются основные преимущества SD-WAN, отсутствие единого международного стандарта, а также примеры внедрения решений от российских компаний, таких как Лаборатория Касперского и Bi.Zone. В статье также подчеркивается пионерская роль России в стандартизации SD-WAN на уровне ФСТЭК. В заключение отмечается, что интеграция SD-WAN в кибербезопасность станет важным шагом к созданию защищенной цифровой среды в регионе.

Ключевые слова: SD-WAN, кибербезопасность, ЕАЭС, интеграция систем безопасности, стандартизация, Лаборатория Касперского, Bi.Zone, ФСТЭК.

Abstract. The article focuses on the role of Software-Defined Wide Area Networks (SD-WAN) as a key tool for building comprehensive cybersecurity in the

member states of the Eurasian Economic Union (EAEU). In the context of increasing cyber threats, SD-WAN offers the capability to optimize network traffic and integrate various security systems. The main advantages of SD-WAN, the lack of a unified international standard, and examples of implementation from Russian companies such as Kaspersky Lab and Bi.Zone are discussed. The article also highlights Russia's pioneering role in the standardization of SD-WAN at the level of the Federal Service for Technical and Export Control (FSTEC). In conclusion, it is emphasized that the integration of SD-WAN into cybersecurity will be an important step toward creating a secure digital environment in the region.

Keywords: SD-WAN, Cybersecurity, EAEU, Integration of security systems, Standardization, Kaspersky Lab, Bi.Zone, FSTEC.

Введение. Современные вызовы в области кибербезопасности требуют от государств новых подходов и технологий, способных эффективно защищать информационные инфраструктуры. В условиях растущих угроз, связанных с кибератаками и утечками данных, программно определяемые сети (SD-WAN) становятся ключевым инструментом для повышения уровня безопасности в государствах-членах Евразийского экономического союза (ЕАЭС). В России данный подход только начинает активно внедряться, однако уже существует ряд значительных решений от компаний, таких как Лаборатория Касперского и Bi.Zone, которые открывают новые горизонты для интеграции кибербезопасности.

Программно определяемые сети (SD-WAN): основные концепции и преимущества. SD-WAN представляет собой архитектуру, которая использует программное обеспечение для управления и оптимизации сетевых соединений, что позволяет организациям гибко управлять своим сетевым трафиком. Основные преимущества SD-WAN включают:

1. Оптимизацию трафика: SD-WAN автоматически выбирает наиболее эффективные маршруты для передачи данных, что значительно улучшает производительность приложений.

2. Снижение затрат: использование недорогих широкополосных соединений для передачи данных вместо дорогих выделенных каналов позволяет сократить операционные расходы.

3. Гибкость и масштабируемость: возможность быстро добавлять новые подключения и интегрировать удаленные офисы без необходимости сложных процедур настройки.

Отсутствие единого стандарта SD-WAN. На международной арене не существует единого стандарта для SD-WAN. Однако два негосударственных объединения, MEF (Metro Ethernet Forum) и ONUG (Open Networking User Group), предлагают свои определения и рекомендации. Эти организации стремятся установить общие практики и критерии для внедрения SD-WAN, что подчеркивает важность стандартизации в этой области [1].

Общая информация о MEF. MEF (Metro Ethernet Forum) – это глобальный консорциум компаний, работающий над ускорением цифровой трансформации в сфере сетевых и облачных технологий. MEF разрабатывает стандарты, автоматизационные рамки и API, а также сертификации и программы выхода на рынок для содействия развитию предложений Network-as-a-Service (NaaS) и их внедрению в автоматизированные экосистемы. MEF является определяющим органом для бизнес- и операционных API в рамках Lifecycle Service Orchestration (LSO)**,** а также для сертификаций и стандартов сетевой связности и безопасности MEF 3.0. Членство в MEF предоставляет организациям доступ к ресурсам и возможностям, способствующим их развитию, включая сети и сотрудничество с ведущими игроками отрасли, доступ к стандартам и сертификатам, а также возможность влиять на направления развития индустрии.

SD-WAN как транспорт для интеграции систем кибербезопасности. Одним из важнейших аспектов внедрения SD-WAN является его способность интегрировать различные системы кибербезопасности, обеспечивая защиту данных на всех уровнях [6]. Благодаря централизации управления и возможности применения различных политик безопасности на уровне сети,

SD-WAN становится надежным транспортом для передачи данных между различными элементами системы кибербезопасности.

Решения от Лаборатории Касперского и Bi.Zone. В России существует несколько решений, которые активно используют концепцию SD-WAN для обеспечения безопасности. Например, Лаборатория Касперского предлагает интегрированные решения, которые позволяют организациям не только оптимизировать сетевой трафик, но и защитить свои данные от внешних угроз. Их технологии включают средства защиты от вирусов, шифрования и мониторинга трафика, что обеспечивает комплексный подход к безопасности.

Другим важным игроком на российском рынке является компания Bi.Zone**,** которая предлагает инновационные решения для обеспечения кибербезопасности. Их платформа позволяет интегрировать SD-WAN с существующими системами безопасности, обеспечивая непрерывный мониторинг и реагирование на инциденты.

Россия как пионер в стандартизации SD-WAN. Россия стала первой страной, которая подошла к решению проблемы комплексно и внедрила терминологию и сертификацию SD-WAN на уровне ФСТЭК (Федеральная служба по техническому и экспортному контролю). Это нововведение подчеркивает стремление к созданию безопасной и стандартной среды для использования SD-WAN в стране и, в конечном итоге, в государствах ЕАЭС [8].

Преимущества интеграции SD-WAN в кибербезопасность следующие:

1. Усиление защиты: SD-WAN позволяет создавать многоуровневую защиту, используя как облачные, так и локальные решения безопасности. Это значительно повышает устойчивость к кибератакам.

2. Упрощение управления: централизованное управление позволяет администраторам легко настраивать политики безопасности и управлять ими в реальном времени.

3. Аналитика и мониторинг**:** SD-WAN предлагает мощные инструменты для анализа сетевого трафика и выявления аномалий, что позволяет быстро реагировать на потенциальные угрозы.

Заключение. Внедрение SD-WAN в государствах-членах ЕАЭС представляет собой важный шаг к созданию комплексной системы кибербезопасности. Существующие решения от таких компаний, как Лаборатория Касперского и Bi.Zone, служат примером того, как можно эффективно интегрировать современные технологии для повышения уровня защиты данных. Поскольку угрозы в киберпространстве продолжают расти, использование SD-WAN станет ключевым фактором в построении надежной и безопасной инфраструктуры для организаций в регионе. Таким образом, внедрение программно определяемых сетей в качестве транспортной системы для интеграции решений кибербезопасности является необходимым шагом для обеспечения устойчивости и безопасности в цифровом пространстве государств-членов ЕАЭС. В условиях отсутствия единого международного стандарта, российская инициатива в области сертификации и терминологии SD-WAN может послужить образцом для других стран, стремящихся к созданию безопасной цифровой среды.

Список источников и литературы:

1. MEF. SD-WAN Service Standards. [Электронный ресурс]. Режим доступа: https://www.mef.net/service-standards/overlay-services/sd-wan/ (дата обращения: 21.10.2024).

2. Глушаков, С. В., Хачиров, Т. С., Соболев, Р. О. Секреты хакера. Защита и атака. − М.: БХВ-Петербург, 2008. − 416 с.

3. Зайцев, О. Rootkits, SpyWare/AdWare, Keyloggers & BackDoors. Обнаружение и защита. − М.: Эксмо, 2010. − 256 с.

4. Кузнецов, М., Симдянов, И. Социальная инженерия и социальные хакеры. − М.: Инфра-М, 2012. − 192 с.

5. Михайлов, Д. М., Жуков, И. Ю. Защита мобильных телефонов от атак. − М.: Русский фонд содействия образованию и науке, 2013. − 240 с.

6. Петренко, С. А., Курбатов, В. А. Политики безопасности компании при работе в интернет. − М.: Диалектика, 2014. − 208 с.

7. Шнайер, Б. Секреты и ложь. Безопасность данных в цифровом мире. − М.: Питер, 2007. − 352 с.

8. Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 N 187-ФЗ : принят Государственной Думой 12 июля 2017 года : одобрен Советом Федерации 19 июля 2017 года. URL: https://www.consultant.ru/document/cons_doc_LAW_220885/ (дата обращения: 21.10.2024).

Диана Альбертовна Пилюгина,
студент 2 курса магистратуры, факультет международных отношений,
Дипломатическая академия МИД России,
E-mail: deanna.pilyugina@yandex.ru

Diana A. Pilyugina,
Master's Degree Student, Faculty of International Relationships,
Diplomatic Academy of the Russian Foreign Ministry,
E-mail: deanna.pilyugina@yandex.ru

ПУТЬ РОССИИ К СУВЕРЕННОМУ ИНТЕРНЕТУ

RUSSIA'S WAY TOWARDS THE SOVEREIGN INTERNET

Аннотация. Данное исследование касается актуального вопроса о стратегии действий России в Интернете. На фоне продолжающегося с 2022 г. разрыва с западным рынком программного обеспечения нередко звучат предположения о том, что Россия могла бы двигаться к отделению Рунета от глобальной сети по китайской модели. В этой работе рассматриваются предпринятые Россией шаги по обеспечению Интернет-независимости и оценивается вероятность постепенной «китаизации» российского сегмента Интернета.

Abstract. This study dwells on the topical issue of Russia's strategy in the Internet. The gap with the Western software market, which continues since 2022, has instigated the discussion about the possibility of Russia's future move towards separating the Runet from the global network, like it has been done in China. The study examines the steps taken by Russia to ensure the independence of its Internet and assesses the likelihood of a gradual "Sinification" of its Russian segment.

Ключевые слова: информационная безопасность, кибербезопасность, Россия, Рунет, суверенный Интернет, закон о суверенном Интернете.

Keywords: informational security, cybersecurity, Russia, Runet, sovereign Internet, the Sovereign Internet Law.

Обновление подхода России к безопасности в сети Интернет. 1 октября 2014 года на заседании Совета Безопасности РФ Президент В.В.Путин заявил, что Россия не собирается контролировать или «огосударствливать» Интернет, но будет принимать меры по обеспечению устойчивости и безопасности Рунета [1]. Это заявление стало своего рода анонсом грядущего радикального изменения российского подхода к Интернету. Если до середины 2010-х этот подход строился преимущественно на тактике свободной конкуренции, то во второй половине прошлого десятилетия Россия впервые декларировала необходимость проведения границ в информационном пространстве.

2016-2020: первые шаги к суверенному интернету. В 2016 г. предметом широкой дискуссии стало принятие Федеральных законов №ФЗ-374 [6] и №ФЗ-375 [7], известных в медиа как «пакет Яровой». Пакет был ориентирован на ужесточение антитеррористических мер, однако наибольший общественный резонанс вызвали его положения, обязывавшие операторов в течение длительного срока хранить данные пользователей и предоставлять их правоохранительным органам по требованию. В медиасреде активно звучали обвинения в нарушении конституционного права на тайну переписки, в установлении государством «тотальной слежки». «Пакет Яровой» вошел в бытовой обиход как «мем».

Едва ли мог быть простым совпадением весомый ажиотаж вокруг внедрения закона, практически не оказывающего влияние на рядового пользователя, но делающего первые серьезные шаги по направлению к обеспечению независимости российской информационной среды. Возможно, этот случай является одним из примеров тактики информационной войны с использованием «мемов».

В 2019 г. был принят закон № 90-ФЗ, получивший неформальное наименование «закон о суверенном интернете» [5]. Этот нормативный акт обязал операторов связи предоставлять информацию в федеральные органы власти, а также предоставил Роскомнадзору возможность напрямую контролировать интернет-траффик. Согласно комментарию В.В.Путина,

«Закон о суверенном Рунете должен не допустить негативные последствия возможного отключения России от мировой Сети, которая управляется в основном из-за границы» [4].

Тенденции дальнейшей стратегии России в сети «Интернет». Возможна ли в России «китаизация» Интернета, создание своего локального автономного сегмента по образцу китайского? В 2021 г. Д.А.Медведев в интервью изданию «Интерфакс» ответил на вопрос о возможности отключения России от интернета: «Технологически для этого все готово. На законодательном уровне тоже все решения приняты, но… это непросто и этого бы очень не хотелось. Я пока, откровенно сказать, не вижу и признаков этого, потому что, по понятным причинам, это же обоюдоострое оружие» [2].

В силу нежелания информационно замыкаться, что неизбежно сказалось бы на темпах экономического и технологического развития, Россия продвигает на международной арене идеи создания альтернативного сети «Интернет» совместного информационно-коммуникативного сетевого кластера для ряда дружественных стран, например, под эгидой БРИКС. Как свидетельствуют опросы ВЦИОМ, российская общественность к этому была в целом готова и до того, как с началом специальной военной операции обострилось противостояние в информационном пространстве: в 2018 г. предложение России о создании независимого интернета в рамках границ стран-членов БРИКС нашло поддержку 58% россиян [3].

Но при этом складывается впечатление, что российские законодатели не спешат с этим, стремясь действовать постепенно и предельно «точечно». Этому есть немало причин, в частности технологических, начиная от необходимости доработки собственной конкурентоспособной операционной системы широкого гражданского применения и заканчивая недостаточным количеством «интеллектуальных трудовых ресурсов» – высокоуровневых специалистов в области информационных технологий. Эта работа активно ведется, однако требует больших финансовых вложений.

Необходимость «кибер-импортозамещения». Несмотря на постепенное обрывание связей с лидерами западного информационного рынка, Россия продолжает вести достаточно мягкую политику в интернете. Закрытие доступа к Meta[5], замедление YouTube и подобные меры ставят своей целью, с одной стороны, ограничить потребление гражданами нежелательного контента, но также вынудить западные компании не ориентироваться на российский рынок, «расчистить пространство» для импортозамещения в информационной среде.

К сожалению, «информационное импортозамещение» продвигается с затруднениями: сказывается нехватка опыта конкуренции в киберсфере. Имея не так много удобных российских аналогов для требуемого программного обеспечения, многие россияне продолжают пользоваться зарубежными продуктами. Так, например, онлайн-форма обучения в школах и значительной части высших учебных заведений до недавнего времени проходила на платформах Zoom и Skype, принадлежащих недружественным странам.

Заключение. Высказывания высших лидеров России позволяют заключить, что отделение российского сегмента интернета не входит в список ближайших приоритетов. Что касается долгосрочного планирования, то стратегия действий России в информационной среде напрямую будет зависеть от конфигурации геополитических сил, которая сложится непосредственно по итогам текущего глобального противостояния; по-видимому, эта стратегия будет еще не раз скорректирована.

Список источников и литературы:

1. Гуржий, Д. А. Цензура в интернете / Д. А. Гуржий // Молодой ученый. — 2015. — № 12 (92). — С. 988-991. — URL: https://moluch.ru/archive/92/20439/ (дата обращения: 15.10.2024).

[5] Организация Meta, а также её продукты Instagram и Facebook, признаны экстремистскими на территории РФ.

2. Дмитрий Медведев: считаю Навального политическим проходимцем, который стремится залезть во власть // Интерфакс: [сайт]. – 2021. – URL: https://www.interfax.ru/russia/748522 (дата обращения: 09.10.2024)

3. Независимый от США интернет: иллюзия или реальность? // ВЦИОМ. Новости. – 2018. – URL: https://wciom.ru/analytical-reviews/analiticheskii-obzor/nezavisimyj-ot-ssha-internet-illyuziya-ili-realnost?ysclid=m269xbvcpx904613035 (дата обращения 11.10.2024).

4. Путин разъяснил понятия суверенного и свободного интернета // РБК: [сайт]. – 2019. – URL: https://www.rbc.ru/rbcfreenews/5dfb77e99a79472644d761d7 (дата обращения: 12.10.2024)

5. Федеральный закон от 01.05.2019 № 90-ФЗ «О внесении изменений в Федеральный закон «О связи» и в Федеральный закон «Об информации, информационных технологиях и защите информации» [Электронный ресурс]: [одобрен Советом Федерации 22 апреля 2019 г.] (дата обращения: 10.10.2024)

6. Федеральный закон от 06.07.2016 г. № 374-ФЗ «О внесении изменений в Федеральный закон «О противодействии терроризму» и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности», 2016 [Электронный ресурс]: [одобрен Советом Федерации 29 июня 2016 г.] (дата обращения: 10.10.2024)

7. Федеральный закон от 06.07.2016 г. № 375-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности», 2016 [Электронный ресурс]: [одобрен Советом Федерации 29 июня 2016 г.] (дата обращения: 10.10.2024)

Николай Васильевич Пичугин,
Мл.н.с., Центр политических исследований и прогнозов,
Институт Китая и современной Азии РАН,
Член исполнительной дирекции Школы МИБ ИАМП,
E-mail: nikolaivpichugin@gmail.com

Nikolay V. Pichugin,
Junior researcher, Center for Political Research and Forecasts,
Institute of China and Contemporary Asia
of the Russian Academy of Sciences,
Member of the Executive Board
of the School of International Information Security
of the Institute of Contemporary International Problems
E-mail: nikolaivpichugin@gmail.com

6-УРОВНЕВАЯ ПАРТИЙНО-ГОСУДАРСТВЕННАЯ СИСТЕМА УПРАВЛЕНИЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КНР

6-LEVEL PARTY-STATE SYSTEM DEPARTMENT OF INFORMATION SECURITY OF THE PEOPLE'S REPUBLIC OF CHINA

Аннотация. Настоящее исследование направлено на систематизацию партийно-государственной системы управления обеспечения информационной безопасности Китайской Народной Республики (далее: КНР). Выделены 6 уровней регулирования, дана краткая характеристика их функционирования на институциональном уровне.

Ключевые слова: партийно-государственная система управления, квазигосударственные структуры, делегирование регулирующих функций, нормативно-правовое регулирование, подзаконные акты, Китай, информационная безопасность.

Abstract. This article is aimed to systematize the party-state management system for ensuring information security in the People's Republic of China (hereinafter: PRC). Six levels of regulation are identified, and a brief description of their functioning at the institutional level is given.

Keywords: party-state system of governance, quasi-state structures, delegation of regulatory functions, legal regulation, subordinate legal acts, China, information security.

Система партийно-государственного управления в рамках 14 пятилетнего плана [3] и Всестороннего плана построения цифрового Китая [4], наряду с «цифровой инфраструктурой», рассматривается в качестве «институциональной базы», обеспечивающей конкурентное преимущество в борьбе за мировое лидерство в цифровом пространстве, которое необходимо продолжать развивать.

Первый уровень – партийное регулирование. Членами Комиссии ЦК КПК по кибербезопасности и информатизации, председателем которой является непосредственно Си Цзиньпин, определяются приоритетные направления развития системы информационной безопасности и цифрового развития КНР, которые затем оформляются сотрудниками Управления по делам кибербезопасности КНР в подзаконные акты, такие как Всесторонний план построения цифрового Китая (2023) [4], Положение об управлении дипфейками (2023) [2], Меры по управлению национальными службами аутентификации личности (проект для обсуждения от 2024) [1]. Управление является «учреждением с двумя вывесками», одновременно выполняющее роль канцелярии Центральной комиссии, а также входящее в число ведомственных подразделений Госсовета под названием Государственной канцелярии по делам сетевой информации, таким образом, выступая в качестве связующего звена с профильными государственными органами [5]. Оно является одной из основных площадок для обсуждения наиболее значимых будущих законов КНР, регулирующих китайское цифровое пространство. Плановые и подзаконные документы, обнародованные на данном уровне, де факто, имеют статус закона.

Второй уровень – государственное регулирование. Сотрудники Министерства промышленности и информационных технологий КНР

(МПИТ), Министерства государственной безопасности КНР (МГБ) и Министерства общественной безопасности КНР (МОБ) ответственны за выполнение постановлений, принятых на партийном уровне. Основными функциями МПИТ выступают обеспечение управления и развития информационно-коммуникационных технологий (ИКТ), информатизации и частично электронной коммерции в Китае, а также реализация ряда задач в сфере связи, телекоммуникаций и радиоуправления [6]. Его сотрудники одновременно участвует в координации и управлении орбитальными позициями космических спутников, предполагающее взаимодействие с структурами Народно-освободительной армии Китая (НОАК).

В зону ответственности МГБ входит обеспечение внешней разведки, проведение как оборонительных, так и наступательных операций в информационном пространстве. Во внутренней структуре Министерства следует выделить 13-е научно-техническое бюро разведывательных технологий, отвечающее за управление и разработку соответствующего оборудования для технических расследований, и 14-е бюро технической разведки [7], должностными обязанностями сотрудников которого являются телекоммуникационная инспекция и разведка.

Среди институциональных и функциональных обязанностей МОБ следует выделить: проведение расследований и рассмотрение уголовных дел в области прав интеллектуальной собственности (ИС), координацию и проведение защитных мер для обеспечения информационной безопасности, организацию выполнения научно-технических работ в области общественной безопасности, включая технологии больших данных и ИКТ [5]. Ведомственным подразделением Министерства является Сетевая полиция, о создании которой было официально объявлено в 2015 году. Её подразделения действуют на провинциальном и городских уровнях. По мере развития китайского законодательства в области защиты прав ИС, деятельность сотрудников Сетевой полиции приобрела открытый характер.

Третий уровень – квазигосударственное регулирование. В число квазигосударственных структур [6] входят как ведомства, непосредственно выполняющие работы в интересах Управления по делам киберпространства КНР и трёх указанных министерств, так и профильные организации, формально обладающие статусом неправительственных и некоммерческих. Подобные структуры могут аккумулировать в себе основные профильные китайские компании, выступая в качестве переговорных площадок между партийно-государственным аппаратом, бизнесом и научным сообществом. Квазигосударственные организации участвуют в процессах подготовки отраслевых стандартов, сертификации и патентирования, а также проводят образовательные компании и мероприятия среди китайских компаний и граждан, в том числе, на коммерческой основе.

Четвёртый уровень – регулирование в рамках отдельных компаний. Китайские корпорации вынуждены самостоятельно создавать департаменты, ответственные как за обеспечение внутренней информационной безопасности, так и за цензуру данных, публикуемых в китайском сегменте сети Интернет. Указанному факту способствуют строгие санкции за несоблюдение регулирующих информационную безопасность в КНР законов и подзаконных актов. Одновременно в подобных нормативно-правовых актах используются размытые формулировки и принцип коллективной ответственности за нарушения [8], что также стимулирует китайские компании к внедрению механизмов саморегулирования.

Пятый уровень – общественное регулирование. Оно обеспечивается, во-первых, за счёт поддержания большого числа площадок для обратной связи

[6] Примечание: Отличительными особенностями квазигосударственных организаций являются преимущественно узкий профиль деятельности, а также широкие возможности для обратной связи с китайскими гражданами. Их фактическая подчинённость партийным и государственным органам, как правило, либо зафиксирована в учредительных документах, либо прослеживается в руководящем составе. В качестве примера можно привести Центр по выявлению нездоровой и незаконной информации (Управление по делам кибербезопасности КНР), Китайский научно-исследовательский институт развития электронно-информационной индустрии (МОБ), Центр оценки рисков информационной безопасности КНР (МГБ), относятся Ассоциация кибербезопасности Китая, Интернет-сообщество Китая, Китайский фонд развития Интернета.

китайских граждан на первых трёх указанных уровнях регулирования. Во-вторых, благодаря существующей в Китае исторически устоявшейся практике информирования властей гражданами о фактах нарушения законодательства, которая на системном уровне поддерживается партийно-государственным аппаратом. Таким образом, ряд угроз информационной безопасности удаётся локализовать на ранних этапах. Специализированные площадки для обратной связи в онлайн-формате, например, существуют в Управлении по делам киберпространства КНР (1-й уровень), МОБ (2-й уровень), Ассоциации кибербезопасности Китая (3-й уровень).

Шестой уровень – международное регулирование. Оно обеспечивается 2 основными факторами. Во-первых, с помощью формирования и развития собственных международных платформ, (Всемирная интернет-конференция, проводящаяся в городе Вучжэнь) и проектов (Цифровой шёлковый путь). Во-вторых, путём стимулирования китайских квазигосударственных структур к активному участию в существующих международных организациях. В результате китайская модель нормативно-правового регулирования цифрового пространства, а также технологические продукты и решения в области информационной безопасности продвигаются среди заинтересованных государств. Одновременно обеспечивается хеджирование рисков от введения санкций на отдельно взятые ИТ-корпорации, такие как Huawei, поскольку их интересы продолжают реализовываться на международном уровне посредством членства в квазигосударственных организациях-альянсах.

Заключение. Китайская 6-уровневая модель управления системой обеспечения информационной безопасности, во-первых, обеспечивается делегированием регулирующих функций со стороны партийно-государственного аппарата квазигосударственным структурам, компаниям и обществу при сохранении централизации власти. Во-вторых, благодаря особенностям нормативно-правовой системы КНР, происходит стимулирование саморегулирования на 4 и 5 уровнях. При этом, деятельность

квазигосударственных организаций может осуществляться, в том числе, на коммерческой основе. В совокупности, указанный подход позволяет экономить государственные средства и ресурсы, а также локализовывать угрозы информационной безопасности на ранних этапах. Одновременно китайское руководство способствует расширению профильного международного сотрудничества, продвигая собственную систему регулирования среди заинтересованных стран, а также обеспечивая хеджирование рисков санкций, за счёт привлечения китайских ИТ-корпораций к участию в международных организациях как отдельно, так и в составе различных отраслевых организаций и альянсов.

Список источников и литературы:

1. 《国家网络身份认证公共服务管理办法（征求意见稿）》 [Электронный ресурс] // официальный Управления по делам киберпространства КНР. 26.07.2024. URL: https://www.cac.gov.cn/2024-07/26/c_1723675813897965.htm (дата обращения: 11.10.2024)
2. 《互联网信息服务深度合成管理规定（征求意见稿）》 [Электронный ресурс] // официальный Управления по делам киберпространства КНР. 28.01.2022. URL: http://www.cac.gov.cn/2022-01/28/c_1644970458520968.htm (дата обращения: 11.10.2024)
3. 《十四五》国家信息化规划 [Электронный ресурс] // официальный сайт Управления по делам киберпространства КНР. 27.02.2023. URL: http://www.cac.gov.cn/2021-12/27/c_1642205314518676.htm (дата обращения: 11.10.2024)
4. 中共中央国务院印发《数字中国建设整体布局规划》 [Электронный ресурс] // Агентство Синьхуа. 27.12.2021. URL: http://www.gov.cn/zhengce/2023-02/27/content_5743484.htm (дата обращения: 11.10.2024)

5. 中共中央印发《深化党和国家机构改革方案》[Электронный ресурс] // 新华网 Агентство Синьхуа. URL: https://baike.baidu.com/reference/4179928/f0f1lTl5ShjN-gBevQ73zF70U-F-t6mUFssv7ZD4hWJ3vWvIlPqZP8iDpAyHWAdmupiuFYUWTnD1-N8KVZPY51N5QricNakhDu_9ysQGyz2synkCW_h_doZZ (дата обращения: 11.10.2024)

6. 中华人民共和国工业和信息化部 [Электронный ресурс] // официальный сайт Министерства промышленности и информационных технологий КНР. 16.09.2015. URL: https://web.archive.org/web/20160730001506/http://www.miit.gov.cn/n1146285/c3722500/content.html (дата обращения: 11.10.2024)

7. Кашин В. Б., Кокошин А. А. О подходах руководства КНР и китайских силовых структур к противоборству в киберпространстве //Военная мысль. – 2022. – №. 6. – С. 119-127.

8. Трощинский П. В., Молотников А. Е. Особенности нормативно-правового регулирования цифровой экономики и цифровых технологий в Китае //Правоведение. – 2019. – Т. 63. – №. 2. – С. 309-326.

Руслан Насимович Шангараев,
доктор политических наук, доцент, профессор кафедры стратегических коммуникаций и государственного управления,
Дипломатическая академия МИД России,
E-mail: shang143@mail.ru

Ruslan N. Shangaraev,
Doctor of Science, Professor,
Associate Professor, Department of Strategic Communications and Public Administration,
Diplomatic Academy of the Russian Foreign Ministry,
E-mail: shang143@mail.ru

ОСОБЕННОСТИ ФУНКЦИОНИРОВАНИЯ СИТУАЦИОННЫХ ЦЕНТРОВ В АМЕРИКЕ

FEATURES OF FUNCTIONING OF SITUATION CENTERS IN AMERICA

Аннотация. Практика применения ситуационного центра как механизма управления в США распространена крайне широко. Ситуационными центрами в стране располагают как органы государственной власти федерального и регионального масштабов, так и большинство муниципалитетов, частные компании и некоммерческие организации.

Abstract. The practice of using the situation center as a management mechanism in the United States is extremely widespread. Situation centers in the country are available both to state authorities of federal and regional levels, as well as to most municipalities, private companies and non-profit organizations.

Ключевые слова: ситуационные центры, Ситуационный центр Президента США, Ситуационная комната Белого Дома, Президентский оперативный центр по чрезвычайным ситуациям, Оперативный центр Государственного департамента США, информационная и аналитическая поддержка, национальная безопасность, Совет национальной безопасности, программно-аппаратное обеспечение.

Keywords: situation centers, Situation Center of the President of the United States, Situation Room of the White House, Presidential Emergency Operations Center, Situation Center of the US Department of State, information and analytical support, national security, National Security Council, software and hardware

Взаимодействие между ситуационными центрами органов государственной власти страны выстроено достаточно тесно, при этом функционирование системы взаимодействия ориентировано на информационную и аналитическую поддержку главы государства в процессе принятия внутри- и внешнеполитических решений. Президентский характер формы правления США предопределил центрирование системы ситуационного управления на главе государства. В непосредственном распоряжении Президента США имеется два таких органа – Ситуационный центр Президента США и Президентский оперативный центр по чрезвычайным ситуациям.

Ситуационный центр Президента США – (другое устоявшееся наименование – «Ситуационная комната Белого Дома», «Комната») представляет собой пункт наблюдения и связи, функционирующий в круглосуточном режиме, обеспечивающий Президента, Помощника по национальной безопасности и членов Совета безопасности США информацией открытого и закрытого характера для выработки и реализации политики в области национальной безопасности [1]. «Комната» обслуживается персоналом Совета национальной безопасности (30 чел.), каждый из которых имеет опыт работы в различных ведомствах или службы в вооруженных силах или спецслужбах. В «комнате» функционируют дежурные смены, обеспечивающие круглосуточное наблюдение за ситуацией в мире и информирование руководства страны о значимых событиях. Ежедневно дежурная смена готовит информационную сводку, проводит краткий брифинг для Президента США. «Комната» располагает всем необходимым программно-аппаратным обеспечением, которое регулярно модернизируется.

Последнее переоборудование состоялось в 2023 г., стоимость работ составила 50 млн долл. США [2]. Следует отметить, что «Комната» предназначена для функционирования в штатных условиях в оперативном режиме. На случай возникновения чрезвычайной ситуации, напрямую угрожающей безопасности первых лиц, комплексное ситуационное управление осуществляется с использованием Президентского оперативного центра по чрезвычайным ситуациям, который также служит укрытием для высшего руководства США. Как уже отмечалось выше, «Ситуационная комната Белого дома» и Президентский оперативный центр по чрезвычайным ситуациям являются частью разветвленной системы органов ситуационного управления, ключевую роль в которой играют оперативные центры (англ. Operations Centre – термин, применяемый в структуре государственного управления США для обозначения структурных подразделений ведомств, схожих по предназначению и набору решаемых задач с отечественными ситуационными центрами).

В качестве еще одного примера рассмотрим более детально ситуационный центр внешнеполитического ведомства страны – Оперативный центр Государственного департамента США. Центр, изначально созданный в 1960-х гг. с целью упрощения процессов мониторинга международной ситуации в условиях Карибского кризиса, соответствующей аналитической и технической поддержки принятия шагов американской стороны в отношении его урегулирования, впоследствии был должным образом доработан и модернизирован, обеспечив масштабирование своей работы на все направления внешней политики США. Центр функционирует в составе Исполнительного секретариата ведомства и насчитывает ок. 100 действующих сотрудников [3]. Структурно ОЦ включает в себя следующие подразделения:

1. Группа оперативных дежурных – наиболее многочисленное подразделение, включающее до половины сотрудников Центра в своем составе, обеспечивает круглосуточный мониторинг событий мировой политики, чрезвычайных и кризисных ситуаций, готовит обзорные доклады и

оперативные информационные документы, задействуются в обеспечении официальных визитов руководства Госдепартамента США за рубеж. Имеет в своем составе специализированный контактный центр для сотрудников ведомства, оказавшихся в условиях чрезвычайных ситуаций за рубежом [4].

2. Штаб содействия урегулированию кризисов – аналитическое подразделение ОЦ, в состав которого входят 5 специалистов по региональной проблематике (в т.ч. По Африке, Ближнему Востоку, Азиатско-тихоокеанскому региону, Европе и Евразии, Северной и Южной Америке), а также ряд вспомогательных сотрудников, в т.ч. Специалист по межведомственному взаимодействию. Подразделение готовит аналитические материалы и экспертные заключения для обеспечения принятия решений в условиях кризисных ситуаций, в т.ч. в случае возникновения угроз жизни и здоровью гражданам США за рубежом (основные потребители – руководство Госдепартамента и других ведомств, Президент США). Штаб регулярно обрабатывает открытые и закрытые источники информации (в т.ч. данные, поступающие по каналам шифрпереписки от зарубежных представительств США). В случае необходимости к его работе привлекаются специалисты из других ведомств, учреждений спецслужб и неправительственных организаций для формирования целевых групп по реагированию на те или иные чрезвычайные ситуации. На базе Штаба на регулярной основе организуются курсы по обучению сотрудников ведомства (в т.ч. Загранучреждений) методам и особенностям работы в условиях чрезвычайных и кризисных ситуаций [4].

Помимо «Ситуационной комнаты Белого дома» ОЦ поддерживает тесное взаимодействие и регулярный обмен данными и аналитикой с аналогичными подразделениями других ведомств, в т.ч. Министерством обороны, ЦРУ и др.

Президентский характер формы правления предопределила ориентированность ситуационных центров США, в особенности, в крупных

ведомствах, на обеспечение преимущественно аналитической и информационной поддержки принятия управленческих решений Президентом США. Заслуживает упоминания то, что по аналогии с отечественной системой, в США реализовано тесное взаимодействие ситуационных центров различных ведомств, а также широко применяется практика их конструирования с учетом специфики сферы деятельности ведомств, в составе которых они создаются.

Список литературы:

1. Смирнов А.И. Глобальная безопасность: инновационные методы анализа конфликтов. : монография / Смирнов А.И., Куроедов Б.В., Кретов В.С. [и др.] Под общ. ред. А.И. Смирнова. – Москва. Общество «Знание» России: 2011. – с.86 – ISBN – 978-5-254-02022-6 URL: https://mgimo.ru/library/publications/1007681/?utm_source=yandex.ru&utm_medium=organic&utm_campaign=yandex.ru&utm_referrer=yandex.ru (дата обращения 17.03.2024) – Текст: электронный.

2. L. Barron-Lopez. Inside the White House Situation Room $50 Million Upgrade. / PBS News Hour (Л. Бэррон-Лопез. Усовершенствование Ситуационной комнаты Белого дома на сумму 50 млн. долл. США. / Пи Би Эс Ньюз Ауэр) URL: https://www.pbs.org/newshour/nation/inside-the-white-house-situation-rooms-50-million-upgrade (дата обращения 18.03.2024) -Текст: электронный.

3. About Us. Executive Secretariat. US Department of State Official Website. (О нас. Исполнительный секретариат. Официальный интернет-сайт Государственного департамента США) – обновляется в течение суток - URL: https://www.state.gov/about-us-executive-secretariat/ (дата обращения 19.03.2024). – Текст: электронный.

4. US Department of State: Foreign Affairs Manual (Указания по международным отношениям Государственного департамента США). URL: https://fam.state.gov (дата обращения 19.03.2024). – Текст: электронный.

СЕКЦИЯ 3

«АКТУАЛЬНЫЕ ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В КОНТЕКСТЕ МЕЖДУНАРОДНОГО ПРАВА»

Алла Юрьевна Ястребова,
доктор юридических наук, доцент,
профессор кафедры международного права,
Дипломатическая академия МИД России,
E-mail: kafedra.mp@dipacademy.ru

Игорь Олегович Анисимов,
кандидат юридических наук,
декан юридического факультета,
Дипломатическая академия МИД России,
E-mail: kafedra.mp@dipacademy.ru

Alla Yu.Yastrebova,
Doctor of Law, Professor of the Department
of International Law, Diplomatic Academy
of the Ministry of Foreign Affairs of Russia
E-mail: kafedra.mp@dipacademy.ru

Igor O. Anisimov,
Ph.D. in Law, Associate Professor, of the Department
of International Law, Diplomatic Academy
of the Ministry of Foreign Affairs of Russia
E-mail: kafedra.mp@dipacademy.ru

ПРАВО НА ИНФОРМАЦИЮ В КОНТЕКСТЕ ОСУЩЕСТВЛЕНИЯ МЕЖДУНАРОДНОЙ МИГРАЦИИ

RIGHT TO INFORMATION IN THE CONTEXT OF INTERNATIONAL MIGRATION ISSUES

Аннотация. Право на информацию выступает основой частного и публичного благосостояния человеческой личности. Оно включает получение и распространение информации. Доступ к информации может быть ограничен только в силу установленных законом оснований, определенных, как правило, тем, что ее содержание составляет государственную, коммерческую или служебную тайну. Тесная связь права на информацию с миграционной сферой обусловлена формированием понимания мигрантами особенностей и правовых институтов иммиграционного законодательства принимающего государства. Глобальный договор о безопасной, упорядоченной и легальной

миграции содержит нормы, касающиеся предоставления точной и своевременной информации, для реализации межгосударственных передвижений людей.

Ключевые слова: право человека на информацию, доступ к информации и его ограничение, обеспечение информационной безопасности, определение международной миграции, информационные аспекты миграционной политики государств, защита прав человека, иммиграционное законодательство.

Abstract. The right to information is the basis of the private and public well-being of the human person. It includes receiving and distributing information. Access to information may be restricted only on the grounds established by law, which are usually determined by the fact that its content is a State, commercial or official secret. The close connection of the right to information with the migration sphere is due to the formation of migrants' understanding of the specifics and legal institutions of the immigration legislation of the host State. The Global Compact for Safe, Orderly and Regular Migration contains standards for the provision of accurate and timely information for the implementation of interstate movements of people.

Keywords: human right to information, access to information and its restriction, information security, definition of international migration, information aspects of migration policy of states, protection of human rights, immigration legislation.

Содержание права на информацию. Ч. 2. ст. 19 Пакта о гражданских и политических правах 1966 г. устанавливает, что каждый человек имеет право на свободное выражение своего мнения; это право включает свободу искать, получать и распространять всякого рода информацию и идеи, независимо от государственных границ, устно, письменно или посредством печати или художественных форм выражения, или иными способами по своему выбору [9]. Право на доступ к информации является неотъемлемой частью фундаментального права на свободу выражения мнения, признанного ст. 19

Всеобщей декларации прав человека 1948 г., которая гласит, что свобода выражения мнения включает свободу «искать, получать и распространять информацию и идеи любыми средствами и независимо от государственных границ» [3]. Данное право получило свое закрепление также в Конвенции СНГ о правах и основных свободах человека 1995 г. Так, ч. 1 ст. 11 указанной Конвенции устанавливает, что «Каждый человек имеет право на свободное выражение своего мнения. Это право включает свободу придерживаться своих мнений, получать и распространять информацию и идеи любым законным способом без вмешательства со стороны государственных властей и независимо от государственных границ» [6]. Таким образом, право на информацию состоит из двух основных элементов: права на получение и права на распространение информации.

Как указывает Т.В. Бушуева, право свободно получать информацию означает право на свободный, без ограничений (кроме случаев, оговоренных законом), доступ к информации. Ограничения на доступ к информации обусловлены, прежде всего, ее содержанием (государственные секреты, коммерческая или служебная тайна, личная и семейная тайна гражданина). Однако, к массовой информации доступ не ограничен [1].

Таким образом, данное право необходимо для обеспечения открытости и прозрачности решений, имеющих общественное значение. Оно тесно связано с общими принципами функционирования гражданского общества, к которым относятся необходимость и обоснованность принимаемых решений, принципы соразмерности и надлежащего администрирования, отчётности и ответственности органов власти перед обществом.

Когда речь идет о праве на свободное получение, распространение и использование информации, государство должно исходить из принципа правового равенства всех участников процесса информационного взаимодействия, вне зависимости от их политического, социального и

экономического статуса. Информация постоянно открыта для всех и предоставляется с гарантией достоверности и полноты.

Особое значение лично для гражданина имеет официальная информация о наличии угроз для здоровья человека вследствие вредных условий производства продукции и услуг, пандемии, экологических опасностей.

Необходимо отметить и право свободного доступа к нормативно-правовым актам, который является важным элементом верховенства права. Он включает информацию о внесении изменений в нормативно-правовые акты, их отмене или признанию недействительными. Так, в соответствии с определением Организации Объединенных Наций по вопросам образования, науки и культуры (ЮНЕСКО), право на доступ к информации можно определить как право искать, получать и передавать информацию, которой владеют государственные органы [5].

Международно-правовые основы обеспечения права на информацию и информационной безопасности. Осуществление права на доступ к информации тесно связано с правовым обеспечением информационной безопасности. В рамках СНГ было принято несколько международно-правовых актов в области защиты информации. Так, например, согласно ст. 6 Соглашения о сотрудничестве государств-участников Содружества Независимых Государств в области обеспечения информационной безопасности 2013 г., «стороны обязуются не разглашать и обеспечить надлежащей защитой информацию ограниченного доступа, которая стала известна им в процессе реализации настоящего Соглашения. В рамках настоящего Соглашения не осуществляется передача сведений, отнесенных законодательством государств − участников настоящего Соглашения к государственной тайне (государственным секретам)» [12].

В 2022 г. государствами-участниками Содружества Независимых Государств утвержден План первоочередных мероприятий по реализации Стратегии обеспечения информационной безопасности на период до 2030

года. Этот документ установил комплекс мер, направленных на практическую реализацию согласованных подходов к регулированию области обеспечения информационной безопасности. При этом План учитывает существующие подходы государств Содружества к данному вопросу, а также наилучшие практики, выработанные в этой сфере.

Еще одним важным региональным международно-правовым актом в сфере защиты информации является Стратегия обеспечения информационной безопасности государств-участников Содружества Независимых Государств 2019 г. В преамбуле к Стратегии дается следующее определение информационной безопасности: это состояние защищенности личности, общества и государства и их интересов от угроз, деструктивных и иных негативных воздействий в информационном пространстве [13].

Важную роль в реализации права на информацию играет открытость и транспарентность государственной власти перед обществом, что получило закрепление в Конвенции Совета Европы о доступе к официальным документам 2008 г. [7] Данная Конвенция является первым международно-правовым договором, в котором признается общее право доступа к официальным документам, которые принимаются государственными органами. В соответствии со ст. 5, ограничение на право доступа к официальным документам разрешается устанавливать только для защиты таких значимых областей, как национальная безопасность, оборона или личная жизнь. Кроме того, Конвенция содержит минимальные стандарты, применяемые при обработке запросов о доступе к официальным документам (форма запросов и сборы в связи с доступом к официальным документам), а также процедура пересмотра принятых решений и дополнительные меры [11].

Как отмечают А.Г. Быкова и Ю.Г. Петрова, в процессе реализации права на доступ к информации гражданин выступает не только потребителем предоставляемой ему информации, но и источником информации, которую он обязан предоставить в органы государственной власти в соответствии с

действующим законодательством. Так, обязанность предоставить информацию о себе возникает в связи с исполнением гражданином других установленных законом прав и обязанностей, реализация которых невозможна без предоставления в органы государственной власти информации о себе (персональные данные) [2].

Таким образом, право на доступ к информации и обеспечение информационной безопасности совместно установлены в ряде международно-правовых актов. В связи с отсутствием универсального международного договора, представляется необходимой общая кодификация принципов и норм, регулирующих право на информацию и доступ к ней.

Право мигрантов на информацию. По определению Международной организации по миграции (МОМ), мигрантом может признаваться лицо, которое переместилось через международные границы или в пределах собственного государства и покинуло свое обычное место жительства, вне зависимости от его правового статуса, добровольного или вынужденного типа перемещения и его причин, продолжительности пребывания [8]. Глобальный договор о безопасной, упорядоченной и легальной миграции [4] ставит в качестве цели 3 для государств-участников предоставление точной и своевременной информации на всех этапах миграции. В качестве действий по реализации указанной цели предполагается создание централизованных общедоступных веб-сайтов с информацией о возможностях легальной миграции для въезжающих лиц; об иммиграционном законодательстве и иммиграционной политике конкретных стран; визовых требованиях; порядке подачи заявлений сборах и критериях изменения визового статуса; требованиях для получения разрешения на работу и в отношении профессиональной квалификации; процедурах оценки ученых степеней и установления их эквивалентности; возможностях обучения и профессиональной подготовки; стоимости и условиях пребывания на территории принимающих государств.

Наличие такой информации позволяет мигрантам принимать обоснованные решения. Здесь можно увидеть определенную дифференциацию запросов в зависимости от намерений людей и причин миграции. А.А. Ткаченко обращает внимание на значение унификации понятий и терминов миграционной сферы, которые позволили бы определять статус вынужденных и добровольных мигрантов и тем самым гарантировать соответствующий международно-правовым нормам уровень социальной защиты [14]. Е.Ю. Умнова высказывает мнение о том, что эффективное взаимодействие субъектов информационной области реализуется посредством прямых и обратных связей в соответствии с диалоговой моделью государственной информационной политики в области миграции. Данный автор считает одной из функций такой политики ее связь с процессом социализации мигрантов, усвоения ими социального опыта, знаний, норм, идеалов, присущих гражданскому обществу и социальной группе, которые их приняли [15]. Вышеприведенные научные позиции вполне могут быть применены при изложении и толковании общих принципов регулирования миграции, обозначенных в Глобальном договоре. Это относится, в частности, к принципам ориентированности на интересы людей, устойчивого развития, вовлеченности в вопросы управления миграцией государственных структур и гражданского общества принимающих государств.

Значение типов и условий миграции для подготовки информационного обеспечения. Представляется, что информация, предоставляемая мигрантам, должна быть сформирована по определенной тематике, в которую включено: 1) понятие существующих видов правового статуса (беженец, лицо, ищущее убежище, трудящийся-мигрант, иностранный гражданин, прибывший с целью воссоединения семьи, репатриант и т.д.), правовых процедур его оформления и санкций за нарушение миграционных правил; 2) толкование действующего иммиграционного законодательства (с помощью правовых комментариев и справочных изданий); 3) компетенция и функции уполномоченных государственных ведомств по вопросам миграции; 4) предоставление

объективных статистических данных по миграции и правовых основ миграционного учета; 5) меры административного и иммиграционного контроля, которые могут быть применены к мигрантам; 6) указание возможностей адаптации и интеграции в принимающем государстве; 7) сопровождение и поддержка мигрантов со стороны общественных организаций.

Подобная информация может быть дифференцирована для отдельных категорий иностранцев. К примеру, для трудящихся-мигрантов на весь период пребывания в стране трудоустройства сохраняется право на обращение за консульским содействием. Помимо этого, информация сочетает в себе правовые основы иммиграции и международно-правовые принципы защиты прав человека. Так, В.В. Пчелинцева замечает, что принципы и нормы международного права содержатся как в институте убежища для вынужденных мигрантов, так и в международном праве защиты и поощрения прав человека [10].

Таким образом, для межгосударственного сотрудничества по информационному обеспечению миграции требуется создание доступных консультационных центров и электронных платформ, которые сочетали бы возможности предоставления консульских услуг, защиты частной жизни и персональных данных таких лиц, привлечения внимания к рискам незаконной миграции, оказания особой помощи детям и семьям мигрантов, формирования благоприятной и ориентированной социальной среды.

Список источников и литературы:

1. Бушуева Т.В. Основы правового регулирования прав граждан на получение и распространение информации // Труды Института государства и права РАН. 2014. №4. С. 28. URL: https://cyberleninka.ru/article/n/osnovy-pravovogo-regulirovaniya-prav-grazhdan-na-poluchenie-i-rasprostranenie-informatsii (дата обращения: 26.11.2024).

2. Быкова А. Г., Петрова Ю. Г. Право граждан на доступ к информации // Сибирское юридическое обозрение. 2013. №1 (20). С. 5. URL: https://cyberleninka.ru/article/n/pravo-grazhdan-na-dostup-k-informatsii (дата обращения: 12.11.2024).

3. Всеобщая декларация прав человека 1948 г. URL: https://www.un.org/ru/documents/decl_conv/declarations/declhr.shtml (дата обращения: 12.11.2024).

4. Глобальный договор о безопасной, упорядоченной и легальной миграции, принят резолюцией ГА ООН 73/195. Представляет собой рекомендательный рамочный документ для обеспечения международного сотрудничества по вопросам миграции (ст. 7) URL: https://migrationnetwork.un.org/sites/g/files/tmzbdl416/files/docs/gcm_russian.pdf (дата обращения: 12.11.2024).

5. Законы о доступе к информации. Официальный сайт ЮНЕСКО. URL: https://www.unesco.org/ru/access-information-laws (дата обращения: 12.11.2024).

6. Конвенция СНГ о правах и основных свободах человека 1995 г. URL: https://cis.minsk.by/page/11326/konvencii-sodruzestva-nezavisimyh-gosudarstv-o-pravah-i-osnovnyh-svobodah-celoveka-26-maa-1995-g-minsk (дата обращения: 12.11.2024).

7. Конвенция Совета Европы о доступе к официальным документам 2008 г. (неофициальный перевод) URL: https://rm.coe.int/16805a937b (дата обращения: 12.11.2024).

8. Мир, достоинство и равенство на здоровой планете. Миграция: глобальные вопросы повестки дня. URL: https://www.un.org/ru/global issues/migration (дата обращения: 12.11.2024).

9. Пакт о гражданских и политических правах 1966 г. URL: https://www.un.org/ru/documents/decl_conv/conventions/pactpol.shtml (дата обращения: 12.11.2024).

10. Пчелинцева В.В. Соотношение института убежища и международного права защиты и поощрения прав человека // Право и миграция в меняющемся мире: сборник материалов круглого стола XV Конвента РАМИ / под научн.ред Д.В.Иванова. М.: Статут, 2024. С. 109. (С. 103-113).

11. Резюме Конвенции Совета Европы о доступе к официальным документам URL: http://conventions.coe.int/Treaty/RUS/Summaries/Html/205.htm (дата обращения: 12.11.2024).

12. Соглашение о сотрудничестве государств-участников Содружества Независимых Государств в области обеспечения информационной безопасности 2013 г. URL: https://cis.minsk.by/reestrv2/doc/4074#text (дата обращения: 12.11.2024).

13. Стратегия обеспечения информационной безопасности государств-участников Содружества Независимых Государств 2019 г. URL: https://base.spinform.ru/show_doc.fwx?rgn=120663#A5MW0UTWLH (дата обращения: 12.11.2024).

14. Ткаченко А.А. Терминология в области миграции: проблемы международной сопоставимости // Демография. Социально-трудовые исследования. 2020. № 4. С. 69. (69-79).

15. Умнова Е.Ю. Государственная миграционная политика в условиях современной миграции населения: автореф.дис. … канд.полит.наук: 23.00.02. Ставрополь: Ставропольский гос.ун-т, 2005. С. 9, 15. (28 с.).

Павел Николаевич Головач,
студент Юридического факультета,
Белорусский государственный университет,
E-mail: pavelgolovac65@gmail.com

Научный руководитель:
Ольга Викторовна Емельянович,
к.ю.н., заместитель декана по международному сотрудничеству и интернационализации образования юридического факультета,
Белорусский государственный университет,
E-mail: emelyanovich@bsu.by

Pavel N. Golovach,
Student of the Law Faculty,
Belarusian State University,
E-mail: pavelgolovac65@gmail.com

Scientific supervisor:
Olga V. Emelianovich,
Ph.D. in Law, Deputy Dean for International Cooperation and Internationalization of Education, Faculty of Law,
Belarusian State University,
E-mail: emelyanovich@bsu.by

О ПРАВОВОМ РЕГУЛИРОВАНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РЕСПУБЛИКИ БЕЛАРУСЬ В КОНТЕКСТЕ ОБЕСПЕЧЕНИЯ МЕЖДУНАРОДНОЙ БЕЗОПАСНОСТИ

ON THE LEGAL REGULATION OF INFORMATION SECURITY OF THE REPUBLIC OF BELARUS IN THE CONTEXT OF ENSURING INTERNATIONAL SECURITY

Аннотация. В условиях глобализации и цифровизации информационная безопасность становится важным элементом системы международной безопасности. Обеспечение информационной безопасности является необходимым условием для стабильного развития национальной безопасности государств в информационной сфере, а также международных отношений, защиты прав и свобод индивидов и юридических лиц. Настоящее исследование направлено на определение специфики правового

регулирования информационной безопасности Республики Беларусь в контексте обеспечения международной безопасности путем анализа международных документов и нормативных правовых актов в данной области.

Ключевые слова: информационная безопасность, международная безопасность, правовое регулирование, международные документы, национальная безопасность, информационные системы, информационные угрозы, международные отношения.

Abstract. In the context of globalization and digitalization, information security is becoming an important element of the international security system. Ensuring information security is a necessary condition for stable development of national security of states in the information sphere and international relations, protection of the rights and freedoms of individuals and legal entities. The present study is aimed at determining the specifics of the legal regulation of information security in the Republic of Belarus in the context of ensuring international security.

Keywords: information security, international security, legal regulation, international documents, national security, information systems, information threats, international relations.

Как суверенное и независимое государство Республика Беларусь признает приоритет общепризнанных принципов международного права и обеспечивает соответствие им законодательства в соответствии со ст. 8 Конституции Республики Беларусь [2].

Нормы права, содержащиеся в ратифицированных международных договорах, являются составной частью действующей системы законодательства Республики Беларусь. При заключении международных договоров, в целях достижения баланса национальных и наднациональных интересов, приоритетным является обеспечение верховенства Конституции Республики Беларусь, незыблемости основ конституционного строя и государственного суверенитета [3].

В соответствии со ст. 18 Конституции в своей внешней политике Республика Беларусь опирается на принципы равенства, неприменения силы или угрозы силой, нерушимости границ, мирного урегулирования споров, невмешательства во внутренние дела и иных общепризнанных принципов и норм международного права. Данные принципы закреплены в Уставе Организации Объединенных Наций (далее – Устав ООН) 1970 года [12]. В частности, п. 7 ст. 2 Устава ООН «невмешательство в дела, по существу входящие во внутреннюю компетенцию любого государства», а также п. 4 ст. 2 Устава ООН «воздержание от угрозы силой или её применения в отношении территориальной неприкосновенности или политической независимости любого государства».

В Республике Беларусь обеспечение информационной безопасности – одно из приоритетных направлений развития государства. Существует ряд нормативных правовых актов, регулирующих информационную безопасность. К ним относятся:

− Закон от 10 ноября 2008 г. № 455-З «Об информации, информатизации и защите информации» [9], регулирующий общественные отношения, связанные с созданием, распространением, использованием и защитой информации, а также с информатизацией и развитием информационных технологий;

− Указ Президента Республики Беларусь от 9 декабря 2019 г. № 449 «О совершенствовании государственного регулирования в области защиты информации» [8], направленный на усиление мер по обеспечению информационной безопасности, включая защиту информации от несанкционированного доступа, утечек и других угроз, а также на улучшение координации и эффективности государственного регулирования в данной сфере;

− Указ Президента Республики Беларусь от 25 октября 2011 г. № 486 «О некоторых мерах по обеспечению безопасности критически важных объектов информатизации» [7], направленный на усиление мер по защите от

различных угроз, включая кибератаки и другие формы несанкционированного доступа;

− иные акты.

Одним из главенствующих актов в Республике в сфере информационной безопасности является новая Концепция национальной безопасности Республики Беларусь, утверждённая решением Всебелорусского народного собрания от 25.04.2024 № 5 (далее – Концепция национальной безопасности), в которой отражены основные направления национальной политики [11]. В ней содержится перечень национальных интересов Республики Беларусь в различных сферах, а также отмечается, что в Республике сформированы и совершенствуются условия, необходимые для предотвращения и нейтрализации различных угроз нацбезопасности.

Стоит отметить, что подобного рода документы, определяющие политику национальной безопасности, приняты во многих странах-членах ООН.

Также 18 марта 2019 года Постановлением Совета безопасности Республики Беларусь в рамках Концепции национальной безопасности была утверждена Концепция информационной безопасности Республики Беларусь (далее – Концепция информационной безопасности) – специализированный документ, регулирующий информационное направление политики нашей страны [6].

Положения Концепции национальной безопасности и Концепции информационной безопасности во многом коррелируют также со ст. 20 Международного пакта о гражданских и политических правах от 16 декабря 1966 г. [5] С одной стороны, современным международным правом закрепляются основы обеспечения информационной безопасности, а с другой поведение государств в информационно-коммуникационном пространстве в настоящее время подробно не регламентировано [4].

15 мая 2023 г. Российской Федерацией в качестве официального документа 77-й сессии Генеральной Ассамблеи ООН была предложена

Обновлённая Концепция Конвенции Организации объединенных наций «Об обеспечении международной информационной безопасности», и Республика Беларусь является одним из её соавторов [1]. Тот факт, что Республика Беларусь является активным участником разработки такого рода актов, свидетельствует о едином подходе и общей согласованности подходов политики нашей страны и общемировой политике зарубежных государств.

Республика Беларусь и Российская Федерация являются надёжными партнерами в сфере информационной безопасности, активно сотрудничая в разработке и внедрении совместных мер по защите информационных систем и ресурсов. 22 февраля 2023 г. постановлением Высшего Государственного Совета Союзного Государства утверждена Концепция информационной безопасности Союзного государства. Документ является итогом тесного взаимодействия компетентных органов двух стран в сфере совместного противодействия современным информационным вызовам и угрозам на основе прочного правового фундамента [10].

Таким образом, обеспечение информационной безопасности является одним из приоритетных направлений политики Республики Беларусь, а также необходимым условием для обеспечения национальной безопасности государства в информационной сфере и стабильного развития международных отношений. Республика Беларусь активно развивает своё законодательство в данной области. Это демонстрирует согласованность подходов Концепции национальной и информационной безопасности Республики Беларусь с международными актами во многих аспектах, что свидетельствует о едином подходе по вопросам обеспечения информационной безопасности и о том, что Республика Беларусь максимально вовлечена в мировые информационные процессы и привержена лучшим мировым и международным практикам обеспечения информационной безопасности. Республика Беларусь готова и в дальнейшем развивать сотрудничество и укреплять связи в области международной информационной безопасности со всеми странами мира.

Список источников и литературы:

1. Конвенция Организации объединенных наций об обеспечении международной информационной безопасности (концепция) [Электронный ресурс] : // Совет Безопасности Российской Федерации : официальный сайт. – 2021. – Режим доступа: http://www.scrf.gov.ru/media/files/file/P7ehXmaBUDOAAc ATW2Rwa3yNK1bNAWl9.pdf. (дата обращения: 06.10.2024).

2. Конституция Республики Беларусь : с изменениями и дополнениями, принятыми на республиканских референдумах 24 ноября 1996 г., 17 октября 2004 г. и 27 февраля 2022 г.. – Минск : Национальный центр правовой информации Республики Беларусь, 2022. – 77 с.

3. Конституция Республики Беларусь : науч.-практ. Комментарий / под общ. Ред. П.П. Миклашевича, О.И. Чуприс, Г.А. Василевича. – Минск : Национальный центр правовой информации Республики Беларусь, 2024. – 544 с.

4. Международно-правовые основы обеспечения международной информационной безопасности / Н. О. Мороз // журнал «Юриспруденция». – 2016. – с. 77–81.

5. Международный пакт о гражданских и политических правах // Организация Объединённых Наций [Электронный ресурс] – 1966. – Режим доступа: https://www.un.org/ru/documents/decl_conv/conventions/pactpol. shtml. (дата обращения: 06.10.2024).

6. О Концепции информационной безопасности Республики Беларусь [Электронный ресурс]: Постановление совета Безопасности Республики Беларусь, 18 марта 2019 г., № 1 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. Центр правовой информ. Респ. Беларусь. – Минск, 2024.

7. О некоторых мерах по обеспечению безопасности критически важных объектов информатизации [Электронный ресурс] : Указ Президента

Респ. Беларусь, 25 октября 2011 г. (в ред. От 19.12.2019), № 486 // Онлайн-сервис готовых правовых решений ilex / ООО «ЮрСпектр». – Минск, 2024.

8. О совершенствовании государственного регулирования в области защиты информации [Электронный ресурс] : Указ Президента Респ. Беларусь, 9 декабря 2019 г., № 449 // Онлайн-сервис готовых правовых решений ilex / ООО «ЮрСпектр». – Минск, 2024.

9. Об информации, информатизации и защите информации [Электронный ресурс] : Закон Респ. Беларусь, 10 ноя. 2019 г., № 455-З : в ред. Закона Респ. Беларусь от 10.10.2022 г. // ЭТАЛОН. Законодательство Республики Беларусь / Нац. Центр правовой информ. Респ. Беларусь. – Минск, 2024.

10. Об утверждении концепции информационной безопасности Союзного государства [Электронный ресурс] // Постановление Высшего Государственного Совета Союзного Государства, 22 фев. 2023 г., №1 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. Центр правовой информ. Респ. Беларусь. – Минск, 2024.

11. Об утверждении Концепции национальной безопасности Республики Беларусь [Электронный ресурс] : решение Всебелорусского народного собрания Респ. Беларусь, 25 апр. 2024 г., № 5 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. Центр правовой информ. Респ. Беларусь. – Минск, 2024.

12. Устав ООН [Электронный ресурс] // Организация Объединённых Наций – Режим доступа: https://www.un.org/ru/about-us/un-charter/full-text. (дата обращения: 06.10.2024).

Евгений Олегович Иванов,
соискатель кафедры мировых
политических процессов,
МГИМО (У) МИД России,
E-mail: eugene4712@mail.ru

Evgeniy O. Ivanov,
Postgraduate researcher,
Department of World Politics,
MGIMO University,
E-mail: eugene4712@mail.ru

ПОДХОДЫ ВЕДУЩИХ ГОСУДАРСТВ ЛАТИНСКОЙ АМЕРИКИ К ВОПРОСУ ПРИМЕНИМОСТИ МЕЖДУНАРОДНОГО ГУМАНИТАРНОГО ПРАВА В ЦИФРОВОЙ СРЕДЕ

APPROACHES OF THE LEADING LATIN AMERICAN COUNTRIES TO THE ISSUE OF APPLICABILITY OF THE INTERNATIONAL HUMANITARIAN LAW IN THE DIGITAL ENVIRONMENT

Аннотация. Исследование рассматривает проблему применимости права вооружённых конфликтов к цифровому пространству и анализирует подходы трёх ведущих стран Латинской Америки (Аргентины, Бразилии и Мексики) к данной проблематике. На основании изучения основополагающих документов и позиций, выраженных на международных дискуссионных площадках, автор приходит к выводу, что Бразилиа и Буэнос-Айрес настаивают на сугубо мирном применении ИКТ, тогда как Мехико считает возможной милитаризацию цифровой среды.

Ключевые слова: международное гуманитарное право, цифровая среда, информационная безопасность, Группа правительственных экспертов, Рабочая группа открытого состава, Аргентина, Бразилия, Мексика.

Abstract. The study investigates the problem of applicability of the armed conflict law to the digital environment and analyzes the approaches of three leading Latin American countries (Brazil, Argentina and Mexico). Based on fundamental documents and positions expressed on the international discussing platforms, the

author draws a conclusion that Brasilia and Buenos Aires insist on the strictly peaceful use of ICT, while Mexico considers possible militarization of the digital environment.

Keywords: international humanitarian law, digital environment, information security, Group of Governmental Experts, Open-ended Working Group, Argentina, Brazil, Mexico.

История вопроса. В соответствии с докладом Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности (ГПЭ) за 2021 год, международное гуманитарное право может быть применено к цифровой среде исключительно в условиях вооружённого конфликта. В мирное же время государства должны воздерживаться от угрозы силой или её применения, а также не вмешиваться во внутренние дела других стран с использованием ИКТ [2, с. 17-18].

В целом такой подход соответствует представлениям «мирового большинства» о цифровых технологиях, что их нужно применять исключительно в мирных целях. Однако «коллективный Запад» во главе с США, напротив, стремится к большей милитаризации ИКТ, не признавая военно-политические угрозы в цифровой среде в качестве предмета обсуждения на международном уровне и желая легализовать собственное вмешательство во внутренние дела других стран с использованием современных технологий [1].

Латинская Америка и международная информационная безопасность (МИБ). Значительной части государств Латинской Америки и Карибского бассейна (ЛАКБ) присущи такие принципы, как уважение суверенитета, невмешательство во внутренние дела, мирное разрешение споров и понимание необходимости совершенствования правовых основ современного международного порядка. По этой причине совершенно неудивительно, что эти внешнеполитические установки влияют и на их подходы к обеспечению

МИБ в целом и вопросу о применимости международного права вооружённых конфликтов к цифровому пространству.

Подход Аргентины. Первая Национальная стратегия по кибербезопасности, принятая в 2019 году во время президентства Маурисио Макри, констатировала, что на фоне роста международной напряжённости ряд государств продвигает идею о военном использовании ИКТ и стремится к её практической реализации, таким образом «провоцируя нестабильность, недоверие между государствами и страх в обществе». Руководство Аргентины заявило о приверженности сугубо мирному использованию ИКТ и о поддержке любых инициатив, нацеленных на соблюдение принципа справедливости в цифровой среде [6, p. 3].

В новой версии документа, принятой в 2023 году при президенте Альберто Фернандесе, в число руководящих принципов было добавлено обеспечение мира и безопасности в цифровом пространстве [5, p. 3]. В вопросе применимости международного права к ИКТ Буэнос-Айрес настаивает на конкретизации видов деятельности государств в цифровой среде, которые могут быть интерпретированы как угроза силой или её применение. Отдельно предложено детализировать в рамках Рабочей группы открытого состава ООН по вопросам безопасности ИКТ (РГОС) пояснения, касающиеся применимости права вооружённых конфликтов к использованию ИКТ в рамках таких конфликтов (но не в мирное время) [8].

Позиция Бразилии. Бразилия, наряду с Россией, Китаем, Индией и рядом других незападных государств, является членом Группы одиннадцати (G11): её участники придерживаются общей позиции, состоящей в недопустимости гонки вооружений в информационном пространстве и развязывания полномасштабных конфликтов с применением ИКТ [3, с. 284]. Поэтому в Национальной стратегии Бразилии в области кибербезопасности, принятой в феврале 2020 года, зафиксировано, что укрепление всеобщего мира и стабильности в цифровой среде является одним из главных приоритетов в обеспечении МИБ.

Среди угроз безопасности ИКТ, помимо их использования в террористических и преступных целях, были также выделены наступательные информационные операции с целью проецирования силы в мирное время. Таким образом, документ открыто уделил внимание военно-политическому аспекту МИБ и обозначил факт неприемлемости милитаризации цифровой среды для Бразилиа [7].

Подход Мексики. В отличие от Бразилии и Аргентины, Мексика разделяет подход США и «коллективного Запада» в части применимости международного гуманитарного права к цифровому пространству. Именно подобная позиция стала причиной непринятия итогового доклада ГПЭ в 2017 году: представители Мехико отстаивали возможность проведения наступательных операций с использованием ИКТ в мирное время, что вызвало резкое неприятие со стороны целого ряда стран, в частности, России, Бразилии и Кубы [4, с. 74-76].

Такая позиция Мексики, вкупе с практически полным игнорированием военно-политических угроз МИБ, объясняется двумя факторами. Во-первых, главными вызовами, стоящими перед Мехико, являются преступность и наркотрафик, тогда как армия де-факто вынуждена выполнять полицейские функции. Во-вторых, в институциональном плане Мексика всегда была близка к Вашингтону, сперва в формате Североамериканской зоны свободной торговли (НАФТА), а позже – в объединении USMCA (США, Мексика, Канада).

Заключение. Можно констатировать, что среди ведущих государств Латинской Америки нет единого подхода к вопросу применимости международного права вооружённых конфликтов к ИКТ-среде. Вместе с тем, позиции Аргентины и Бразилии, основанные на неприятии милитаризации цифрового пространства, уважении «цифрового суверенитета» и «неприменении силы в цифре», отражают то, как воспринимают цифровую среду страны «мирового большинства», которые отвергают устремления Запада сохранить своё доминирование в области ИКТ, не гнушаясь их

использованием в военно-политических целях, противоречащих общепризнанным принципам международного права.

Список источников и литературы:

1. Коротков С.В., Смирнов А.А. О взаимосвязи киберпреступлений и международного гуманитарного права в контексте обеспечения международной информационной безопасности. *Международная жизнь*. Available at: https://interaffairs.ru/news/show/38329 (Дата обращения: 14.10.2024).

2. Международная информационная безопасность: подходы России. Под рук. А.В. Крутских, Е.С. Зиновьевой. М., 2021, 47 с. Available at: https://mgimo.ru/upload/iblock/047/01fgupojoj7ka0tw75bw19li4bmurfse/%D0%94%D0%BE%D0%BA%D0%BB%D0%B0%D0%B4%20%D1%80%D1%83%D1%81%D1%81%D0%BA%D0%B8%D0%B9.pdf (Дата обращения: 14.10.2024).

3. Международная информационная безопасность: Теория и практика. Под общ. Ред. А.В. Крутских. М., 2021, Издательство «Аспект Пресс», 384 с.

4. Стадник И.Т., Цветкова Н.А. Место и роль стран Латинской Америки в системе кибербезопасности. *Латинская Америка*. М., 2021, №4, сс. 69-84.

5. Estrategia Nacional de Ciberseguridad de la República Argentina. *El Gobierno de Argentina*. El 14 de julio de 2023. 9 p. Available at: https://www.boletinoficial.gob.ar/detalleAviso/primera/293377/20230904 (Дата обращения: 08.10.2024).

6. Estrategia Nacional de Ciberseguridad de la República Argentina. *International Telecommunication Union*. El 24 de mayo de 2019. 9 p. Available at: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Argentina%20National%20Cybersecurity%20Strategy_anexo_5740509_1.pdf (Дата обращения: 14.10.2024).

7. Estratégia Nacional de Segurança Cibernética. *Presidência da República*. De 5 de fevereiro de 2020. Available at: http://www.planalto.gov.br/CCIVIL_03/_Ato2019-2022/2020/Decreto/D10222.htm (Дата обращения: 06.10.2024).

8. Initial “Pre-draft” of the report of the OEWG on developments in the field of information and telecommunications in the context of international security. Comments by Argentina. *United Nations*. April, 2020. Available at: https://front.un-arm.org/wp-content/uploads/2020/04/oewg-ict-comments-argentina-3.pdf (Дата обращения: 08.10.2024).

Юлия Сергеевна Нечаева,
ведущий советник отдела,
Министерство юстиции Российской Федерации,
E-mail: nechyulia@mail.ru

Yulia S.Nechaeva,
Senior Advisor of the Department,
Ministry of Justice of the Russian Federation,
E-mail: nechyulia@mail.ru

ОСНОВНЫЕ КОНЦЕПЦИИ ОПРЕДЕЛЕНИЯ ПРАВОСУБЪЕКТНОСТИ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ОТНОШЕНИИ ОБЪЕКТОВ ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

MAIN CONCEPTS OF DETERMINING THE LEGAL PERSONALITY OF ARTIFICIAL INTELLIGENCE IN RELATION TO INTELLECTUAL PROPERTY OBJECTS

Аннотация. В настоящем исследовании рассмотрены основные точки зрения российских и зарубежных ученых, а также судебная практика в части определения правосубъектности искусственного интеллекта в отношении объектов интеллектуальной собственности.

Ключевые слова: искусственный интеллект, интеллектуальная собственность, правосубъектность, нейросети, авторское право.

Abstract: The article examines the main points of view of Russian and foreign researchers, as well as judicial practice in terms of determining the legal personality of artificial intelligence in relation to intellectual property.

Keywords: artificial intelligence, intellectual property, legal personality, neural networks, copyright.

Текущий статус искусственного интеллекта. Развитие цифровых технологий приводит к значительным результатам, упрощая многие жизненные процессы и освобождая человечество от тяжелого физического труда. Искусственный интеллект становится неотъемлемой частью жизни современного общества в цифровую эпоху. За последнее десятилетие

получили свое развитие инструменты, оказывающие содействие в решении интеллектуальных и творческих задач, которые управляются искусственным интеллектом (например, генеративные нейросети). Искусственный интеллект способен сделать за несколько минут то, на что у человека ушли бы часы или дни. Например, генерация изображений, мелодий, замена лиц на видео, замена голоса в музыкальных композициях, создание литературных работ.

В 2024 г. две российские генеративные модели вошли в рейтинг 10 лучших нейросетей в мире от TechBullion, заняв пятое и десятое места, что свидетельствует о достаточно высоком уровне развития технологий в стране и конкурентоспособности в рассматриваемой сфере (Kandinsky на пятом месте, YandexArt на десятом месте) среди генеративных моделей, разработанных в США, Индии и Китае (Midjourney, SDXL Turbo, DALL-E 3, Imagen 2, Firefly, Titan Image Generator, Kalaido AI, Tongyi Wanxiang).

Такой резкий прорыв в развитии искусственного интеллекта и его повсеместное распространение открыли безграничный спектр возможностей для его использования как прикладного инструмента, и в то же время поставило юридическое сообщество перед необходимостью определения правового статуса искусственного интеллекта и результатов его деятельности, и вызвало ряд насущных вопросов: может ли искусственный интеллект обладать правосубъектностью? Кто является автором произведений, создаваемых с помощью нейросетей? Нарушаются ли авторские права лиц, чьи произведения используются для обучения нейросетей?

Как известно, большинство нейросетей генерируют изображения, литературные, музыкальные и аудиовизуальные произведения на основе существующих результатов деятельности человека, используемых создателем нейросети для ее обучения. Пользователь нейросети формулирует текстовый запрос и получает бесконечное количество уникальных неповторяющихся изображений. Любой другой пользователь может использовать тот же самый запрос, при этом изображение, генерируемое нейросетью, будет всегда

уникальным, тем самым обеспечивая пользователя контентом, который не будет нарушать чьи-либо авторские права.

Такие изображения используются повсеместно − в рекламе, в блогах, в качестве иллюстраций к статьям − в любых сферах, где необходимо визуальное сопровождение какого-либо материала, позволяя экономить время и средства на услуги дизайнеров, фотографов, художников и других специалистов.

В то же время использование нейросетей не урегулировано на законодательном уровне. В настоящее время существуют отдельные судебные акты либо правовые нормы в данной сфере, однако комплексное законодательное регулирование на национальном и, тем более, на международном уровнях отсутствует. Это связано в первую очередь с тем, что ученые юристы и даже представители судебных систем в разных государствах еще не пришли к единому мнению по поводу того, обладает ли искусственный интеллект правосубъектностью наравне с человеком или является инструментом для реализации интеллектуальной и творческой деятельности человека.

Существующие точки зрения. Научная доктрина расходится во мнении об определении правосубъектности искусственного интеллекта, которым создаются объекты интеллектуальной собственности. Существуют противоположные мнения, свидетельствующие как о нецелесообразности наделения искусственного интеллекта правосубъектностью (В.А. Свечников [6], А.В. Гурко [2], Дэн Л. Берк [7]), так и о возможности предоставления ему некоторых прав (Л. Огуама [8]) либо указания создателя или пользователя искусственного интеллекта в качестве автора результатов деятельности искусственного интеллекта (Д.А. Грачева [1]). П.А. Каштанова [4] отмечает, что в российской доктрине активно обсуждается подход к защите произведений, созданных искусственным интеллектом, в рамках смежного права (П. Ролинсон, Е.А. Ариевич, Д.Е. Ермолина [5], В.О. Калятин [3] и другие).

Стоит отметить, что и судебная практика кардинально отличается в разных юрисдикциях. Так, в 2019 г. в Китае было принято решение Народного суда округа Наньшань, Шэньчжэнь, провинция Гуандун, Юэ 0305 Мин Чу №14010 Гражданское решение от 25.11.2019 [9] о признании авторских прав у искусственного интеллекта. Противоположная точка зрения была выражена судом Австралии в решении об отказе в защите авторских прав искусственного интеллекта по делу IceTV Pty Limited v Nine Network Australia Pty Limited HCA 14 от 22.04.2009 [10].

Заключение. На наш взгляд, учитывая текущий уровень развития и осознанности искусственного интеллекта, говорить о наделении его правосубъектностью наравне с человеком преждевременно.

В будущем, если Четвертая промышленная революция, которая в соответствии с Концепцией Клауса Шваба предполагает повсеместное внедрение киберфизических систем (таких как искусственный интеллект, роботы, 3D-печать, нанотехнологии, биотехнологии) в производство и обслуживание человеческих потребностей, включая быт, труд и досуг, приведет к тому, что искусственный интеллект будет способен существовать, мыслить и творить автономно без участия человека, а также в случае, если изменится концепция понимания авторства, которая сейчас предполагает наличие “души” для создания уникального авторского произведения, юридическое сообщество сможет вернуться к вопросу о расширении субъектного состава правоотношений в сфере интеллектуальной собственности.

Список источников и литературы:

1. Грачева Д.А. Особенности развития права интеллектуальной собственности в контексте использования искусственного интеллекта // ЭКОНОМИКА. ПРАВО. ОБЩЕСТВО. 2022. Т. 7, № 4 (32). С. 20-25.

2. Гурко А.В. К вопросу о возможности правовой охраны результатов «интеллектуальной» деятельности систем искусственного интеллекта // ЭКОНОМИКА. ПРАВО. ОБЩЕСТВО. 2022. №1 (29). С. 76-86.

3. Калятин В.О. Объекты авторского права, созданные с использованием компьютера // Патенты и лицензии. Интеллектуальные права. 2011. № 5. С. 22-25.

4. Каштанова П.А. Перспективы правовой охраны произведений, создаваемых с использованием искусственного интеллекта в России // Журнал Суда по интеллектуальным правам. Март 2023. Вып. 1 (39). С. 120-132.

5. Ролинсон П., Ариевич Е.А., Ермолина Д.Е. Объекты интеллектуальной собственности, создаваемые с помощью искусственного интеллекта: особенности правового режима в России и за рубежом // Закон. 2018. № 5.

6. Свечников В.А. К вопросу об определении правовой природы искусственного интеллекта // ЭКОНОМИКА. ПРАВО. ОБЩЕСТВО. 2023. Т. 8, № 3 (35). С. 86-95.

7. Dan L. Burk. AI Patents and the Self-Assembling Machine. Available at: https://www.researchgate.net/publication/351591454_AI_Patents_and_the_Self-Assembling_Machine (Accessed: 15.11.2024).

8. L. Oguama. Intellectual Property and Artificial Intelligence: Emerging Prospects and Challenges. Available at: https://www.researchgate.net/publication/359095420_Intellectual_Property_and_Artificial_Intelligence_Emerging_Prospects_and_Challenges (Accessed: 15.11.2024).

9. Primary People’s Court of Nanshan District, China [2019]: Tencent Company v Yingxun Company, Case No. Y0305MC No. 14010. Available at: https://www.wipo.int/wipolex/ru/text/588679 (Accessed: 15.11.2024).

10. IceTV Pty Ltd v Nine Network Australia Pty Ltd [2009] HCA 14. Available at: https://www.wipo.int/wipolex/en/text/578440 (Accessed: 15.11.2024).

Тигран Давидович Оганесян,
к.ю.н., доцент кафедры международного права,
Дипломатическая академия МИД России,
E-mail: kafedra.mp@dipacademy.ru

Tigran D. Oganesian,
Ph.D. in Law, Associate Professor of the Department of International Law,
Diplomatic Academy of the Ministry of Foreign Affairs of Russia,
E-mail: kafedra.mp@dipacademy.ru

НАЦИОНАЛЬНАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ДАННЫХ: ОБНОВЛЕННЫЕ СТАНДАРТЫ ЕВРОПЕЙСКОГО ПРАВОСУДИЯ

NATIONAL SECURITY AND DATA PROTECTION: UPDATED STANDARDS OF EUROPEAN JUSTICE

Аннотация. В исследовании рассматриваются отдельные аспекты защиты персональных данных в контексте соотношения интересов национальной безопасности и права на уважение частной жизни. Особое внимание уделяется обновленным стандартам европейского правосудия, проанализированных сквозь призму практики ЕСПЧ по ключевым делам.

Ключевые слова: защита персональных данных; массовое наблюдение; конфиденциальность; право на уважение частной жизни; национальная безопасность; европейское правосудие.

Abstract. The study examines certain aspects of personal data protection in the context of the correlation of national security interests and the right to respect for private life. Special attention is paid to the updated standards of European justice, analyzed through the prism of the ECHR practice in key cases.

Keywords: protection of personal data; mass surveillance; confidentiality; the right to respect for private life; national security; European justice.

Несмотря на многочисленные преимущества, цифровой век создает проблемы для конфиденциальности и защиты персональных данных миллионов граждан. Массовое наблюдение и технологии, позволяющие

национальным органам хранить и обрабатывать данные миллионов людей, представляют серьезную угрозу для права на неприкосновенность частной жизни, гарантированное статьей 8 Конвенцией о защите прав человека и основных свобод 1950 г. (далее – Конвенция). В этой связи поиск баланса между интересами национальной безопасности и право граждан на защиту персональных данных приобретает не только особую актуальность, но ставит перед органами международного правосудия новые вопросы. Одним из таких органов является Европейский Суд по правам человека (далее − ЕСПЧ), которые за последние несколько лет попытался установить европейские стандарты по данному вопросу.

Обновленными стандартами можно считать правовые позиции ЕСПЧ по делу «Big Brother Watch и другие против Соединенного Королевства» [1] от 25 мая 2021 года. Дело касалось жалоб журналистов и правозащитных организаций на три различных режима слежки: (1) массовый перехват сообщений; (2) получение перехваченных материалов от иностранных правительств и разведывательных служб; (3) получение коммуникационных данных от поставщиков услуг связи. Большая палата ЕСПЧ постановила, что имело место нарушение статьи 8 Конвенции в отношении режима массового перехвата; что имело место нарушение статьи 8 в отношении режима получения коммуникационных данных от поставщиков услуг связи. Суд, в частности, счел, что из-за множества угроз, с которыми государства сталкиваются в современном обществе, введение режима массового перехвата само по себе не является нарушением Конвенции. Однако такой режим должен быть подчинен «комплексным гарантиям», что означает, что на национальном уровне на каждом этапе процесса должна проводиться оценка необходимости и соразмерности принимаемых мер; что массовый перехват должен осуществляться с независимого разрешения на национальном уровне. с самого начала, когда определялись цель и масштаб операции; и что эта операция должна подлежать надзору и независимой проверке задним числом.

Другое дело «Центрум Фор Раттвиса против Швеции» [2] от 25 мая 2021 года касалось предполагаемого риска того, что сообщения фонда-заявителя были или будут перехвачены и изучены средствами радиотехнической разведки Швеции. ЕСПЧ установил, что, хотя основные характеристики шведского режима массового перехвата соответствуют требованиям Конвенции о качестве законодательства, этот режим, тем не менее, страдает тремя недостатками: отсутствием четкого правила об уничтожении перехваченных материалов, которые не содержат персональных данных; отсутствием требования в сигналах Закон о разведке или другое соответствующее законодательство, согласно которому при принятии решения о передаче разведывательных материалов иностранным партнерам учитывались интересы частных лиц в области неприкосновенности частной жизни; и отсутствие эффективного контроля задним числом. В результате этих недостатков система не соответствовала требованию о «комплексных» гарантиях, она превысила пределы усмотрения, предоставленные государству-ответчику в этом отношении, и в целом не обеспечивала защиту от риска произвола и злоупотреблений.

Обновлением стандартов также можно считать постановление по делу «Гашчак против Словакии» [3] от 23 июня 2022 года, которое касалось операции по наблюдению, проведенной в 2005 и 2006 годах Словацкой разведывательной службой (SIS), и полученных ею разведывательных материалов. ЕСПЧ, в частности, отметил, что операция имела многочисленные недостатки, некоторые из которых были признаны на национальном уровне

Технология распознавания лиц в московском метро, в свою очередь, также стала предметом оценки ЕСПЧ в контексте защиты данных в деле «Glukhin v. Russia» [4]. Дело касалось использования российскими властями технологии распознавания лиц против заявителя, который устроил «одиночную демонстрацию» в московском метрополитене с картонной фигурой активиста Константина Котова в натуральную величину, дело

которого привлекло значительное внимание средств массовой информации. вызвав общественный резонанс. По словам заявителя, полиция использовала технологию распознавания лиц, чтобы идентифицировать его в социальных сетях, и собрала видеозаписи с камер видеонаблюдения в московском метро. По этой причине он был осужден за то, что не уведомил власти о своей демонстрации. И скриншоты соцсети, и записи с камер видеонаблюдения были использованы против него в административном процессе. Заявитель, в частности, утверждал, что его административное осуждение и использование технологии распознавания лиц при обработке его персональных данных нарушили его право на уважение частной жизни и свободу выражения мнений.

ЕСПЧ установил, что он обладает юрисдикцией для рассмотрения данного дела, поскольку факты, дающие основание для предполагаемых нарушений Конвенции, имели место до 16 сентября 2022 года, даты, когда Россия перестала быть участницей Европейской конвенции. ЕСПЧ постановил, что в отношении заявителя имело место нарушение статьи 8 (право на уважение частной жизни) Конвенции, установив, что обработка его биометрических персональных данных с использованием технологии распознавания лиц в рамках производства по делу об административном правонарушении − во-первых, для идентификации его по фотографиям а видеозапись, опубликованная в Интернете, и, во-вторых, обнаружение и арест его во время поездки в московском метро не соответствовали «насущной социальной потребности» и не могли рассматриваться как «необходимые в демократическом обществе».

Вышеупомянутые решения служат напоминанием о том, что технологии, используемые органами национальной безопасности, часто используются для сбора и хранения данных отдельных лиц и группы. Поэтому их использование должно тщательно регулироваться, а злоупотребление осуждаться. Существует множество других прав, которые могут соприкасаться с технологией распознавания лиц: вопросы равенства, дискриминации, свободы выражения мнения и т.д. Таким образом, нельзя не

видеть последствий обновленных стандартов для будущего законодательства европейских государств по этой теме.

Список источников и литературы:

1. Постановление ЕСПЧ по делу «Big Brother Watch и другие против Соединенного Королевства» от 25 мая 2021 года. URL: https://hudoc.echr.coe.int/eng-press?i=003-7028496-9484349 (дата обращения 24.11.2024)

2. Постановление ЕСПЧ по делу «Центрум Фор Раттвиса против Швеции» от 25 мая 2021 года. URL: https://hudoc.echr.coe.int/eng-press?i=003-7028476-9484327 (дата обращения 24.11.2024)

3. Постановление ЕСПЧ по делу «Гашчак против Словакии» от 23 июня 2022 года. URL: https://hudoc.echr.coe.int/eng-press?i=003-7367294-10067169 (дата обращения 24.11.2024)

4. Постановление ЕСПЧ по делу «Глухин против России» от 4 июля 2023 года. URL: https://hudoc.echr.coe.int/eng-press?i=003-7694109-10618091 (дата обращения 24.11.2024)

Александр Владимирович Орешеч,
советник Уполномоченного по правам человека в Брянской области,
преподаватель Брянского филиала РАНХиГС
при Президенте Российской Федерации,
E-mail: akteon757@yandex.ru

Alexander V. Oreshech,
Advisor to the Ombudsman in the Bryansk region, lecturer at the Bryansk branch of RANEPA under the President of the Russian Federation,
E-mail: akteon757@yandex.ru

ОСОБЕННОСТИ СОБЛЮДЕНИЯ И ЗАЩИТЫ ЦИФРОВЫХ ПРАВ ГРАЖДАН

FEATURES OF OBSERVANCES AND PROTECTION OF DIGITAL RIGHTS OF CITIZENS

Аннотация. Целью данной статьи является рассмотрение проблем, с которыми сталкиваются правозащитные организации при защите прав и свобод человека и гражданина в границах конкретного региона России. В статье исследуется текущее состояние защиты прав в цифровой сфере, освещаются основные риски и изменения, а также приводится анализ правовой базы и законодательных предложений в области цифровых прав человека и гражданина.

Ключевые слова: цифровые права, правозащитные организации, цифровизация, защита прав в цифровой среде, Уполномоченный по правам человека в Брянской области, юридическая помощь.

Abstract. The purpose of this article is to examine the challenges faced by human rights organizations in safeguarding human and civil rights and liberties within the borders of a specific region in Russia. The article explores the current state of rights protection in the digital realm, highlights crucial risks and developments, and provides an analysis of the legal framework and legislative proposals in the area of digital human and civil rights.

Keywords: digital rights, human rights organizations, digitalization, protection of rights in the digital environment, Ombudsman in the Bryansk region, legal assistance.

Сегодня цифровизация всех сфер жизнедеятельности, в особенности темпы ее развития, самым непосредственным образом влияет на права человека. Она упрощает механизм реализации традиционных прав и расширяет возможности по их защите. Большинство граждан, в особенности молодого возраста, посредством цифровых сервисов обращаются в органы государственной власти, оплачивают услуги, покупают товары, совершают множество сделок. Не ограничена скорость обмена и распространения информации через сервисы электронной почты и мессенджеры.

С уверенностью можно сказать, что в Российской Федерации сформировано новое поколение прав человека – цифровые права. Под цифровыми правами понимаются права людей на доступ, использование, создание и публикацию цифровых произведений, на доступ и использование компьютеров и иных электронных устройств, а также коммуникационных сетей, в частности сети интернет, беспрепятственный обмен информацией между пользователями сети интернет. В их число можно включить такие права как, право на цифровую подпись, на защиту персональных данных, а также право свободно общаться и выражать свое мнение, право на забвение и другие.

В сфере информационного права действуют Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» и целый ряд связанных с ним других законодательных актов, регулирующих оборот информации, в том числе «О персональных данных», «О защите детей от информации, причиняющей вред их здоровью и развитию» и др.

В 2023 году Межпарламентской Ассамблеей государств-участников СНГ были приняты два модельных закона «О цифровых правах» и «О цифровом пространстве, его инфраструктуре и регулировании в государствах-

участниках СНГ».

В Резолюции Генеральной Ассамблеи ООН от 18 декабря 2013 г. №68/167 «Право на неприкосновенность личной жизни в цифровой век» отмечается, что быстрые темпы технологического развития позволяют людям во всех регионах мира пользоваться новыми информационными и коммуникационными технологиями и в то же время повышают способность правительств, компаний и физических лиц отслеживать, перехватывать и собирать информацию, что может нарушать или ущемлять права человека (особенно право на неприкосновенность личной жизни) [2].

К сожалению, цифровизация наряду с возможностями представляет и угрозы. Отмечается высокий рост преступности с использованием информационных технологий и довольно невысокий процент случаев, в которых можно защитить и восстановить права потерпевших. Остро стоит проблема защиты персональных данных. Нередко взламываются кабинеты сервисов государственных услуг, а личная информация гражданина становится доступной для мошенников.

Значительная часть преступлений в финансовой сфере совершена с помощью информационно-телекоммуникационных технологий. Еженедельно жители Брянской области переводят на счета мошенников более 10 миллионов рублей.

Самыми распространенными способами совершения данных преступлений по-прежнему остаются мошенничества, совершенные при осуществлении следующих операций: списание денежных средств под предлогом разблокировки банковской карты либо предотвращения списания денежных средств; под предлогом покупки (продажи) товара в сети Интернет путем получения сведений о реквизитах банковской карты; перечисление денежных средств под предлогом покупки (продажи) товара в сети Интернет путем оплаты (предоплаты) за товар; перечисление либо передача денежных средств под предлогом не привлечения к уголовной ответственности родственников и знакомых потерпевших; под предлогом выдачи кредитов,

займов в сети Интернет; под предлогом получения компенсации за ранее приобретенные биологические активные добавки, а так же оказания помощи экстрасенсами; перечисление денежных средств, совершенное посредством взлома персональных станиц (аккаунтов) в социальных сетях.

В связи с активно развивающейся сферой применения информационных технологий, позволяющей злоумышленниками приобретать и использовать неидентифицируемые SIM-карты, пользоваться услугами IP-телефонии, программными технологиями виртуальных частных сетей «VPN», криптографических протоколов для безопасной связи «SSL», различных способов шифрования данных на распространенных интернет-сервисах, программ по подмене абонентского номера, а также возможностей зарубежных телекоммуникационных компаний, позволяющих менять адрес пользователя в сети Интернет, и таким образом избегать идентификации, установление местонахождения преступников не только усложняется, но и становится практически невозможной.

В связи с этим целесообразно совершенствование нормативно-правовой базы в части ужесточения требований для пользователей «IP- телефонии» с целью устранения анонимного использования данной услуги.

В соответствии с п. 9 ст. 46 Федерального закона РФ «О связи» оператор связи, пропуская через сеть вызовы, осуществленные с подменой абонентского номера, не выполняет обязанность, возложенную на него законодательством Российской Федерации передать абонентский номер в неизменном виде.

В 2024 году Федеральная служба безопасности Российской Федерации потребовала у российских операторов связи запретить предоставлять клиентам возможность использовать VoIP-аккаунты как с иностранных IP-адресов, так и принадлежащих российским провайдерам хостинга, а подведомственное Роскомнадзору ФГУП «Главный радиочастотный центр» разослало операторам связи уведомление о запрете пропускать звонки с номеров телефонов, не загруженных в систему «Антифрод». По новым

требованиям они не должны пропускать звонки своим абонентам от операторов, не подключенных к данной системе [4].

Несмотря на эти шаги, предпринятые контролирующими органами государственной власти, данная проблема не решена, и жители страны ежедневно становятся жертвами мошеннических действий в цифровом пространстве. Одной из острых проблем в данной сфере можно назвать нарушение прав потерпевшего на возмещение материального и морального вреда.

К факторам риска следует отнести недостаточную цифровую и юридическую грамотность населения, в связи с чем на постоянной основе необходимо проводить профилактическую работу с населением.

В конце 1990-х годов, в период становления государства и бурным ростом законодательного потока, в российском обществе появился спрос на правовую информацию. В этой связи, совместными усилиями ФАПСИ, Минкультуры России и региональных властей было найдено решение по использованию общедоступных библиотек в качестве мест общественного доступа к информации, построения на их основе сети публичных центров правовой информации. Создание таких центров позволило гражданам получить бесплатный доступ к электронным справочным правовым системам [3].

Вместе с тем, сегодня не все граждане могут воспользоваться информационной системой ввиду низкого уровня не только правовой, но и цифровой грамотности. Многим нуждающимся в правовой поддержке необходимы разъяснения норм законодательства в конкретной жизненной ситуации.

Одним из основных направлений деятельности Уполномоченного по правам человека в Брянской области является содействие правовому просвещению по вопросам прав и свобод человека и гражданина. Разъяснение и правовые консультации в процессе работы с обращениями граждан, общение во время личного приема, размещение информации на различных интернет-

площадках, выпуск ежегодных и специальных докладов – это основной, но не полный список форм правового просвещения населения Брянщины.

Цифровые инструменты активно внедряются в правозащитную среду. Из цифровых сервисов уполномоченных по права человека можно отметить интернет-приемные, через которые наблюдается рост обращений граждан. Сегодня готовится информационная федеральная система «ГИС УПЧ».

Одним из направлений содействия в правовом просвещении Уполномоченного по правам человека в Брянской области является организация и проведение юридических консультаций граждан сотрудниками аппарата Уполномоченного, на базе Публичного центра правовой информации Брянской областной научной универсальной библиотеки имени Ф.И. Тютчева [1].

Жители Брянской области могут обратиться к специалистам за разъяснением законодательства в сфере прав человека и гражданина, дополнительно могут получить информацию о компетенции государственных органов и порядке обращения к ним. Сегодня к этой работе присоединились сотрудники правоохранительных органов, адвокаты и нотариусы.

В заключении считаю необходимым отметить, что решением вышеназванных проблем может стать объединение законодательства, регулирующего права человека в цифровом пространстве и, возможно, создание Цифрового кодекса Российской Федерации. Еще в 2018 году Председатель Конституционного Суда Российской Федерации Валерий Зорькин на Петербуржском международном форуме в Санкт-Петербурге отмечал необходимость создания такого документа.

Вместе с тем, в 2023 году Совет при Президенте Российской Федерации по кодификации и совершенствованию гражданского законодательства отверг идею разработки Цифрового кодекса, в том числе ввиду того, что стабильность закрепленных им обобщающих правил, невозможно обеспечить в условиях бурного развития цифровых технологий, что в свою очередь потребует постоянной корректировки содержания норм такого кодекса [5].

Безусловно невозможно не согласиться с данным заключением, однако разработка основных правил регулирования в сфере информационных технологий и цифровых прав граждан, их систематизация, необходима уже сейчас.

Список источников и литературы:

1. Ежегодные доклады Уполномоченного по правам человека в Брянской области. URL: https://ombudsman.bryansk.in (дата обращения 24.11.2024)

2. Зорькин В.Д. Право в цифровом мире: выступление на Петербургском международном юридическом форуме // Российская газета. №115. 2018.

3. Официальный сайт Федеральной службы охраны Российской Федерации. URL: http://fso.gov.ru (дата обращения 24.11.2024)

4. ФСБ ввела новые ограничения для пользователей IP-телефонии / РБК. URL: https://www.rbc.ru/technology_and_media/04/07/2024/668570169a79479ffd56d8bc (дата обращения 24.11.2024)

5. Экспертное заключение по проекту федерального закона № 411043–8 «О внесении изменений в часть четвертую Гражданского кодекса Российской Федерации» (в части установления порядка использования отдельных объектов авторских и смежных прав, правообладатели которых неизвестны), принято на заседании Совета при Президенте Российской Федерации по кодификации и совершенствованию гражданского законодательства 1 декабря 2023 г. № 235-2/2023.

Наталья Валерьевна Савельева,
младший научный сотрудник,
Институт физики Земли им. О.Ю. Шмидта РАН,
выпускник магистратуры МГЮА им. О.Е. Кутафина,
независимый исследователь в области
международного космического права,
E-mail: nasa2000@yandex.ru

Natalie V. Savelyeva
Researcher, Schmidt Institute of the Earth Physics
of the Russian academy of science
Magister of International Law, Kutafin Moscow State Law University,
Independent Researcher in the International Space Law,
E-mail: nasa2000@yandex.ru

ВОЗМОЖНОСТИ РАСПРОСТРАНЕНИЯ ПОЛОЖЕНИЙ КОНВЕНЦИИ ООН ПРОТИВ КИБЕРПРЕСТУПНОСТИ НА КИБЕРПРЕСТУПЛЕНИЯ В ОТНОШЕНИИ СПУТНИКОВЫХ СИСТЕМ

CYBERCRIMES IN OUTER SPACE AND CRIMINAL JURISDICTION OF STATES: INTERNATIONAL LEGAL ANALYSIS

Аннотация. XXI век ознаменовался стремительным развитием информационно-коммуникационных технологий (ИКТ) и их активным применением в космосе, в частности, при реализации систем космической связи, навигации, глобальных спутниковых группировок для дистанционного зондирования Земли. Киберпространство стремительно расширяется, выходит в космос и становится глобальной ареной антропогенной деятельности. Регулирование отношений в киберпространстве давно вышло за рамки национальных юрисдикций. Для обеспечения эффективного взаимодействия в киберпространстве, как и в космосе, необходимы универсальные международно-правовые инструменты. Работа по созданию таких инструментов ведется давно, при активном участии нашей страны. В начале августа 2024 года прошла заключительная сессия Специального комитета ООН по разработке всеобъемлющей конвенции по противодействию информационной преступности. По итогам сессии 9 августа 2024 года был

единогласно принят итоговый проекта будущей конвенции и вынесен на утверждение 79-й сессией Генеральной Ассамблеи ООН. Согласно проекту новой конвенции, криминализации подлежат такие правонарушения, как незаконный доступ, незаконный перехват, воздействие на электронные данные и информационные системы и пр. Также конвенция предусматривает ответственность юридических лиц за совершение преступлений с использованием ИКТ. Ниже приводятся результаты исследования возможности применения составов правонарушений, предусмотренных статьями 7-10 указанной конвенции, при рассмотрении дел, связанных с незаконным использованием систем космической связи, навигации и дистанционного зондирования Земли из космоса.

Ключевые слова: международное космическое право, информационно-коммуникационные технологии, информационная безопасность, киберпреступления, уголовная юстиция, спутники, спутниковые группировки

Abstract. The XXI century was marked by the rapid development of information and communication technologies (ICT) and their active application in space, in particular, in the implementation of space communication systems, navigation, global satellite groupings for remote sensing of the Earth. Today we experience rapid expansion of cyber activities into space domain, its transformation into a global environment for activities of millions of people. Legal regulation of those activities in the cyber space has long gone beyond national jurisdictions. Universal international legal instruments are needed to ensure effective interaction in either cyber or in outer space. Development of such instrument took has been underway for a long time, with the active participation of the Russian Federation. In early August 2024, the final session of the UN Ad Hoc Committee on the Development of a Comprehensive Convention on Combating Information Crime was held. Following the session on August 9, 2024, the final draft of the future convention was unanimously adopted and submitted for approval by the 79th session of the UN General Assembly. According to the draft, offences such as illegal access, illegal interception, impact on electronic data and information systems, etc. are

subject to criminalization. The Convention also provides for the liability of legal entities for committing crimes using ICT. This paper deals with the problem of applying the provisions of the articles 7-10 of the said Convention to illegal use of space communications, navigation and remote sensing systems from space.

Keywords: international space law, information and communication technologies, information security, criminal jurisdiction, satellites, satellite.

Введение. В последние годы проблема защиты спутниковых бортовых систем от киберугроз становится все более актуальной. К примеру, в России взлом низкоорбитального спутника RUVDS был включен в состав задач киберучений, которые проводились в июле 2023 года на киберполигоне Standoff [22]. В США в рамках конференции DEF CON 31 [7] в августе 2023 года был организован открытый хакатон Hack-A-Sat 4 по взлому исследовательского кубсата Moonlighter [26], запущенного в интересах армейского командования космических сил США.

Существуют объективные факторы, почему вопросы кибер-безопасности спутников становятся все более насущными с каждым годом:

- рост общего числа спутников на орбите (12 224 по данным UNOOSA [18]);
- коммерциализация отраслей космической связи неминуемо приводит к стандартизации, использованию типовых готовых решений;
- доступность на открытом рынке готовых технологий и продуктов, используемых для производства серийных коммерческих спутников;
- использование прошивок [9] и ПО с открытым кодом [8], доступность технической документации на отдельные системы;
- привлечение сторонних подрядчиков из коммерческого сектора создает риски взлома наземного пункта управления (например, атака на сеть Центра управления полетами Кеннеди в 2005 году [17]);
- возможность создания фальшивых, либо аренды наземных станций связи [6].

Последствия киберпреступлений в отношении спутников могут быть катастрофическими, причем не только для самих спутников, к примеру:

- вывод из строя спутника (к примеру, захват спутника ROSAT в 1998 году и вывод из строя солнечных батарей [16]);
- дестабилизация работы спутникового оборудования (к примеру, атака на спутники дистанционного зондирования Земли[7]);
- перехват и подмена широковещательных сигналов для трансляции определенного контента [5], либо с целью дезинформации [3];
- взлом и перехват спутникового канала связи (к примеру, для маскировки места нахождения серверов, используемых для атак ботнетов группировкой Turla [25], использование бразильскими преступными группировками спутников военной связи США [24], незаконное использовали террористическими формированиями терминалов Starlink [1] в обход территориальных ограничений);
- глушение сигнала спутников навигации и (или) связи для дестабилизации работы критической инфраструктуры, управления воздушным, морским или дорожным движением [4].

Стоит отметить, что методы незаконного доступа к спутникам развиваются, появляются все новые угрозы, к примеру, уже не является невозможной ситуация, когда преступная группировка запускает собственный спутник для незаконного доступа к бортовым системам космических аппаратов на орбите по каналам межспутниковой связи.

Ответственность за киберпреступления в международном праве. До недавнего времени в международном праве отсутствовали универсальные инструменты, регулирующие вопросы ответственности за киберпреступления. В Договоре о космосе 1967 года [2] и связанных документах кибер-угрозы не упоминаются в принципе. Тем не менее, термины «кибератака», «незаконный

[7] К примеру, вмешательство в работу спутников Landsat-7 и Terra AM-1 в 2008 году через станцию связи Svabald на Шпицбергене. URL: https://www.space.com/13423-hackers-government-satellites.html (дата обращения: 21.10.2024)

доступ» или «незаконное использование» подразумевают активное воздействие на объект с использованием ИКТ с корыстными и (или) политическими целями, что противоречит основным принципам международного сотрудничества в космосе, отраженным в системообразующих документах международного космического права, согласно которым космическая инфраструктура может использоваться исключительно в мирных целях. Возникает вопрос, какая ответственность может быть возложена за подобные проступки?

На региональном уровне в отношении международных киберпреступлений применяется Конвенция о преступности в сфере компьютерной информации ETS 185, подписанная в Будапеште 23 ноября 2001 г., известная как «Будапештская конвенция» [23]. Это первый международно-правовой инструмент, в первую очередь регулирующий вопросы уголовной ответственности за киберпреступления «*против конфиденциальности, целостности и доступности компьютерных данных и систем*» [23].

Между странами СНГ действует Соглашение о сотрудничестве в борьбе с преступлениями в сфере информационных технологий [11], в котором предусмотрены восемь составов уголовно-наказуемых деяний в сфере ИТ, а также процедурные моменты взаимодействия при расследовании оных.

Лигой арабских государств в 2010 году была принята Конвенция о борьбе с преступлениями в области информационных технологий [14] с целью унификации национального законодательства по борьбе с киберпреступлениями. Между странами ШОС в 2010 году заключено Соглашение о сотрудничестве в области обеспечения международной информационной безопасности [10], приложение 2 которого содержит согласованный список кибер-угроз. В 2014 году была принята Конвенция Африканского союза о кибер-безопасности и защите персональных данных [13]. В ЕС имеется ряд директив, регулирующих вопросы кибер-безопасности, к примеру, Директива об атаках на информационные системы [15], которая

была принята прежде всего для противодействия крупномасштабным кибер-атакам путем введения жестких уголовных наказаний в национальное законодательство стран-участников ЕС.

В национальных законах о космической деятельности ответственность за киберпреступления в космосе, как правило, специально не оговаривается. Следует отметить, что сфера применения национального законодательства в космосе ограничена, так как в соответствии с международным космическим правом, космос и небесные тела являются достоянием всего человечества и не подлежат национализации. Соответственно, никакая страна не обладает «полноценной» юрисдикцией за пределами своих космических кораблей или конструкций.

Важной вехой в области развития международного сотрудничества государств стало принятие в августе 2024 года и вынесение на утверждение 79-й сессии Генеральной ассамблеи ООН [12] проекта всеобъемлющей конвенции по кибер-преступности [21] (далее – «Конвенция»). Конвенция решает две важнейшие задачи: унификация национального законодательства по борьбе с кибер-преступностью и формирование правового базиса международного сотрудничества по предотвращению, расследованию киберпреступлений и судебному преследованию за оные. В сравнении с действующими региональными соглашениями, Конвенция обладает рядом преимуществ:

1. Универсальность: возможность противодействия транснациональной организованной преступности и терроризму. Следует отметить, что ратифицировать Конвенцию имеют право не только государства и ММПО, но и уполномоченные «региональные организации экономической интеграции», что делает Конвенцию модельным законом не только для государств, но и региональных объединений различного толка.

2. Унификация составов киберпреступлений (Глава II, статьи 7-17). Стоит отметить, что изначально Российская Федерация предлагала 30 криминализировать около 30 деяний, однако ввиду противодействия стран т.н.

«западной коалиции» во главе с США, в итоговый текст Конвенции не вошли преступления, связанные с террористической и экстремистской деятельностью, распространением наркотиков, незаконным оборотом оружия, склонение к самоубийству, реабилитация нацизма и др.

3. Унификация процессуальных полномочий при расследовании киберпреступлений (Глава IV). Здесь следует отметить, что в статье 5 Конвенции явным образом прописан запрет трансграничного доступа в данным, то есть, впервые в универсальном международном договоре применена концепция «цифрового суверенитета» государства. Отсутствие подобного запрета в Будапештской конвенции стало причиной отказа Российской Федерации от ее подписания.

4. Фиксация механизмов взаимодействия для расследования киберпреступлений путем создания национальных контактных центров (Глава V, статья 41 «Сеть 24/7» отслеживание и возвращение доходов от преступлений, совместные расследования, сбор и передача технических данных и содержимого сообщений).

Хотя Конвенция предусматривает уголовную, административную, гражданско-правовую ответственность только для физических и юридических лиц, сам факт криминализации широкого списка деяний является мощным сдерживающим фактором не только в отношении частных лиц и организованных транснациональных преступных групп, но и отдельных представителей публичной власти. Политику государств и ММПО формируют отдельные личности, либо властные группировки, которые могут быть привлечены к ответственности за превышение полномочий в случае использования своей власти для совершения деяний, признанных уголовно-наказуемыми на международном уровне.

Выводы относительно применимости положений Конвенции к спутниковым системам. Современные спутники – это автономные беспилотные программно-аппаратные комплексы. Небольшое изменение данных может привести к сбою в работе программных средств и выводу из

строя ключевых систем или даже всего спутника. К примеру, изменение параметров ориентации солнечных батарей может привести либо к перегреву системы, либо полностью лишить спутник электричества, если панели будут раскрываться только в тени Земли. Поэтому очень важно, что в Конвенции речь идет не просто о действиях в отношении данных (статья 9), но информационно-коммуникационных систем (ИКС) в целом (статьи. 7-8, 10), а также о неправомерном использовании любых устройств (статья 11) или ИКС в целом (статьи 12-13) для совершения преступлений.

Для оценки практической эффективности новой Конвенции потребуются десятилетия. Тем не менее, сам факт согласования проекта первого универсального международного договора о противодействии кибер-преступности является большим достижением, прежде всего, отечественной дипломатии, так как именно Российская Федерация выступила инициатором и стала основной движущей силой принятия Конвенции.

Список источников и литературы:

1. ВСУ взломали терминалы Starlink, чтобы использовать интернет бесплатно. URL: https://www.mk.ru/politics/2024/04/19/vsu-vzlomali-terminaly-starlink-chtoby-ispolzovat-internet-besplatno.html?ysclid=m2iveotx3n66589682 (дата обращения: 21.10.2024)

2. Договор о принципах деятельности государств по исследованию и использованию космического пространства, включая Луну и другие небесные тела. Принят резолюцией 2222 (XXI) Генеральной Ассамблеи от 19 декабря 1966 года. Официальный сайт ООН. [URL: https://www.un.org/ru/documents/decl_conv/conventions/outer_space_governing.shtml (дата обращения: 22.10.2024).

3. Заведомо-ложные сообщения о воздушной тревоге 28 февраля 2023 года. URL: https://lenta.ru/news/2023/02/28/channels/ (дата обращения: 19.10.2024).

4. Заявление МИД России в связи с попытками киевского режима воздействовать на российские гражданские спутники связи. URL: https://mid.ru/ru/foreign_policy/news/1862007/ (дата обращения: 21.10.2024).

5. Массовый взлом спутникового ТВ (09.05.2024). URL: https://tv-incidents.fandom.com/
ru/wiki/Массовый_взлом_спутникового_ТВ_(09.05.2024) (дата обращения: 19.10.2024).

6. Наземные станции как сервисы или системы GSaaS (Ground Station as a Service) разработки Amazon URL: https://aws.amazon.com/ru/ground-station/ и Microsof URL: https://azure.microsoft.com/en-us/products/orbital/ (дата обращения: 19.10.2024).

7. Официальный сайт конференции DEF CON. URL: https://defcon.org/ (дата обращения: 19.10.2024).

8. ПО спутника Чилийского университета SUCHAI Cubesat на GitHub. URL: https://github.com/spel-uchile/SUCHAI (дата обращения: 19.10.2024).

9. Прошивка студенческого спутника OreSat Принстонского университета на GitHub на базе ChibiOS для микроконтроллеров M0 и M4. URL: https://github.com/oresat/oresat-firmware (дата обращения: 19.10.2024).

10. Соглашение между правительствами государств − членов ШОС о сотрудничестве в области обеспечения международной информационной безопасности. Официальный интернет-портал правовой информации. URL: http://pravo.gov.ru/proxy/ips/?docbody=&link_id=198&nd=203002652&collection=1&ysclid=m2k8o7u5p4639107584 (дата обращения: 22.10.2024).

11. Соглашение о сотрудничестве государств − участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий, Душанбе, 28 сентября 2018 года. Официальный интернет-портал правовой информации. URL: http://publication.pravo.gov.ru/Document/View/0001202207180005?ysclid=m2g7a621x9793411749 (дата обращения: 22.10.2024).

12. Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes. Available at: https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home (Accessed: 22.10.2024).

13. African Union Convention on Cyber Security and Personal Data Protection. Available at: https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection (дата обращения: 22.10.2024).

14. Arab Convention on Combating Information Technology Offences. Available at: https://itlaw.fandom.com/wiki/Arab_Convention_on_Combating_Information_Technology_Offences (Accessed: 22.10.2024).

15. Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA. Available at: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:218:0008:0014:EN:PDF (Accessed: 22.10.2024).

16. Hackers could shut down satellites – or turn them into weapons. URL: https://theconversation.com/hackers-could-shut-down-satellites-or-turn-them-into-weapons-130932 (дата обращения: 19.10.2024).

17. NASA Computers Hacked By Intruders. URL: https://www.satellitetoday.com/government-military/2008/12/01/nasa-computers-hacked-by-intruders/ (дата обращения: 19.10.2024).

18. Online Index of Objects Launched into Outer Space. Official site UNOOSA. URL: https://www.unoosa.org/oosa/osoindex/ (дата обращения: 22.10.2024).

19. Open-ended working group on security of and in the use of information and communications technologies 2021–2025. Available at: https://meetings.unoda.org/meeting/57871/documents?f%5B0%5D=document_type_meeting%3AFinal%20reports (Accessed: 22.10.2024).

20. Outer Space and Cyber Space. Similarities, Interrelations and Legal Perspectives edited by Annette Froehlich, European Space Policy Institute, Vienna, Austria; Springer Nature Switzerland AG, 2021, ISBN 978-3-030-80022-2 ISBN 978-3-030-80023-9 (eBook).

21. Reconvened concluding session of the Ad Hoc Committee. Available at: https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/ahc_reconvened_concluding_session/main (Accessed: 22.10.2024).

22. Standoff 12. Перезагрузка: новый формат киберучений поможет компаниям построить результативную безопасность. URL: https://www.ptsecurity.com/ru-ru/about/news/standoff-12-perezagruzka-novyj-format-kiberuchenij-pomozhet-kompaniyam-postroit-rezultativnuyu-bezopasnost/?sphrase_id=295536 (дата обращения: 19.10.2024).

23. The Budapest Convention (ETS No. 185) and its Protocols. Available at: https://www.coe.int/en/web/cybercrime/the-budapest-convention (Accessed: 22.10.2024).

24. The Great Brazilian Sat-Hack Crackdown. URL: https://www.wired.com/2009/04/fleetcom/ (дата обращения: 19.10.2024).

25. Turla и спутниковый интернет: управление APT-атаками в небе. URL: https://securelist.ru/turla-i-sputnikovyj-internet-upravlenie-apt-atakami-v-nebe/26923/ (дата обращения: 19.10.2024).

26. Uncle Sam wants DEF CON hackers to pwn this Moonlighter satellite in space. URL: https://www.theregister.com/2023/06/03/moonlighter_satellite_hacking/ (дата обращения: 19.10.2024).

Руслан Васильевич Собко,
к.ф.н., доцент кафедры ГиСЭД ПФ РГУП
E-mail: r.sobco@mail.ru

Татьяна Леонидовна Тян-Юшан,
студентка юридического факультета ПФ РГУП
E-mail: tatiianaaaaa@yandex.ru

Ruslan V. Sobko,
Ph.D. in Philosophy, Associate Professor,
GISED Department, PF RGUP,
E-mail: r.sobco@mail.ru

Tatyana L. Tyan-Yushan,
student of the Faculty of Law of the PF RGUP
E-mail: tatiianaaaaa@yandex.ru

ПРАВОВОЕ РЕГУЛИРОВАНИЕ БЕСПИЛОТНЫХ ТРАНСПОРТНЫХ СРЕДСТВ В РОССИИ И ЗАРУБЕЖНЫХ СТРАНАХ

LEGAL REGULATION OF UNMANNED VEHICLES IN RUSSIA AND FOREIGN COUNTRIES

Аннотация. Данная статья направлена на проведение анализа проблематики правового регулирования сфера эксплуатации беспилотных транспортных средств. В работе рассмотрена особенности функционирования беспилотных транспортных средств, нормативно-правовая база регулирования сферы их использования в разных странах. Актуальность исследования обусловлена необходимостью разработки эффективных механизмов правового регулирования искусственного интеллекта в транспортных средствах, которые позволят обеспечить безопасность общества и установят ответственность при ДТП и в других ситуациях. Научная новизна исследования заключается в комплексном анализе проблем правового регулирования автономных транспортных средств и разработке предложений по их решению. В результате проведенного анализа предложены

меры по совершенствованию законодательства в целях недопущения правовых коллизий.

Ключевые слова: беспилотный автомобиль, искусственный интеллект, автономность, автопилот, законодательство, ответственность.

Abstract. This article is aimed at analyzing the problems of legal regulation of the sphere of operation of unmanned vehicles. The paper considers the features of the functioning of unmanned vehicles, the regulatory framework for regulating the scope of their use in different countries. The relevance of the study is due to the need to develop effective mechanisms for the legal regulation of artificial intelligence in vehicles, which will ensure the safety of society and establish liability in case of an accident and in other situations. The scientific novelty of the research lies in a comprehensive analysis of the problems of legal regulation of autonomous vehicles and the development of proposals for their solution. As a result of the analysis, measures are proposed to improve legislation in order to prevent legal conflicts.

Keywords: self-driving car, artificial intelligence, autonomy, autopilot, legislation, responsibility.

В последнее время большую популярность и огласку приобрели беспилотные (или автономные) автомобили, которые способны частично или полностью заменить водителя за счет использования искусственного интеллекта. Как утверждают разработчики, по уровню безопасности управления транспортным средством искусственный интеллект в несколько раз превосходит человека. Но практика показывает несовершенство законодательства в разных странах, поэтому правовое регулирование использования беспилотных автомобилей является важной задачей, стоящей перед законодателями во всем мире.

Механизм работы беспилотных автомобилей. В работе рассматриваются механизм работы беспилотных автомобилей, который включает в себя такие устройства, как камера, радар, датчики и лидар,

позволяющие передать информацию в сервер транспортного средства. Это позволяет искусственному интеллекту оценивать ситуацию на дороге и принимать верное решение [11]. Беспилотные автомобили приобретают все большую популярность, как на Российских дорогах, так и за рубежом. Самые известные производители автономных транспортных средств: Tesla, Audi, Яндекс, Камаз.

Практика использования беспилотных автомобилей. Практика показывает, что данный вид транспорта не совсем «автономный» и требует наличие водителя внутри автомобиля для контроля дорожной ситуации. Первая авария с участием беспилотного автомобиля произошла во Флориде (США) в мае 2015 г., в результате которой погиб водитель. Автомобиль Tesla на режиме автопилота протаранил тягач с прицепом на перекрестке. Сама компания Tesla, комментируя ДТП, утверждала, что никакой неисправности в машине не было выявлено, но, по мнению компании, причина ДТП может состоять в том, что автоматика не успела распознать опасность из-за белого цвета прицепа грузовика на фоне яркого неба. Но не был решён и вопрос об уголовной ответственности за причинённый вред. Рассмотрев практику, возникает вопрос о правовом регулировании использования беспилотных автомобилей в настоящее время, а в особенности вопрос об ответственности в случае ДТП.

Законодательство о беспилотных автомобилях. В Германии в 2017 году принят закон, согласно которому беспилотные автомобили могут осуществлять движение по дорогам общего пользования только в случае нахождения за рулем человека и установка бортового самописца. Закон Германии также увеличивает ответственность того, кто управляет машиной с автопилотом. То есть если человек отвлекается от вождения, но через 5 секунд система требует того, чтобы он вспомнил об управлении. Если говорить об ответственности, в Германии действует презумпция виновности, согласно которой в случае ДТП виновным будет владелец транспортного средства, если

не докажет, что виной аварийной ситуации стала неисправность беспилотного транспортного средства [4].

В США нет общего закона, действующего на территории всех штатов, но есть документ, содержащий нормы рекомендательного характера, которые юридически не являются обязательными [6]. В большинстве штатов США (Калифорния, Сан-Франциско, Нью-Йорк) официально разрешено передвижение беспилотных автомобилей по дорогам общего пользования. Хоть и США принято считать одним из лидеров в испытании и внедрении автономных автомобилей, на момент 2024 года некоторые штаты ограничили передвижение беспилотных автомобилей из-за большого количества ДТП с их участием [7]. Например, в конце марта 2024 года администрация Нью-Йорка объявила о новых правилах по эксплуатации в городе беспилотных транспортных средств. Испытывать такие автомобили без водителя, готового в любой момент взять управление на себя, запрещается [5]. Также в США в апреле 2024 года опубликовали документ, согласно которому с 2029 года все производимые беспилотные автомобили должны будут оснащаться системой экстренного торможения (AEB).

В Российской Федерации 8 августа 2023 года Правительство РФ вынесло Постановление №1296 «О внесении изменений в пункт 89 Программы экспериментального правового режима в сфере цифровых инноваций по эксплуатации высокоавтоматизированных транспортных средств в отношении реализации инициативы "Беспилотные логистические коридоры" на автомобильной дороге общего пользования федерального значения М-11 "Нева"» [2]. 10 июня 2021 года Министерство Транспорта Российской Федерации представило законопроект «О высокоавтоматизированных транспортных средствах» [3]. Предполагается, что закон в случае принятия законопроекта вступит в силу только с 1 марта 2025 года. Законопроект установил, что при ДТП виновным считается владелец, находившийся в машине, если причиной аварии не стали недостатки автомобильного средства [10]. В таком случае водитель имеет право обратиться к компании-

изготовителю за возмещением вреда. То есть действует презумпция виновности: водитель виноват, если не докажет обратного. [8] Можно сделать вывод о развитии норм, регулирующих использование беспилотных транспортных средств на дорогах общего пользования. Несмотря на существование законопроекта и повсеместного развития законодательства в сфере регулирования беспилотных автомобилей, эксплуатация данного вида транспорта требует более детальной проработки и недопущения правовых коллизий.

В первую очередь, необходимо выделить правила допуска беспилотных автомобилей общего пользования, а также критерии, по которым автомобиль может быть отнесен к высокоавтоматизированным. Ведь существуют автомобили, оснащенные функциями искусственного интеллекта, но не могут осуществлять автономно осуществлять движение. Например, автомобили китайских производителей оснащены функцией автоматического паркинга.

Также существует проблема отсутствия единой нормы УК, регулирующую дорожно-транспортную ситуации с участием беспилотного автомобиля. В случае вины водителя транспортного средства за основу можно взять ст.264 УК РФ (Нарушение правил дорожного движения и эксплуатации транспортных средств). Так как в основу функционирования высокоавтоматизированного транспортного средства заложен искусственный интеллект, являющийся компьютерной программой, то при построении нормы об ответственности за общественно опасные деяния, связанные с использованием робокаров, предлагается использовать и конструкции диспозиций статей о преступлениях в сфере компьютерной информации (глава 28 УК РФ) [1]. Таким образом, предлагается создать отдельную норму УК, которая будет регулировать ответственность за ДТП с участием беспилотного средства [9].

В Российской Федерации ведется активная работа по совершенствованию законодательства в области регулирования передвижения беспилотных транспортных средств. Рассмотренные в работы предложения

являются необходимыми мерами, с принятием которых возможно устранение некоторых пробелов в праве.

Список источников и литературы:

1. Уголовный кодекс Российской Федерации от 13.06.1996 N 63-ФЗ (ред. от 02.10.2024) / [Электронный ресурс] // : [сайт]. − URL: https://www.consultant.ru/document/cons_doc_LAW_10699/b729b65a24b312d2cbee8543a8afdfb15ebb4046/ (дата обращения: 14.10.2024).

2. Постановление Правительства Российской Федерации от 08.08.2023 № 1296 «О внесении изменений в пункт 89 Программы экспериментального правового режима в сфере цифровых инноваций по эксплуатации высокоавтоматизированных транспортных средств в отношении реализации инициативы "Беспилотные логистические коридоры" на автомобильной дороге общего пользования федерального значения М-11 "Нева"» / [Электронный ресурс] // : [сайт]. − URL: http://publication.pravo.gov.ru/document/0001202308090025 (дата обращения: 16.10.2024).

3. Проект Федерального закона «О высокоавтоматизированных транспортных средствах и о внесении изменений в отдельные законодательные акты Российской Федерации» / [Электронный ресурс] // Информационно- правовой портал "Гарант.Ру" : [сайт]. − URL: https://base.garant.ru/56880577/ (дата обращения: 14.10.2024).

__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl117s1648.pdf%27%5D__1580953977 66 (дата обращения:14.10.2024)

4. New York City welcomes robotaxis − but only with safety drivers / [Электронный ресурс] // : [сайт]. − URL: https://www.theverge.com/2024/3/28/24108894/nyc-autonomous-robotaxi-safety-driver-permit-eric-adams (дата обращения: 16.10.2024).

5. Беспилотные автомобили (мировой рынок) [Электронный ресурс]: Мировые новости рынка 2024 − Режим доступа: https://www.tadviser.ru/index.php/ (дата обращения: 14.10.2024)

6. Дремлюга Р. И., Яковенко А. А Регулирование тестирования беспилотного автотранспорта: опыт Европы [Текст] / Р. И. Дремлюга, А. А. Яковенко // Право. − 2020. − С. 105-116

7. Минтранс определил, кто виноват при авариях с беспилотными автомобилями / [Электронный ресурс] // Кодекс : [сайт]. − URL: https://kodeks.ru/news/read/mintrans-opredelil-kto-vinovat-pri-avariyah-s bespilotnymi avtomobilyami?ysclid=m27m7fna1s419814875 (дата обращения: 14.10.2024).

8. Рязанов, Н. С. Актуальные вопросы уголовно-правового обеспечения безопасного использования беспилотного транспорта [Текст] / Н. С. Рязанов // Право. − 2020. − № . − С. 80-83

9. Сазонова М. Беспилотные автомобили: как планируется регулировать их эксплуатацию в России? / Сазонова М. [Электронный ресурс] // Информационно- правовой портал "Гарант.Ру" : [сайт]. − URL: https://www.garant.ru/article/1471258/ (дата обращения: 14.10.2024).

10. Смирнова Т.И. Беспилотные автомобили: сколько стоят, когда поступят в продажу и как ИИ справляется с бездорожьем и лихачами / Татьяна Смирнова [Электронный ресурс] // Мировой рынок : [сайт]. − URL: https://cloud.vk.com/blog/bespilotnye-avtomobili-skolko-stoat-kogda-postupat-v-prodazu (дата обращения: 14.10.2024).

Арина Алексеевна Штанова,
Студентка Международно-правового факультета,
МГИМО МИД России
E-mail: Shtanova0412@yandex.ru

Arina A. Shtanova,
Student, Faculty of International Law,
MGIMO University,
E-mail: Shtanova0412@yandex.ru

НЕЙРОБЕЗОПАСНОСТЬ КАК НОВОЕ НАПРАВЛЕНИЕ В МЕЖДУНАРОДНОМ ПРАВЕ

NEUROSECURITY AS A NEW DIRECTION OF INTERNATIONAL LAW

Аннотация. Данная статья определяет основные проблемы применения нейротехнологий, обосновывает выделение нейробезопасности в качестве нового направления международного права, а также выявляет необходимость правового регулирования данной сферы.

Ключевые слова: нейротехнологии, нейроправа, нейробезопасность, геномное право, искусственный интеллект, биоэтика.

Absrtact. This article defines the main issues related to the application of neurotechnologies, justifies the concept of neurosecurity as a new direction in international law, and highlights the need for legal regulation in this area.

Key words: neurotechnology, neuro law, neuro security, genomic law, artificial intelligence, bioethics.

Процесс юридификации общества, то есть расширения предмета правового регулирования, неизбежно приводит к возникновению новых поколений прав человека: соматические права, генетические права, нейроправа.

Современный уровень развития нейротехнологий предопределяет их использование исключительно в картировании и изменении активности мозга. Однако в будущем станет возможным использование технологий нейроинтерфейсов, позволяющих управлять внешними устройствами при помощи электрических сигналов мозга; вставных протезов, обеспечивающих доступ в Интернет; создание аватаров человека, способных управлять транспортными средствами; электростимулирование мозга для лечений заболеваний [2, с.208].

Безусловно, применение нейротехнологий не только ведет к перспективе лечения болезней Альцгеймера, Паркинсона, а также заболеваний центральной нервной системы человека, улучшению психических, когнитивных характеристик человеческого мозга, но и создает множество опасностей [1, с. 15]: нарушение нейроразнообразия, управление поведением человека, его мыслями и чувствами (воплощение идей трансгуманизма), нарушение нейронного суверенитета и нейронного достоинства человека, его конституционных прав, социальных норм (религиозных, моральных, этических, др.). В связи с чем необходима детальная правовая регламентация данной сферы.

Пока рано говорить о выделении правового регулирования нейронных исследований и практики обращения их результатов в качестве подотрасли международного биоправа, так как не разработан достаточный массив законодательства на национальном и международном уровне. Однако правовая доктрина предлагает следующие направления юридической регламентации в рамках предмета «зарождающейся» подотрасли [5, с.143]: 1) нейронная идентичность, защита нейронной информации, право не знать свой нейронный код, запрет применения нейронного оружия (нейроцида), противодействие нейрохакингу; 2) нейронная регистрация, нейронная паспортизация, национальные персонифицированные нейробанки; 3) правовой статус участников нейронных исследований, биоэтика, «кодекс нейронных исследований»; 4) услуги по обработке, хранению и внедрению

результатов нейронных исследований; патентование нейротехнологий; «нейронный рынок».

Особое внимание уделяется проблемам нейроэтики, вопросу об ответственности разработчиков технологий, воздействующих на нервную систему человека и способствующих изменениям в ее функционировании. В связи с чем в международном праве выделяется ряд важных актов, содержащих нормы-принципы и нормы-декларации мягкого права и устанавливающих ограничения применения нейротехнологий [4, с. 110]: Конвенция Совета Европы о правах человека и биомедицине (1997 г.); Конвенция о защите прав и достоинства человека в связи с применением достижений биологии и медицины (1997 г.); Всеобщая декларация ЮНЕСКО о биоэтике и правах человека (2005 г.); Рекомендации Международного комитета ЮНЕСКО по биоэтике в применении нейроправ (2022 г.).

Можно выделить тенденцию международных медико-биологических организаций и исследовательских структур стран к закреплению в своих актах запрета (временного или абсолютного) на применение нейротехнологий. Подобное положение содержит ст.6 Директивы Европейского Союза от 6 июля 1998 года №98/44 «О правовой охране биотехнологических изобретений: «Изобретения считаются непатентоспособными, если их коммерческое использование противоречит публичному порядку или морали». Однако законодатель не дал четкого определения понятий «публичный порядок» и «мораль», что безусловно вызвало немало вопросов в правоприменительной практике.

Так, в 2004 году международная организация «Гринпис» обратилась в Федеральный патентный суд Германии с ходатайством об аннулировании патента, выданного в 1999 году ученому Боннского университета Оливеру Брюстле. Патент был нацелен на получение изолированных и очищенных нейронных клеток из эмбриональных стволовых клеток и на их использование для лечения нейронных дефектов. После аннулирования патента ученый обратился в Федеральный Верховный суд Германии, который, в свою очередь,

обратился за разъяснениями ст.6 Директивы ЕС №98/44 в Суд Европейского Союза. Суд Европейского Союза постановил, что в данном случае использование биотехнологий противоречит публичному порядку, так как запрещается проводить любые модификации с эмбрионами человека (в коммерческих, промышленных и научных целях).

Что же касается национальных правовых систем, Республика Чили стала первым в мире государством, которое разработало законопроект о защите прав человека в условиях цифровизации, применения технологий генного и нейронного редактирования. В рамках проекта нормативно-правового акта выделены следующие аспекты защиты нейроправ: 1) защита данных человеческого разума и нейроданных; 2) ограничения на нейротехнологию чтения; 3) справедливый доступ к нейротехнологиям; 4) запрет применения нейроалгоритмов. В Российской Федерации на данный момент действует федеральная программа Министерства образования и науки «Мозг, здоровье, интеллект, инновации» на 2021-2029 год, призванная разработать новые полезные нейротехнологии, а также развить прежние разработки ученых [3, с.83].

Вполне обоснованно определение правового статуса искусственного интеллекта в рамках рассмотрения данной темы, так как ему уделяется главенствующая роль в процессе сбора и обработки нейроинформации, разработки новых технологий. Если рассматривать искусственный интеллект в качестве субъекта правоотношений, то он не подпадает под определения физического и юридического лица, в связи с чем в доктрине предлагается наделить искусственный интеллект особым статусом – «электронное лицо». С одной стороны, отсутствие воли не позволяет выделить искусственный интеллект в качестве самостоятельного субъекта. Однако и объектом правоотношений его признать невозможно в силу способности принимать решения и непредсказуемости действий.

Заключение. Подводя итог вышесказанному, представляется выделить нейробезопасность как новое, развивающееся направление международного

права, которое требует тщательной правовой регламентации аспектов ответственности разработчиков и операторов нейротехнологий, определения их статуса, соответствия поведения данных лиц нормам биоэтики, а также обоснованности причисления нейротехнологий к объектам патентных прав.

Список использованной литературы:

1. Burbon Diego, Burbon Luisa. A Critical Perspective on NeuroRights: Comments Regarding Ethics and Law. 2021.

2. Алферова Е.В. Нейроправо: достижения в области нейронауки и их применение в криминологии, криминалистике и правосудии. (Обзор) // Социальные и гуманитарные науки. Отечественная и зарубежная литература: ИАЖ. Сер. 4: Государство и право. — 2023. — № 2. — С. 206 — 216.

3. Бондаренко Александр Александрович. Формирование категории «нейроправа»: обобщение российского и международного опыта // Юридическая наука. 2023. №8. С. 82 — 85.

4. Будник Р. А. Становление нейроправа: опыт Китая и курс ООН // Журнал зарубежного законодательства и сравнительного правоведения. 2023. Т. 19. № 2. С. 108 — 119.

5. Трикоз Е.Н. Защита прав человека в контексте развития биоэтики и геномики (Обзор международного круглого стола) // Вестник Российского университета дружбы народов. Серия: Юридические науки. 2019. Т. 23. № 1. С. 141 — 154.

СЕКЦИЯ 4

«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ОБЩЕСТВО»

Сергей Сергеевич Дейкало,
магистрант кафедры журналистики,
Гродненский государственный университет им. Янки Купалы,
E-mail: mediacenter@grsu.by

Sergej S. Dejkalo,
Master's Degree Student, Department of Journalism,
Yanka Kupala State University of Grodno,
E-mail: mediacenter@grsu.by

ВОПРОС О МЕЖГОСУДАРСТВЕННЫХ МЕДИАХОЛДИНГАХ В КОНТЕКСТЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

QUESTION ABOUT INTERSTATE MEDIA HOLDINGS IN THE CONTEXT OF INFORMATION SECURITY

Аннотация. Рассматривается взаимосвязь тенденций концентрации СМИ и развития международных коммуникаций в информационном обществе. Дается краткий обзор сотрудничества Беларуси и России в сфере массовых медиакоммуникаций. В контексте задач информационной безопасности рассматриваются перспективы развития единого медиахолдинга Союзного государства Беларуси и России.

Ключевые слова: Беларусь, Россия, медиахолдинг, процессы концентрации СМИ, информационная безопасность.

Abstract. The author discusses the relationship between trends in media concentration and the development of international communications in the information society. The article provides a brief overview of cooperation between Belarus and Russia in the field of mass media communications. The prospects for the development of a single media holding of the Union State of Belarus and Russia are considered in the context of information security tasks.

Keywords: Belarus, Russia, media holding, mass media concentration processes, information security.

Тенденции концентрации СМИ и международные коммуникации. Международная коммуникация является важнейшим направлением информационной политики как отдельных государств, так и их интеграционных объединений. Одна из тенденций на рынке международных коммуникаций – «возрастающая концентрация медиа, находящихся в собственности крупных корпораций» [5], создание различных конвергентных структур (транснациональные медиакомпании, международные информационные агентства, международные медиахолдинги, международные издательские дома) с целью усиления политического и экономического влияния их учредителей [8]. Такие медиахолдинги «по сути, решают, что будет экспортировано медиакомпаниями на рынок идей» [6], и могут преследовать разные, в том числе деструктивные, цели, например, информационной борьбы «в отношении русского и русскоязычного населения на постсоветской территории, в Европе и всем мире» [8]. Еще в 1970-е гг. отмечалось, что западные транснациональные медиамонополии нанесли значительный ущерб всему миру, в том числе вели подрывную деятельность и вмешивались во внутренние дела других государств [8]. Один из инструментов общего противодействия Беларуси и России современным информационным угрозам (киберпреступность, информационный терроризм и экстремизм, операции информационной войны) – это укрепление сотрудничества в сфере медиа, создание и развитие межгосударственных медиакомпаний.

Сотрудничество Беларуси и России в сфере медиакоммуникаций. Успешное развитие межгосударственного информационного обмена, координация информационной повестки дня возможны благодаря общему русскоязычному пространству двух стран и общей системе ценностей белорусского и российского народов, а также неизменным принципам стратегического равноправного партнерства двух государств. Эффективно функционируют СМИ, которые посвящены вопросам союзного строительства и учредителями которых являются Парламентское собрание и Совет

Министров Союза Беларуси и России: газеты «Союзное Вече», «Союз. Беларусь – Россия», журнал «Союзное государство», «Телерадиовещательное объединение Союза», информационно-аналитический портал Союзного государства. С 1 января 2022 года начала работу российско-белорусская Ассоциация региональных медиа, в которую «входят медиахолдинги наиболее тесно связанных между собой регионов Беларуси и России (от Калининграда и Подмосковья до Бреста и Новополоцка)» [2]. Повестку дня Союзного государства продвигает Содружество журналистов и блогеров Беларуси и России «Друзья – Сябры». Регулярно проводятся российско-белорусские медиафорумы, рассчитанные на аудиторию разного уровня: например, в мае 2024 года в Пскове прошел II Российско-белорусский форум студенческих СМИ «Индустрия медиа». Положительно зарекомендовали себя учебные занятия и мастер-классы для начинающих российских и белорусских журналистов, которые проводились под патронатом Международного журналистского клуба «Мастерская BY-RU». В то же время сегодня некоторые медиаэксперты признаются, что Россия и Беларусь «пока проигрывают в информационном пространстве в интернете из-за отсутствия собственных инструментов распространения информации» [4].

Медиахолдинг Союзного государства России и Беларуси. На заседании Высшего государственного совета в январе 2024 года лидеры России и Беларуси приняли решение о создании совместного медиахолдинга. Планируется, что в начале 2025 года начнет работу автономная некоммерческая организация «Медиакомпания Союзного государства», которая будет зарегистрирована в России с представительством в Беларуси [7]. В условиях информационных угроз, общих для России и Беларуси, главным фактором создания союзного медиахолдинга является необходимость обеспечения информационной безопасности и защиты информационных интересов двух стран в мировом медиапространстве. В работе медиахолдинга четко определяются две цели: внутренняя – создание благоприятных условий для функционирования единого информационного пространства, внешняя –

повышение международного авторитета Союзного государства. Так, Председатель Комиссии Парламентского Собрания по информационной политике А.Наумович отмечает: «Наша интеграция во многом напрямую зависит от того, насколько граждане Беларуси и России осведомлены о достижениях и проблемах» [1]. Деятельность медиахолдинга призвана служить решению таких задач, как расширение аудитории союзных медиа в интернет-среде, повышение экономической эффективности союзных редакций, совместное освоение самых передовых информационных технологий. В рамках новых интеграционных союзов «необходимо создавать эффективный механизм противодействия информационным атакам, а также обеспечивать регулируемость информационных потоков» [3].

Заключение. У России и Беларуси существует общее видение основных информационных угроз и способов противодействия им. Межгосударственный медиахолдинг может стать важным субъектом международной медиакоммуникации, в том числе транслирующим позицию Союзного государства России и Беларуси во внешнюю среду и создающим имидж данного интеграционного объединения в мировой политической системе. Медиахолдинг позволит усилить влияние на мировое общественное мнение и увеличить медиаактивность двух стран в мировой информационной сфере.

Список источников и литературы:

1. Андрей Наумович: «Делаем ставку на передовые технологии и соцсети» // Союзное вече. – URL: https://www.souzveche.ru/articles/tribune_deputy/45281/ (дата обращения: 14.10.2024).

2. Белорусско-российская Ассоциация региональных медиа начала работу с 1 января 2022 года // Министерство информации Республики Беларусь. – URL: http://www.mininform.gov.by/news/all/belorussko-rossiyskaya-

assotsiatsiya-regionalnykh-media-nachala-rabotu-s-1-yanvarya-2022-goda/ (дата обращения: 10.10.2024).

3. Булва В. И. Проблемы информационной безопасности на евразийском пространстве: пути их преодоления в рамках ШОС // Международный журнал конституционного и государственного права. – 2019. – № 2. – С. 98–102.

4. В Минске считают, что Белоруссия и РФ проигрывают Западу инфополе в интернете // ТАСС. – URL: https://tass.ru/mezhdunarodnaya-panorama/21348875 (дата обращения: 12.10.2024).

5. Лебедева Е. Медиахолдинг как субъект международной коммуникации: тенденции и перспективы // Национальные медиахолдинги в контексте реализации государственной информационной политики: материалы науч.-практ. конф. – Минск: Изд. центр БГУ, 2014. – С. 88–92.

6. Орлова В. Глобальные телесети новостей на информационном рынке. – М.: РИП-холдинг, 2003. – 168 с.

7. Осипов М. Замминистра цифрового развития РФ: рассчитываем, что реформы позволят повысить эффективность союзных медиа // Беларусь сегодня. – URL: https://www.sb.by/articles/zamministra-tsifrovogo-razvitiya-rf-rasschityvaem-chto-reformy-pozvolyat-povysit-effektivnost-soyuzn.html (дата обращения: 10.10.2024).

8. Современный медиахолдинг: формы существования и проблемы институционализации: коллективная монография / отв. ред. Б. Я. Мисонжников. – М.: ФЛИНТА: Наука, 2017. – 496 с.

Евгений Владленович Зогранян,
Аспирант кафедры политологии и политического управления,
ИОН РАНХиГС при Президенте РФ,
E-mail: zogranyane@mail.ru

Eugene V. Zogranyan,
Postgraduate student, Department of
Political Science and Political Management,
RANEPA,
E-mail: zogranyane@mail.ru

ЛАТЕНТНЫЕ СЕТЕВЫЕ ОБЩНОСТИ ИЛИ КОЛОНИЗАЦИЯ БУДУЩЕГО

LATENT NETWORK COMMUNITIES OR COLONIZATION OF THE FUTURE

Аннотация. Данная статья посвящена новым вероятным угрозам и вызовам в области информационной безопасности, которые могут быть использованы в качестве инструмента политических технологий национального и международного уровней в силу своей универсальности. Актуальность исследования обусловлена активным внедрением ИКТ в политическую сферу, а также их использованием для ведения гибридных войн и воздействия на политическую и социальную сферы государств.

Ключевые слова: ИКТ, информационное пространство, сетевые общности, сетевые структуры, сбор персональной информации.

Abstract. This article is devoted to new potential threats and challenges in the field of information security, which can be used as a tool of political technologies at the national and international levels due to their universality. The relevance of the study is explained by the active introduction of ICT into the political sphere, as well as their use for conducting hybrid wars and influencing the political and social spheres of states.

Keywords: ICT, information space, network communities, network structures, collection of personal information.

Сегодня мы являемся свидетелями того, как область ИКТ становится пространством футуристических спекуляций, которые охотно распространяются СМИ и альтернативными медиа. При этом зачастую популярным становится то, что соответствует «большой пятерке» и «горячей десятке» [3], но не всегда является наиболее важным или существенным.

Частичное юридическое регулирование сбора персональных данных оставляет широкий ряд сценариев недобросовестного использования ИКТ, в частности, создание сетевых общностей, в том числе и политических, на основе моделей конкретных пользователей, созданных за счет заранее обработанной персональной информации широкого спектра, от данных акселерометра в смартфоне, до классической активности на различных цифровых платформах [4].

Стоит отметить, что искусственное создание сетевых структур в информационном пространстве – это совсем не новое явление, я бы даже сказал, вполне обыденное. Однако развитие ИКТ помогая решать одни вопросы, порождает ряд новых вызовов и угроз [1].

Информационное пространство на сегодняшний день является практически прозрачным, а любое объединение пользователей для подготовки противоправных действий имеет определенный алгоритм функционирования, что на определенных этапах делает возможным предотвращение противоправных действий. При этом каждый этап осуществления требует определенного времени, в течении которого происходит коммуникация звеньев сетевой структуры, что при относительно высокой скорости обмена информацией по сравнению с иерархическими структурами все же является слабым местом.

Можно предположить, что на сегодняшний день или в ближайшем будущем становится возможным сделать процесс искусственного создания

сетевых общностей менее отслеживаемым, при этом повысив скорость функционирования такого рода сетевых структур. Например, становится возможным организовать процесс коммуникации специально подготовленной языковой модели с заранее определенными отдельными звеньями потенциальной сетевой общности без перекрестных ссылок, без непосредственной коммуникации между потенциальными звеньями будущей сетевой общности. Сетевая структура создается внутри моделируемого пространства вероятностей, а так как это пространство не выходит за пределы виртуальной модели, то для внешнего наблюдателя задача по выявлению угрозы усложняется. При этом мы выходим за рамки классического понимания временной структуры цикла функционирования сетевых общностей [5]. Сам цикл сокращается за счет исключения ряда стадий подготовки, что позволяет перейти к реализации поставленных задач практически сразу, точнее практически без предварительной коммуникации звеньев между собой.

Таким образом, мы видим существование вероятности попыток скорее не предсказания будущего поведения звеньев, а попытки захвата и колонизации будущего. Лучшая спящая ячейка это та, которую невозможно раскрыть. Невозможно обнаружить то, чего не существует. И, говоря о реализации определенной вероятности, важно отметить, что для противодействующей стороны становится сложно противопоставить что-то конкретное заранее именно с точки зрения тактических действий, а совершение хода уже подразумевает запаздывание в ответной реакции. Как показали белорусские события 2020 года [2], скорость реакции иерархических структур и институтов практически всегда ниже скорости реакции сетевых структур. Данная особенность делает разрыв в скорости реакции еще более значимым так как реакция осуществляется уже на стадии реализации действия, а не на стадии планирования и подготовки.

Заключение. В связи с этим хотелось бы обратить внимание на проблемы, связанные с отсутствием четкого регулирования сбора

персональных данных широкого спектра. В освещенном выше вопросе ключевое значение имеет именно сбор персональных данных пользователей, который ради безопасности и стабильности всего мирового сообщества должен быть прозрачным и отслеживаемым процессом. При отсутствии контроля в данной области как на региональном, так и на глобальном уровне, мы рискуем столкнуться не только с новыми угрозами и вызовами для существующего порядка вещей, но и угрозой колонизации нашего общего будущего.

Список источников и литературы:

1. Бек У. Общество риска. На пути к другому модерну. М.:Прогресс-Традиция. 2000. − 384 с.

2. Белоконев С. Ю., Волохов А. Е. Протестные выступления 2020 г. в Беларуси и возможная институциональная трансформация политической системы. Власть. 2022. 30 (2). С. 45-51.

3. Иванов Д. В. Глэм-капитализм: общество потребления в XXI в // ЖССА. 2011. №5. URL: https://cyberleninka.ru/article/n/glem-kapitalizm-obschestvo-potrebleniya-v-xxi-v (дата обращения: 16.10.2024).

4. Масалович А. Ваши данные утекли. Теневой рынок информации. URL: https://youtu.be/WIVtpFKMi-w?si=RqRbj0owIGS-KggT (дата обращения: 16.10.2024).

5. Galor O. A Two-Sector Overlapping-Generations Model: A Global Characterization of the Dynamical System // Econometrica. 60 (6). 1992. P. 1351-1386.

Федор Васильевич Ниточкин,
аспирант МГЮА им. О.Е.Кутафина, ответственный секретарь
Координационного совета по общественному контролю за голосованием при
Общественной палате Российской Федерации;
E-mail: nitochkin@oprf.ru

Fedor V. Nitochkin,
Postgraduate student, Kutafin Moscow State Law University,
Executive office of the Civic Chamber of the Russian Federation,
Executive secretary of the Coordinating council for public control over voting,
E-mail: nitochkin@oprf.ru

«ФЕЙКИ» О ВЫБОРАХ КАК УГРОЗА НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ

"FAKE NEWS" ABOUT ELECTIONS AS A THREAT TO NATIONAL SECURITY

Аннотация. В статье делается попытка раскрыть источники и проанализировать причины распространения «фейков» о выборах. Определяется их значение для подрыва легитимности избирательного процесса и публичной власти. Даются предложения по противодействию данной угрозе национальной безопасности.

Ключевые слова: выборы, избирательный процесс, избирательная система, мониторинговая миссия, «цветная революция», «фейковые новости», «фейки».

Abstract. This article attempts to uncover the sources and to analyze the reasons for the spread of "fakes" about elections. Their importance for undermining the legitimacy of the electoral process and public authority is determined. Proposals are being made to counter this threat to national security.

Keywords: elections, electoral process, electoral system, monitoring mission, "color revolution", "fake news", "fakes".

Тенденции политизации мониторинга избирательных процессов в мире. 2024 год стал знаковым для института выборов по всему миру. Баллотирование проходит в 64 странах на всех континентах, в том числе в Европе (19 стран), Африке (18 государств), Азии (16), Америке (7) и Океании (4). Президентские кампании состоялись в крупнейших демократиях мира, среди которых Россия, Индонезия, Мексика и США. Кроме того, в 2024 году были проведены выборы в Европейский парламент. По экспертным оценкам, в голосовании приняли участие более 2 млрд. избирателей в странах, совокупное население которых превышает 4 млрд. человек, что составляет половину населения Земли [6]. Журнал «Time» назвал 2024 год «решающим для демократии» («make-or-break year for democracy») «поскольку само количество выборов − и то, что они отражают или не отражают волю различных народов, − может существенно повлиять на будущее мира» [10].

Вывод журналистов «Time» интересен тем, что он ставит под сомнение способность народов самостоятельно, без посторонней помощи с учетом своих национальных особенностей сформировать оптимальную модель избирательной системы, позволяющую однозначно установить волю населения. Будто бы недостаточно зафиксировать отсутствие на выборах нарушений, способных повлиять на достоверность волеизъявления граждан, чтобы признать их демократичными. Для этого якобы требуется соответствующее «удостоверение», полученное от мониторинговых миссий, направленных странами «свободного мира». И это с учётом того, что даваемая ими оценка зачастую грешит субъективностью и предвзятостью. В этой связи вспоминается определение, которое дал выборам в Государственную Думу Федерального Собрания Российской Федерации 7 декабря 2003 года представитель делегации ОБСЕ Брюс Джордж: «свободные, но несправедливые» [7].

Мировое сообщество никогда не наделяло отдельные государства или межгосударственные объединения правом служить «мерилом» демократии. В резолюции Генассамблеи ООН от 19 декабря 2023 года, посвящённой

«усилению роли Организации Объединенных Наций в содействии переходу к демократии и проведению периодических и подлинных выборов», об этом говорится со всей определенностью: «хотя у демократии есть общие черты, единой модели демократии не существует и демократия не является собственностью какой-либо одной страны или какого-либо одного региона» [1]. Также не существует идеальной, подходящей для всех стран демократической избирательной системы. Совершенно справедливо отмечает И.Б. Борисов: «Гамма современных избирательных систем настолько разнообразна и многогранна, что дать объективную и справедливую оценку конкретной модели избирательной системы может только один беспристрастный арбитр – национальный избиратель» [5].

Несмотря на то, что страны Запада давно утратили монополию на оценку легитимности избирательных процессов, они по-прежнему настаивают на своём праве «измерять прогресс демократии» в суверенных государствах. Отчеты мониторинговых миссий БДИПЧ ОБСЕ и ПАСЕ при этом зачастую основываются на мнениях оппозиционных партий и кандидатов, докладах НКО, выполняющих функции иностранных агентов, а также на иной недостоверной, ангажированной, превратно интерпретированной и просто ложной информации («фейках»).

В случае же если выборы признаются ими недемократичными, не соответствующими международным электоральным стандартам, это может стать основанием для непризнания легитимности власти и инспирирования попыток её свержения в результате разного рода «цветных революций». Примерами развития событий по такому сценарию могут служить: «бульдозерная революция» после досрочных выборов президента Югославии в 2000 году, «революция роз» по итогам парламентских выборов в Грузии в 2003 году, «оранжевая революция» и третий тур президентских выборов на Украине в 2004 году, «тюльпановая революция» после парламентских выборов в Киргизии в 2005 году. В основе всех этих государственных

переворотов лежит подрыв легитимности избирательного процесса через распространение «фейков» о выборах.

«*Фейки» как угроза национальной безопасности.* О масштабах распространения «фейков» о выборах в сети Интернет свидетельствует упоминание этой проблемы в «Дорожной карте» Генерального секретаря ООН по цифровому сотрудничеству. Там указывается, что «Кибератаки и кампании по дезинформации, направленные против инфраструктуры, необходимой для проведения выборов, политических партий и политиков, подрывают возможности участия в политической жизни, а также легитимность важнейших институтов и сеют недовольство и недоверие» [3]. В России под «фейковыми новостями» (или просто «фейками») понимается недостоверная общественно значимая информация, распространяемая под видом достоверных сообщений и создающая угрозу для безопасности [4]. В действующей редакции Стратегии национальной безопасности Российской Федерации угроза внешнего вмешательства путём распространения ложной информации для инспирирования «цветных революций» оценивается со всей серьёзностью [2].

В последнее время «фейки» о выборах всё чаще становятся частью информационной кампании против российской избирательной системы, их количество остается значительным, а общественная опасность возрастает. Так, общественная организация «Лига безопасного интернета» зафиксировала 8,5 тысячи «фейков» в ходе Общероссийского голосования по вопросу одобрения изменений в Конституцию Российской Федерации в 2020 году» [8]. С 2022 года к «фейкам» о выборах добавились провокационные сообщения о специальной военной операции. Широкое распространение получили вбросы о голосовании «под дулом автоматов» на новых территориях, проведении мобилизационных мероприятий на избирательных участках, взыскании долгов с людей, пришедших на голосование, минировании помещений избирательных комиссий. Одним из направлений стало также распространение непроверенной и заведомо ложной информации для

дискредитации дистанционного электронного голосования (ДЭГ). К «фейкам» можно отнести некорректную интерпретацию статистических данных, использование и распространение сомнительных электоральных теорий, якобы подтверждающих массовость фальсификаций.

Цель «фейковых новостей» − дестабилизация общественной и политической обстановки и делигитимация выборной системы в стране. Можно согласиться с экспертами АНО «Диалог Регионы», которые выделяют следующие основные задачи «фейков» во время выборов: снижение явки; очернение оппонентов; подрыв доверия к выборам; убеждение граждан в отсутствии конкуренции; дискредитация новых форм голосования; увеличение социальной напряженности; подрыв легитимности институтов власти; дискредитация государства на международной арене [9].

Ответственность за распространение «фейков». Сегодня «фейки» − это часто встречающийся и общественно опасный вид нарушений на выборах. Административная ответственность за распространение «фейков» о выборах может наступить на основании статьи 13.15 КоАП, а уголовная − статьи 207.1 УК РФ. Однако сложившуюся практику правоприменения, в соответствии с которой наказание несут преимущественно распространители, а не создатели «фейков», нельзя назвать эффективной. Большинство самых опасных сообщений о выборах распространяется через зарубежные IT-платформы и социальные сети, находящиеся вне российской юрисдикции. В этой ситуации распространители «фейков» из числа простых граждан сами являются их жертвами и нуждаются скорее в правовом просвещении и привитии правил «цифровой гигиены».

Представляется, что ключевыми направлениями обеспечения национальной безопасности и защиты электорального суверенитета в настоящее время являются распространение норм национального законодательства на иностранные ИТ-платформы, ужесточение ответственности за производство ими ложной информации, регулирование

статуса блогеров-миллионников, а также повышение правовой и цифровой культуры избирателей.

Список источников и литературы:

1. Резолюция, принятая Генеральной Ассамблеей ООН 19 декабря 2023 года (A/78/481/Add.2, пункт 139). URL: https://documents.un.org/doc/undoc/gen/n23/422/88/pdf/n2342288.pdf (дата обращения: 10.11.2024).

2. Указ Президента Российской Федерации от 02.07.2021 г. № 400 «О Стратегии национальной безопасности Российской Федерации». URL: https://www.consultant.ru/document/cons_doc_LAW_389271/ (дата обращения: 10.11.2024).

3. Дорожная карта по цифровому сотрудничеству: осуществление рекомендаций Группы высокого уровня по цифровому сотрудничеству. Принята Генеральной Ассамблеей ООН 29 мая 2020 года (A/74/821, пункт 62). URL: https://documents.un.org/doc/undoc/gen/n20/102/53/pdf/n2010253.pdf. (дата обращения: 10.11.2024).

4. Статья 15.3 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

5. Игорь Борисов. Электоральный суверенитет. – М.: РОИИП, 2010. С. 2.

6. Какие президентские и парламентские выборы запланированы в мире в 2024 году. ТАСС. 30.12.2023. URL: https://tass.ru/info/19655535 (дата обращения: 10.11.2024).

7. «Выборы были свободными, но несправедливыми». Газета.ру. 08.12.2003. URL: https://www.gazeta.ru/2003/12/08/vyborybylisv.shtml (дата обращения: 10.11.2024).

8. Лига безопасного интернета выявила около 8,5 тысячи фейков о голосовании. РГ. 01.07.2020. URL: https://rg.ru/2020/07/01/liga-bezopasnogo-

interneta-vyiavila-okolo-85-tysiachi-fejkov-o-golosovanii.html (дата обращения: 10.11.2024).

9. Названы самые ожидаемые фейки на нынешних выборах. Лента.ру. 08.09.2023. URL: https://lenta.ru/news/2023/09/08/feiks/?ysclid=m1g6j743i0972597372 (дата обращения: 10.11.2024).

10. Country-by-Country Results So Far in the World's Biggest-Ever Election Year. TIME. 01.07.2024. URL: https://time.com/6991526/world-elections-results-2024/ (Accessed: 10.11.2024).

СЕКЦИЯ 5

«ФАКТОР ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В МЕЖДУНАРОДНЫХ ОТНОШЕНИЯХ И МИРОВОЙ ЭКОНОМИКЕ: МЕЖДУ МИФОМ И РЕАЛЬНОСТЬЮ»

Артем Андреевич Аствацатуров,
студент 4-го курса бакалавриата,
Институт истории и международных отношений,
Южный федеральный университет,
E-mail: astva@sfedu.ru

Artem A. Astvatsaturov,
4th year Student (bachelor),
Institute of History and International Relations,
Southern Federal University (SFedU),
E-mail: astva@sfedu.ru

КАК ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ ИЗМЕНИЛ СТРАТЕГИЧЕСКИЕ НАСТУПАТЕЛЬНЫЕ ВООРУЖЕНИЯ В США (НА ПРИМЕРЕ РАЗВИТИЯ ИНТЕГРИРОВАННОЙ СИСТЕМЫ СДЕРЖИВАНИЯ)

HOW ARTIFICIAL INTELLIGENCE CHANGED STRATEGIC OFFENSIVE ARMS IN THE U.S. (ON THE EXAMPLE OF INTEGRATED DETERRENCE SYSTEM DEVELOPMENT)

Аннотация. В настоящем исследовании представлен обзор и анализ развитию стратегических ядерных сил в контексте интегрированного сдерживания в рамках внедрения ИИ в качестве новой угрозы для международной безопасности. В рамках исследования были определены два наиболее релевантных сценария развития системы интегрированного сдерживания США в контексте интеграции ИИ в решение задач военно-стратегического планирования. В конце исследования были выработаны рекомендации с целью укрепления национальной безопасности Российской Федерации.

Ключевые слова: ИИ, гиперзвуковые вооружения, США, стратегические наступательные вооружения, противоспутниковое оружие, революция в военном деле, СЯС.

Abstract. In present research was presented review and analysis of strategic nuclear forces development in context of integrate deterrence in framework of its defining as newest international security threat. In framework of study were defined

two the most relevant scenarios of integrate system deterrence development in context of AI integration for military strategic planning policymaking. In the end of research were added recommendations with a purpose of strengthening national security of the Russian Federation.

Keywords: AI, hypersonic weapons, the U.S., strategic offensive arms, anti-satellite weapons, revolution in military affairs. SNF.

После завершения Революции в военном деле (РВД) в Соединенных Штатах и становления однополярной системы международных отношений изменился характер военно-технологического развития Стратегических ядерных сил (СЯС) США. Начиная с периода президентства Джорджа Уокера Буша (2001-2009 гг.) изменился характер предъявляемых требований к СЯС США в связи с окончательной реконцептуализацией архитектуры глобальной безопасности. Особенностью модернизации СЯС США в период развития американского внешнеполитического курса в XXI веке является постепенный последовательный процесс интеграции систем ПРО со стратегическими наступательными вооружениями (СНВ) нового типа (гиперзвуковые вооружения как один из ярких примеров таких вооружений) [5]. Уже к началу президентства Барака Обамы и вплоть до периода президента Джозефа Байдена возникает ситуация, когда искусственный интеллект (ИИ) начинает использоваться в военно-политическом секторе США в контексте совершенствования лазерных систем воздушного базирования для поражения целей непосредственно с параллельным развитием гиперзвуковых вооружений [3]. ИИ используется в качестве связи между элементами управления и координации мониторинга и системы координации механизмов по воздействию на ПРО, противоспутникового вооружения (ПСО) и непосредственно гиперзвуковых боевых блоков в целях мониторинга, сбора информации и одновременной передачи информации по всем линиям организации системы NC3 (Nuclear Command, Control and Coordination) в СЯС США [4].

Проблемы развития ИИ с целью дальнейшего подрыва международной безопасности. На современном этапе развития технологий и присутствия такой тенденции как «спин-офф» (т. е. трансфер разработок из гражданской сферы в военную) наблюдается развитие следующей отрицательной тенденции как феномен неуправляемых технологий [1]. Все это лишь усугубляет и без того хрупкую систему глобальной безопасности. Полагаем, что в условиях преобладания глобальной неопределенности и тенденции на хаотизацию международных отношений на современном этапе нельзя говорить о возможности воссоздания международно-правовой системы, состоящих из норм «жесткого права» (т.е. императивных норм) в целях разрешения образовавшейся проблемы международной безопасности и ее последующего разрешения. Для понимания характера поведения основных акторов международных отношений, в том числе в рамках определения новой линии стратегического соперничества США и России, необходимо понимать будущих характер развития новых СНВ и системы интегрированного сдерживания. В рамках данного исследования с помощью сценарного подхода были определены два наиболее вероятных сценария развития ИИ в контексте модернизации национальных СЯС в США с помощью прогностического метода в международных отношениях на основе изучения основных линий и стратегий поведения военно-политического руководства США, описанных в аналитических докладах Корпорации РЭНД [2], а также исходя из выдержки основных концептов Стратегии национальной безопасности США 2022 года [6].

Таблица 1. Сценарии развития системы интегрированного сдерживания США с использованием ИИ

Сценарий	**Описание развития сценария**	**Индикаторы**
Развитие ИИ для защиты	Развитие систем автоматов типа «en-	• Развитие системы автоматов «en-

от кибератак КВО	rapport» с дальнейшей блокировкой любых внешних сигналов и попыток повлиять на изменение работу КВО (в том числе АЭС, ядерных объектов), в связи с чем любая попытка внедрения в систему блокируется автоматом. Возможность трансфера развития системы «en-rapport» и в обратном направлении – для совершения массовых кибератак, однако первичные оборонительные цели являются средством «маскировки»	rapport» в США посредством тренда на увеличение финансирования программы • Развитие концептов в рамках системы национальной безопасности США на становление системы противодействие кибератакам • Увеличение упоминаний в СМИ о массовых DDoS атак на ядерные объекты с обвинением США
Система «Гиперзвуковые вооружения – ПСО»	Развитие системы гиперзвуковых летательных аппаратов для мониторинга приближающих объектов / средств связи и коммуникации для последовательной мгновенной передачи с помощью ИИ, после чего противоспутниковое оружие за счет своих военно-технологических особенностей поражает	• Увеличение финансирования на новые финансовые годы и в рамках принятия бюджета программы гиперзвуковых вооружений • Использование в рамках дискурса представителей МО США информации о необходимости интеграции гиперзвуковых

	одновременно и объекты врага в воздушном пространстве, и его спутниковые системы	вооружений в новую систему NC3

Источник: создано на базе исследования автора

Заключение. В настоящее время мы можем говорить о том, что гиперзвуковые вооружения в последующем могут быть связаны с помощью системы координат передачи данных с системой ПСО и непосредственно включены в новую систему требований для СЯС США. Для Российской Федерации особо важно в ближайшее десятилетие развивать и внедрять ИИ в систему обеспечения национальной безопасности. Считаем, что модернизация Национального центра управления обороной (НЦУО) с целью внедрения процессов автоматизации и элементов ИИ сможет также повлиять на развитии процесса сбора, обработки и системы линий координаций информации и развития элементов противодействия американской системы интегрированного сдерживания, что является необходимостью для ВС РФ с целью развития паритета в области новаторского подхода управления обороной и национальными СЯС совместно с продолжением курса на интенсификацию наращивания собственных гиперзвуковых вооружений.

Список источников и литературы:

1. Кокошин А.А. Вопросы прикладной теории войны. М.: Изд. дом Высшей школы экономики, 2019. – 227 с.

2. Lane, Matthew, Bryan, Frederick. Forecasting Demand for U.S. Ground Forces. Assessing Future Trends in Armed Conflict and U.S. Military Interventions. California, Santa-Monica: RAND Corporation Publ., 2022. – 263 с.

3. 2022 Nuclear Posture Review. [Электронный ресурс] URL: https://fas.org/wp-content/uploads/2023/07/2022-Nuclear-Posture Review.pdf. (дата обращения: 23.09.2024).

4. Deputy Secretary of Defense Dr. Kathleen Hicks Discusses Advances in AI and Data in the DOD. The U.S. Department of Defense. [Электронный ресурс] URL: https://www.defense.gov/Multimedia/Videos/videoid/846412/. (дата обращения: 23.09.2024).

5. Hypersonics and Missile Defense: Issues for Congress. The U.S. Congressional Research Service. [Электронный ресурс] URL: https://crsreports.congress.gov/product/pdf/IF/IF11623. (дата обращения: 23.09.2024).

6. The U.S. National Security Strategy. October 2022. [Электронный ресурс] URL: https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf/. (дата обращения: 23.09.2024).

Анастасия Андреевна Васильева,
Магистрант Юридического факультета имени М. М. Сперанского,
Российской академии народного хозяйства
и государственной службы при Президенте РФ
E-mail: nast.vasiljva2010@yandex.ru

Anastasia A. Vasilyeva,
Undergraduate student M. M. Speransky Faculty of Law,
Russian Presidential Academy of National
Economy and Public Administration,
E-mail: nast.vasiljva2010@yandex.ru

МЕЖДУНАРОДНО-ПРАВОВЫЕ АСПЕКТЫ РАЗВИТИЯ И ПРИМЕНЕНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

INTERNATIONAL LEGAL ASPECTS OF THE DEVELOPMENT AND APPLICATION OF ARTIFICIAL INTELLIGENCE

Аннотация. Стремительное развитие искусственного интеллекта и сопутствующих технологий порождает множество правовых и этических вопросов, требующих незамедлительного внимания. В условиях недостаточного регулирования ИИ может угрожать правам человека и безопасности данных, что подчеркивает необходимость международной координации для создания единых стандартов его использования.

Ключевые слова: искусственный интеллект, информационная безопасность, этические принципы, блокчейн, белая книга.

Abstract. The rapid development of artificial intelligence and related technologies raises many legal and ethical issues that require immediate attention. In conditions of insufficient regulation and may threaten human rights and data security, which underlines the need for international coordination to create uniform standards for its use.

Keywords: artificial intelligence, information security, ethical principles, blockchain, white paper.

Стремительное развитие в области искусственного интеллекта (ИИ) и появление революционных технологий, в значительной степени основанных на ИИ, включая робототехнику, Интернет вещей (IoT) и блокчейн, создают ряд сложных юридических вопросов. При отсутствии надлежащего правового регулирования существует риск, что это развитие может поставить под угрозу широкий спектр прав и свобод отдельных лиц, а также подорвать важнейшие цели международно-правового регулирования: обеспечение безопасности и благополучия людей, поддержание мира и безопасности, развитие дружественных отношений между нациями и укрепление сотрудничества во всём международном сообществе.

Ярким примером уже существующих рисков служит система КОМПАС (COMPAS), используемая в Соединённых Штатах Америки. Расшифровывается данная система как профилирование управления правонарушителями для альтернативных санкций. Она используется для выявления риска рецидива при принятии решений о предварительном заключении в уголовных делах. КОМПАС заведомо завышает риск рецидива для афроамериканских национальностей. Данный пример говорит о том, права некоторых категорий граждан могут нарушаться из-за применения технологий искусственного интеллекта [1].

Этические вопросы, поднимаемые учеными, были освещены Комиссией по эффективности правосудия Совета Европы. Рабочей группой данной Комиссии были разработаны этические принципы использования ИИ в отправлении правосудия. Там содержится около 5 принципов, подтверждающих некоторые проблемы в данной сфере. Например, один из принципов – это безопасность данных: при обработке судебных решений и данных следует использовать сертифицированные источники и данные, которые не могут быть изменены. Решением подобной проблемы может стать применение технологий блокчейна, поскольку они обеспечивают неизменность информации (так как данная технология разрешает вопрос о том, что данные могут изменить) [2].

Этика использования ИИ является одной из главных тем международных дискуссий. ИИ, будучи инструментом, который активно применяется для анализа данных и автоматизации решений, может нарушать права человека, если его использование не будет соответствовать международным стандартам. Особую обеспокоенность вызывает защита личных данных. Международные правовые нормы, такие как Общий регламент по защите данных (GDPR) в Европейском Союзе, уже направлены на защиту персональных данных. Недавно в Европейском Союзе был введен новый закон о защите персональных данных (GDPR) [3]. То, что часто называют Общим регламентом о защите данных ЕС, на самом деле является серией директив ЕС: Регламент (EU) 2016/679 [4], Директива (EU) 2016/680 [5]. Однако на данный момент страны по-разному подходят к вопросу защиты данных. Например, в Европе действует строгий GDPR, в то время как в США и Китае применяются другие подходы. Создание единых международных правил обмена данными, которые бы учитывали интересы как технологических компаний, так и граждан, стало бы важным шагом в международном регулировании ИИ.

Технологии ИИ могут использоваться в различных сферах. Одна из таких сфер – это кибербезопасность. С помощью искусственного интеллекта куда проще взломать системы безопасности, найти обходные пути для своих целей и задач. Например, последнее время очень активно распространяется система deepfakes. Она заключается в том, что модель искусственного интеллекта обучается на большом количестве информации, касаемой конкретного человека: фото, видео, аудио. А затем воспроизводится для целей и задач мошенников. Был такой случай, связанный с использованием голоса актрисы совсем в других сферах: Алена Андропова согласилась использовать её голос для внутреннего использования в «Т-банке», но ее данные утекли и были использованы мошенниками для озвучки [6].

Каждая страна по-своему пытается урегулировать данный вопрос. В нескольких государствах есть так называемая белая книга. Возможно и

региональное взаимодействие. Например, существует Белая книга по искусственному интеллекту, подготовленная Европейской комиссией в 2020 году [7]. Данный документ выражает обеспокоенность и предлагает риск-ориентированный подход к регулированию ИИ, а также превосходство человека над системой искусственного интеллекта. Также есть Белая книга по искусственному интеллекту, подготовленная Китайской академией информационных и коммуникационных технологий в 2022 году [8]. Она является неким обзорным документом, в котором можно обратить внимание на риски, связанные с ИИ, а также опыт других стран и перспективы развития.

Заключение. Стремительное развитие искусственного интеллекта и тесно связанных с ним технологий неизбежно порождает сложные юридические, этические и технические вопросы, влияющие на права и свободы людей. На примере системы КОМПАС в США видно, что автоматизированные решения могут приводить к дискриминации отдельных групп населения. В то же время ключевые международные документы и инициативы, такие как этические принципы Комиссии по эффективности правосудия Совета Европы, Общий регламент по защите данных (GDPR) в Европейском союзе и различные «Белые книги» по ИИ, подтверждают необходимость выработки единых подходов к регулированию, ориентированных на соблюдение прав человека и обеспечение прозрачности. Задействование блокчейна для сохранения неизменности данных, внедрение механизмов контроля за deepfake-технологиями и разработка риск-ориентированных стратегий использования ИИ могут стать основой для ответственного и безопасного применения искусственного интеллекта во всех сферах общественной жизни. В конечном счёте, только международное сотрудничество и совместное развитие стандартов позволят реализовать огромный потенциал ИИ, не нарушая при этом фундаментальные права и принципы справедливости.

Список источников и литературы:

1. Tim Brennan, William Dieterich and Beate Ehret Correctional Offender Management Profiles for Alternative Sanctions (COMPAS) // Criminal Justice and Behavior. - 2017. - С. 20-40. (дата обращения: 02.09.2024).

2. CEPEJ European Ethical Charter on the use of artificial intelligence (AI) in judicial systems and their environment // European Commission for the Efficiency of Justice (CEPEJ) URL: https://www.coe.int/en/web/cepej/cepej-european-ethical-charter-on-the-use-of-artificial-intelligence-ai-in-judicial-systems-and-their-environment (дата обращения: 29.09.2024).

3. GDPR (General Data Protection Regulation) // GDPR URL: https://ogdpr.eu/ru?ysclid=m2darzn6ik993728809 (дата обращения: 01.10.2024).

4. Регламент (ЕС) 2016/679 // GDPR URL: https://ogdpr.eu/ru/gdpr-2016-679 (дата обращения: 02.10.2024).

5. Директива 2016/680 // GDPR URL: https://ogdpr.eu/ru/gdpr-2016-680 (дата обращения: 02.10.2024).

6. Актриса озвучки подала в суд на «Тинькофф» из-за использования её голоса для синтеза аудиорекламы // vc.ru URL: https://vc.ru/legal/817601-aktrisa-ozvuchki-podala-v-sud-na-tinkoff-iz-za-ispolzovaniya-ee-golosa-dlya-sinteza-audioreklamy-porno?ysclid=m2efbtagmt651123895 (дата обращения: 27.09.2024).

7. WHITE PAPER On Artificial Intelligence - A European approach to excellence and trust // URL: https://commission.europa.eu/system/files/2020-02/commission-white-paper-artificial-intelligence-feb2020_en.pdf (дата обращения: 16.09.2024).

8. Белая книга по искусственному интеллекту (2022) // URL: https://ai.gov.ru/knowledgebase/dokumenty-po-razvitiyu-ii-v-drugikh-stranakh/2022_belaya_kniga_po_iskusstvennomu_intellektu_artificial_intelligence_white_paper_caict/ (дата обращения: 16.09.2024).

Екатерина Алексеевна Виноградова,
к.п.н., директор, Научно-исследовательский центр
Технологии искусственного интеллекта
в международных отношениях (НИЦТИИМО)
E-mail: vinogradovacatherine7@gmail.com

Ekaterina A. Vinogradova,
Ph.D. in Political Science,
Director, Research Center
for Artificial Intelligence Technologies
in International Relations (RC-AITIR),
E-mail: vinogradovacatherine7@gmail.com

НЕСАНКЦИОНИРОВАННОЕ ИСПОЛЬЗОВАНИЕ ПОЛИТИЧЕСКИХ ДИПФЕЙКОВ В МЕЖДУНАРОДНОЙ ПРАКТИКЕ

UNAUTHORIZED USE OF POLITICAL DEEPFAKES IN INTERNATIONAL PRACTICE

Аннотация. В работе дается характеристика несанкционированного использования на политических дипфейков на выборах 2023-2024 гг. Политический дипфейк автор данного исследования определяет как специальную кампанию с применением технологии искусственного интеллекта для подрыва репутации политических лидеров с целью изменения хода избирательной борьбы или для дискредитации уже действующего политика.

Ключевые слова: политический дипфейк, международные отношения, дезинформация, когнитивная безопасность, политический лидер, политические выборы.

Abstract. This work provides a characterization of unauthorized usage in the political elections of 2023-2024. The author defines political deepfake as a specialized campaign utilizing artificial intelligence technology aimed at undermining the reputation of political leaders, with the objective of altering the course of electoral competition or discrediting an incumbent politician.

Keywords: political deepfake, international relations, disinformation, cognitive security, political leader, political elections.

Дипфейки в политической практике. Политический дипфейк, как инструмент пропаганды, активно применяется в дезинформационных кампаниях и информационно-психологических операциях по всему миру, представляя угрозу национальной безопасности.

Согласно отчету Европола за 2022 год, значительный прогресс в доступности технологий дипфейк был достигнут благодаря внедрению генеративно-состязательных сетей, описанных Яном Гудфеллоу из компании Google в 2014 году [1]. В конце 2018 года общественное внимание привлекли потенциальные политические риски, связанные с использованием технологии дипфейк. Поводом послужил видеоролик Дональда Трампа, в котором он призывал Бельгию покинуть Парижское климатическое соглашение. Видеоролик распространила Фламандская социал-демократическая политическая партия в Бельгии (Vooruit) с целью привлечения внимания к манипулированию общественным мнением по вопросам, связанным с изменением климата.

Первым официально признанным злонамеренным политическим дипфейком стал инцидент с главой МИД и заместителем премьер-министра Бельгии Софи Вильмес в 2020 году [2]. В данном видеоролике политик произносила вымышленную речь о связи между COVID-19 и изменением климата.

Статистический анализ. Социологические исследования последних лет показывают, что использование политических дипфейков во время проведения выборов вызывают у целевых аудиторий обеспокоенность и недоверие к официальным СМИ. В частности, в 2023 году кампания Luminate провела исследование, которое показало, что более 70% граждан Великобритании выражали беспокойство относительно воздействия дипфейков на предстоящие выборы в стране [3].

Несанкционированное использование политических дипфейков во время выборов является глобальной проблемой.

Многочисленные исследования утверждают, что к 2026 году до 90% онлайн-контента может быть создано с использованием синтетических технологий [4]. Это подразумевает, что дипфейки, вероятно, станут распространенным инструментом для киберпреступлений и прямого вмешательства в выборные процессы.

Согласно данным компании Sumsub за 2024 год, количество дипфейков по всему миру выросло более чем на 245% [5]. В некоторых странах, где выборы были намечены на 2024 год, таких как США, Индия, Индонезия, Мексика и Южная Африка, отмечен значительный прирост дипфейков [6].

Заключение. Применение политических дипфейков в ходе выборов 2023-2024 годов подчеркивает растущую угрозу применения цифровых технологий для воздействия на целевые аудитории различных стран.

Несмотря на наличие законодательных норм, ограничений и рекомендаций, активность по распространению дезинформации с применением политических дипфейков в последние годы значительно возросла, что приводит к их массовой вирусализации [7]. Одной из основных проблем в регулировании политических дипфейков является их скрытность, обусловленная использованием различных типов манипуляций. Кроме того, значительным препятствием для регулирования этой технологии является отсутствие общепризнанных международных стандартов.

Список источников и литературы:

1. Ballotpedia’s Artificial Intelligence Deepfake Legislation Tracker. Annual Report. // State of Deepfake Legislation, 2024. — 13 p.

2. Виноградова Е.А. Злонамеренное использование политических дипфейков и попытки их нейтрализации в странах Латинкой Америки // Латинская Америка. 2023, №. 5. С. 35-48. DOI: 10.31857/S0044748X0025404-3.

3. Busch Ella, Ware Jacob. The Weaponisation of Deepfakes. Digital Deception by the Far-Right. // ICCT Policy Brief December. 2023. — 20 p. DOI: 10.19165/2023.2.07 20.

4. Pawelec Maria. Deepfakes als Chance für die Demokratie? // The Nomos eLibrary. 2024. P.89-101. DOI: https://doi.org/10.5771/9783748928928-89, am 07.08.2024, 13:32:45.

5. Robichaud-Durand S. L'hypertrucage: analyse du phénomène des «deepfakes» et recommandations. // Lex Electronica. 2023. Volume 28. № 4. P. 78-98. DOI: https://doi.org/10.7202/1108807aradresse copiéeune.

6. Ziobroń Agata. Political deepfake. Remarks de lege lata and postulates de lege ferenda. Rozprawy i Materiały. 2024. № 1 (34). P.79-95. DOI: 10.48269/2451-0807-sp-2024-1-04.

7. Deepfake Cases Surge in Countries Holding 2024 Elections, Sumsub Research Shows. URL: https://sumsub.com/newsroom/deepfake-cases-surge-in-countries-holding-2024-elections-sumsub-research-shows/ (дата обращения: 22.07.2024)

Анна Николаевна Журих,
Студент факультета политических и социальных технологий,
Российский государственный социальный университет,
E-mail: dc.report1589@gmail.com

Anna N. Zhurikh,
Student of the Faculty of Political and Social Technologies,
Russian State Social University,
E-mail: dc.report1589@gmail.com

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ. ПЕРСПЕКТИВЫ И УГРОЗЫ В ОБЛАСТИ МЕЖДУНАРОДНЫХ ОТНОШЕНИЙ

ARTIFICIAL INTELLIGENCE. PROSPECTS AND THREATS IN THE FIELD OF INTERNATIONAL RELATIONS

Аннотация. В рамках данного исследования предпринята попытка ознакомиться с характеристиками, принципом работы и областью применения некоторых программ на основе искусственного интеллекта. Данный разбор направлен на то, чтобы классифицировать таковые программы, а также постараться определить перспективы и потенциальные угрозы подобных программ.

Ключевые слова: ИИ, классификация приложений, международные отношения, программы на основе ИИ, угрозы безопасности, изменение голоса и внешности.

Abstract. In the framework of this study, an attempt is made to get acquainted with the characteristics, principle of operation and field of application of some programs based on artificial intelligence. This analysis is aimed to classify such programs, as well asto try to determine the prospects and potential threats of such programs.

Keywords: AI, classification of applications, international relations, AI-based programs, security threats, voice and appearance modification.

Классификация основных характеристик программ на основе искусственного интеллекта. На сегодняшний день программы на основе искусственного интеллекта широко используются во всех сферах деятельности, от развлечений до медицины. Рассмотрим программы по изменению голоса и внешности, находящиеся в свободном доступе и позиционирующиеся создателями как инструменты маркетинга, средства развлечения и коммуникации. Классифицируем их по самым распространенным функциям – в первую очередь, это изменение голоса. С помощью программ для работы с голосом можно записывать подкасты, проводить стримы, онлайн-конференции или развлекаться, сохраняя анонимность. Такие программы умеют работать в режиме реального времени напрямую с микрофона, с загруженными аудиофайлами, с текстом. Способны изменять голос в мессенджерах, играх и любых приложениях. Добавлять эхо, создавать эффект плохого микрофона. Менять голос во время звонка на женский, мужской, детский или на голос кого-то из знаменитостей. Умеют выбирать подходящую эмоциональную окраску текста и генерировать диалог с разными голосами, способны добавлять паузы в речь, менять тембр и усиливать отдельные слова. Некоторые программы могут всё это осуществлять на разных языках.

Таким образом, актуальный на 2024 год «Synthesis» имеет в библиотеке 34 женских и 35 мужских профессиональных чрезвычайно реалистичных голосов [10]. У голосового генератора «Lovo.ai» самая большая в мире библиотека из более чем 500 голосов с более чем 20 эмоциями и более чем 150 языками. Голоса звучат по-человечески реалистично. Есть редактор произношения, акцента, скорости и высоты тона. База данных звуковых эффектов, бесплатной музыки, стоковых фото и видео [7]. Программа «HitPaw VoicePea» считается одним из лучших приложений для геймеров, стримеров, блогеров. Позволяет изменить свой голос в режиме реального времени. Интегрируется со всеми популярными играми и программами [6].

Следующая функция – изменение внешности. Такие программы способны изменять внешность на фото и видео, включая цвет волос, форму лица, возраст. Многие программы уже сейчас умеют генерировать не только анимацию и виртуальных персонажей, но и специализируются на замене лиц на видео с высокой степенью реализма. Применяют сложные алгоритмы, благодаря которым у видео сохраняется естественный вид без видимых цифровых изменений.

Если инструмент «Akool Face Swap» обеспечивает высококачественные, реалистичные результаты, будучи простым в использовании. Не требует специальных навыков [4]. А платформа «Based Labs AI Face Swapper» гарантирует естественный вид изображения, без явных признаков цифровых манипуляций [5]. Работает на различных платформах, включая десктопные и мобильные устройства, то приложение «Pixble» использует искусственный интеллект для точного обнаружения и отображения деталей лица. Создает точные и реалистичные 3D-замены лица. Обрабатывает изображения, снятые под разными углами или сбоку. Обеспечивает убедительно реалистичную смену лица [8]. Программа «Swapface» легко интегрируется с виртуальными камерами, такими как «OBS», что облегчает создание гиперреалистичных дипфейков в режиме реального времени для прямой трансляции на различных платформах, включая «Skype», «Zoom», «Teams» и «Meet». Особенность «Swapface», это удивительно реалистичная визуализация его дипфейков, из-за чего становится все труднее различать фактические кадры и контент, синтезированный искусственным интеллектом. Это делает «Swapface» предпочтительным выбором среди стримеров [9].

Так называемые дипфейки уже активно проявляются, в том числе в международной политике. Напомню о том, как в 2023 году на прямой линии с президентом России Владимиром Владимировичем Путиным, вопрос о том, как президент относится к опасностям, которые несет в нашу жизнь искусственный интеллект и нейросети, задавал двойник-президента, представившийся студентом СПбГУ [3]. А российские пранкеры Владимир

Кузнецов и Андрей Столяров, более известные как Вован и Лексус, уже неоднократно звонили различным иностранным лидерам и вели с ними разговор от лица других политиков, после чего содержание беседы становилось достоянием общественности.

Перспективы и угрозы программ на основе искусственного интеллекта. На основании вышеизложенных характеристик хочу отметить, что искусственный интеллект в целом, и программы на его основе в частности, несут в себе как огромные возможности, так и серьезные риски для международных отношений.

К ключевым угрозам можно отнести то, что подобные программы способны повысить эффективность сбора информации в разведывательной сфере, создавая угрозы национальной безопасности [13]. Дипфейки могут использоваться для создания фальшивых видеозаписей политиков и лидеров мнений, что непременно отразится на их репутации и подорвет доверие к ним. Кроме того, данные программы могут использоваться для разжигания межнациональных конфликтов и манипуляций общественным мнением, путем распространения дезинформации и пропаганды. Наконец, отсутствие гарантий безопасного и этичного развития и применения подобных программ, а также контроля за ними. В 2018 году М.П. Булавина в своем обзоре «Риски и угрозы новых технологий, основанных на искусственном интеллекте» справедливо подняла вопрос не только о том, кто будет контролером таких программ, но и о том, кто сможет проконтролировать самого контроллера [1].

Заключение. Искусственный интеллект – это мощный инструмент, который может, как помочь решить глобальные проблемы, так и усугубить их. Сами по себе программы с использованием искусственного интеллекта не опасны, как это и задумывалось разработчиками. Опасность заключается в том, как эти программы используются человеком.

Очевидно, что предотвратить развитие искусственного интеллекта невозможно. Если говорить о национальной безопасности то, единственной надежной защитой может стать только разработка более совершенных

программ, способных работать на опережение [2], то есть руководствоваться теми же принципами, что и при разработке вооружения [11].

В рамках международных отношений безусловно следует разработать механизмы регулирования таких программ и внедрить общие стандарты и правила [12]. Не менее важно донести до общественности идею критически осмысливать информацию, которую они получают, и уметь отличать правду от фейка. Разрабатывать защитные программы и алгоритмы, которые будут помогать распознавать потенциально опасные продукты таких программ и предотвращать их распространение.

Список источников и литературы:

1. М.П. Булавинова. Риски и угрозы новых технологий, основанных на искусственном интеллекте. 2018.02.004 С. 33-36. URL: https://cyberleninka.ru/article/n/riski-i-ugrozy-novyh-tehnologiy-osnovannyh-na-iskusstvennom-intellekte-obzor/viewer (дата обращения 20.10.2024)

2. А.С. Киселев. О необходимости правового регулирования в сфере искусственного интеллекта: дипфейк как угроза национальной безопасности. Вестник Московского государственного областного университета. Серия: Юриспруденция. 2021/№3 С. 54-62. URL: https://cyberleninka.ru/article/n/o-neobhodimosti-pravovogo-regulirovaniya-v-sfere-iskusstvennogo-intellekta-dipfeyk-kak-ugroza-natsionalnoy-bezopasnosti/viewer (дата обращения 20.10.2024)

3. Прямая линия с президентом РФ от 14.12.2023 года. Репортаж Е. Аксеновой 14.12.2023 15:30 Елизавета Аксенова. URL: https://spbdnevnik.ru/news/2023-12-14/video-vopros-putinu-zadal-ego-dvoynik-iz-peterburga (дата обращения 20.10.2024)

4. Сайт программы на основе искусственного интеллекта Akool Face Swap. URL: https://akool.com/apps/faceswap (дата обращения 20.10.2024)

5. Сайт программы на основе искусственного интеллекта Based Labs AI Face Swapper. URL: https://www.basedlabs.ai/apps/face-swap (дата обращения 20.10.2024)

6. Сайт программы на основе искусственного интеллекта HitPaw VoicePea. URL: https://www.hitpaw.com/photo-enhancer.html (дата обращения 20.10.2024)

7. Сайт программы на основе искусственного интеллекта Lovo.ai. URL: /https://lovo.ai// (дата обращения 20.10.2024)

8. Сайт программы на основе искусственного интеллекта Pixble. URL: https://pixble.com/ (дата обращения 20.10.2024)

9. Сайт программы на основе искусственного интеллекта Swapface. URL: https://www.swapface.org/#/home (дата обращения 20.10.2024)

10. Сайт программы на основе искусственного интеллекта Synthesis. URL: https://synthesys.io/ (дата обращения 20.10.2024)

11. Указ Президента РФ Об Основах государственной политики Российской
Федерации в области ядерного сдерживания от 2 июня 2020 г. № 355. URL: https://www.mid.ru/ru/foreign_policy/international_safety/disarmament/1434131/(дата обращения 20.10.2024)

12. Указ Президента РФ от 10.10.2019 N 490 (ред. от 15.02.2024) "О развитии искусственного интеллекта в Российской Федерации" (вместе с «Национальной стратегией развития искусственного интеллекта на период до 2030 года»). URL: https://www.consultant.ru/document/cons_doc_LAW_335184/ (дата обращения 20.10.2024)

13. Федеральный закон «Об обороне» от 31.05.1996 N 61-ФЗ (последняя редакция). URL: https://www.consultant.ru/document/cons_doc_LAW_10591/ (дата обращения 20.10.2024)

Ксения Викторовна Власова,
к.и.н., доцент,
E-mail: kv_vlasova@vyatsu.ru

Виктория Александровна Мухачева,
студент, факультет истории, политических наук и культурологии,
Вятский государственный университет,
E-mail: mukhacheva.victoria@gmail.com

Ksenia V. Vlasova,
Ph.D. in Historical Sciences, Associate Professor,
E-mail: kv_vlasova@vyatsu.ru

Victoria A. Mukhacheva,
Student, Faculty of History, Political Sciences and Cultural Studies,
Vyatka State University,
E-mail: mukhacheva.victoria@gmail.com

ОТ МИФА К МАНИПУЛЯЦИИ: ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ И ПРОБЛЕМА РАСПРОСТРАНЕНИЯ ДЕЗИНФОРМАЦИИ В ГЛОБАЛЬНОЙ ПОЛИТИКЕ

FROM MYTH TO MANIPULATION: ARTIFICIAL INTELLIGENCE AND THE PROBLEM OF SPREADING DISINFORMATION IN GLOBAL POLITICS

Аннотация. Настоящее исследование направлено на изучение рисков, связанных с использованием искусственного интеллекта (ИИ) в распространении дезинформации, эскалации кибервойн и иных угроз, исходящих от применения ИКТ. Подчеркивается необходимость разработки этических и правовых норм. Работа призывает к созданию и использованию единых норм для регулирования ИИ.

Ключевые слова: искусственный интеллект, ИИ, международные отношения, политическая манипуляция, дезинформация

Abstract. The present study is aimed at studying the risks associated with the use of artificial intelligence (AI) in spreading disinformation, escalating cyberwarfare, etc. The need to develop ethical and legal norms is emphasized. The item calls for the creation and use of uniform norms to regulate AI.

Keywords: artificial intelligence, AI, international relations, political manipulation, disinformation.

Что такое искусственный интеллект и чем он может быть опасен? В книге «Искусственный интеллект: современный подход» [2] С. Рассел и П. Норвик дали следующее определение искусственного интеллекта (ИИ): «область компьютерных наук, которая занимается созданием систем, способными выполнять задачи, которые требуют в себя человеческие навыки: обучение, рассуждение, восприятие и принятие решений. Искусственный интеллект стремится к имитации поведения человека» [2, pp. 1-4]. В настоящее время можно наблюдать, что имеется огромное количество бесплатных сайтов для имитации голоса/характера/внешности и т.д., на которые пользователь самостоятельно загружают нужные данные. Конечно, многие сайты такого рода, включая бесплатные, не могут создать идеально точное изображение, точно воспроизвести голос, но они все равно являются «угрозой», особенно в эпоху развития социальных сетей таких, как X (бывший Twitter)[8], TikTok, Instagram[9] и многие другие, где при помощи настроенных алгоритмов показа постов информация распространяется довольно быстро. Например, загруженное в TikTok видео уже на следующий день может набрать миллионные просмотры, и речь идет не об одном-двух миллионах, а 5-10, что значительно ускоряет процесс распространения дипфейков – синтетических медиа, созданных с помощью методов ИИ-генерации для подделки аудиовизуального представления человека. Между тем опасность ИИ заключается в том, что его развитие и применение потенциально не контролируемы: например, в кибервойнах, различных манипуляциях общественным мнением, влиянии на экономику и международные отношения

[8]С 14 марта 2022 г. доступ пользователям из России ограничен по решению Роскомнадзора.
[9] Организация Meta, а также её продукты Instagram и Facebook, упомянутые в тезисах, признаны экстремистскими на территории РФ.

через дезинформационные вбросы. В такой ситуации критически важно применять этический и правовой контроль над использованием ИИ.

Этические нормы и правовые механизмы регулирования ИИ: необходимость общего решения. В сентябре 2024 г. ООН был выпущен доклад о необходимости регулятивных мер в использовании ИИ, где подчеркнуто, что «сегодня на глобальном уровне существует дефицит управление в отношении ИИ» [1, с. 6].Тем не менее, в настоящее время не существует какого-то межгосударственного этического и правого контроля, нормы которого обязались бы соблюдать все государства или их союзы. Это связано с тем, что в некоторых государствах или объединениях уже принято свое собственное законодательство в сфере ИИ: например, закон № 2024/1689 об искусственном интеллекте в Европейском Союзе [3]; билль о правах ИИ в США [4]. Таким образом, отсутствие единого международного этического стандарта для регулирования сферы ИИ может повлечь за собой следующие угрозы:

1. Эскалацию кибервойн и дезинформации: государства могут использовать ИИ для атак на критическую инфраструктуру противника, что приведет к разрушениям последнего без физического вмешательства. Также возможны информационные войны, где так называемые дипфейки и фейковые новости подрывают доверие к официальным источникам. В то же время анонимность в кибератаках затрудняет идентификацию агрессоров, а быстрое распространение дезинформации может дестабилизировать политическую систему мира.

2. Неравенство в доступе к технологиям: более развитые государства могут использовать ИИ для своего доминирования на международной арене, из-за чего менее технологически развитые страны останутся в уязвимом положении и без надлежащей правовой защиты.

3. Отсутствие защиты прав человека: без четкого этического регулирования ИИ могут нарушаться приватность, способствуя дискриминации и манипуляции поддельной аудиовизуальной информацией.

Перечисленные выше угрозы указывают на необходимость создания единого этического стандарта по регулированию ИИ на базе ООН для ограничения дезинформации, защиты личной информации и равного доступа к технологиям.

Заключение. С одной стороны ИИ в современном мире это помощник, с его помощью можно создавать музыку, редактировать текст или предлагать какие-то творческие решения, другой – ИИ можно назвать инструментом , помогающим в «не тех руках» создавать и распространять ложную информацию, создавать образ врага, вскрывать личную информацию и т.д. Однако ИИ необходимо регулировать во избежание использования его в недобросовестных целях. Примерами подобного регулирования можно использовать следующие меры предосторожности:

1. Разработку международных стандартов, что поможет создать единое представление об ИИ и ввести одинаковые правовые и этические нормы регулирования;
2. Создание национальных регулятивных органов, что приведет к исполнению международных стандартов и поможет выявить пробелы и проблемы в кибербезопасности отдельного взятого государства;
3. Мониторинг и оценка: данные действия помогут оперативно реагировать на воздействие ИИ на общество и государство.

Список источников и литературы:

1. Управление искусственным интеллектом в интересах человечества. Сентябрь 2024 г. [Электронный ресурс]. URL: https://www.un.org/sites/un2.un.org/files/governing_ai_for_humanity_final_report_ru_summary.pdf (дата обращения: 13.10.2024).
2. Russell S., Norvig P. Artificial Intelligence: A Modern Approach USA. 21 December 2021. [Электронный ресурс]. URL: https://people.engr.tamu.edu/guni/csce421/files/AI_Russell_Norvig.pdf (дата обращения: 13.10.2024).

3. EU AI Act № 2024/1689: First Regulation on Artificial Intelligence. 8 July 2023 [Электронный ресурс]. URL: https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence (дата обращения: 13.10.2024).

4. Blueprint for an AI Bill of Rights. Washington, DC. October 2022 [Электронный ресурс]. URL: https://www.whitehouse.gov/ostp/ai-bill-of-rights/#applying (дата обращения: 13.10.2024).

Аревик Жораевна Мартиросян,
к.ю.н., научный сотрудник ИАМП, руководитель Школы МИБ ИАМП,
ст.преподаватель кафедры стратегических коммуникаций
и государственного управления,
Дипломатическая академия МИД России,
E-mail: a.martirosian@dipacademy.ru

Arevik G. Martirosyan,
Ph.D, in Law, Researcher, Institute of Contemporary International Studies,
Head of the International Information Security School,
Senior Lecturer, Department of Strategic Communications
and Public Administration,
Diplomatic Academy of the Russian Ministry of Foreign Affairs,
E-mail: a.martirosian@dipacademy.ru

МЕЖДУНАРОДНОЕ РЕГУЛИРОВАНИЕ ИИ: ОСНОВНЫЕ ИТОГИ И ТЕНДЕНЦИИ 2024 Г.

INTERNATIONAL REGULATION OF AI: KEY RESULTS AND TRENDS OF 2024

Аннотация. Автором раскрыты основные вехи 2024 года в части разработки норм регулирования ИИ на международном уровне и тенденции в данной области. Рассмотрены доклад Консультативного органа ООН высокого уровня по ИИ, Глобальный цифровой договор, две резолюции Генеральной Ассамблеи ООН, Закон ЕС о регулировании искусственного интеллекта, Рамочная конвенция Совета Европы об искусственном интеллекте, правах человека, демократии и верховенстве закона, Казанская декларация БРИКС относительно положений, предметом которых выступает ИИ и управление ИИ.

Ключевые слова: искусственный интеллект, международное регулирование ИИ, ООН, управление ИИ.

Abstract. The author reveals the main milestones of 2024 in terms of the development of AI regulation at the international level and trends in this area. The provisions of report of the UN High-level Advisory Body on AI, the Global Digital

Compact, two resolutions of the UN General Assembly, the EU Law on the Regulation of Artificial Intelligence, the Council of Europe Framework Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law, the BRICS Kazan Declaration dedicated to AI and AI governance are considered.

Key words: artificial intelligence, international regulation of AI, the United Nations, AI governance.

В 2024 г. произошли значительные события в области международного регулирования искусственного интеллекта (ИИ), которые можно охарактеризовать как важный этап в формировании, если не глобальных подходов, то, как минимум, тенденций в направлении управления этой технологией. Организация Объединенных Наций (ООН) сыграла ключевую роль в продвижении ИИ-повестки.

Консультативный орган ООН высокого уровня по ИИ опубликовал доклад, содержащий семь ключевых рекомендаций по управлению рисками, связанными с искусственным интеллектом:

- создание международной научной группы по ИИ;
- организация нового политического диалога по управлению ИИ;
- создание центра обмена стандартами ИИ;
- формирование глобальной сети по наращиванию потенциала;
- учреждение глобального фонда для ИИ;
- разработка глобальной системы данных ИИ;
- создание «офиса» ИИ в Секретариате ООН [4].

Эти рекомендации, как заявляются, направлены на формирование «глобально инклюзивной и распределенной архитектуры управления ИИ» и призывают государства и заинтересованные стороны к совместной работе для содействия развитию и защите прав человека.

Примечательно, что многие положения нашли свое отражение в Глобальном цифровом договоре (ГЦД) [3]. ГЦД содержит раздел,

посвященный искусственному интеллекту: там зафиксированы базовые принципы разработки и применения ИИ – общие для большинства существующих национальных и международных походов в регулировании – доверенный характер ИИ, его безопасность, защищенность, надежность. Положения ГЦД – это нормы мягкого права, они будут носить декларативный характер и существенно не смогут повлиять на цифровую монополию отдельных стран и крупных корпораций. Несмотря на достаточно противоречивую природу ГЦД, процесс его разработки в очередной раз подтверждает необходимость четко выстроенного институционального механизма (организационно-правовой основы), в том числе по ИИ, нужно четко определить у каких органов системы ООН есть на то соответствующий мандат.

Важной вехой стало принятие первых резолюций ГА ООН по ИИ. Генеральная Ассамблея ООН приняла две исторические резолюции по ИИ в этому году: Резолюция «Использование возможностей безопасных, защищенных и надежных систем искусственного интеллекта для устойчивого развития» (A/78/265) (подчеркивает важность использования безопасных, защищенных и надежных систем ИИ для достижения целей устойчивого развития. Она акцентирует внимание на необходимости разработки и внедрения технологий, которые способствуют социальному и экономическому прогрессу, не нарушая при этом права человека) от 21 марта 2024 года [6] и Резолюция 78/311 «Укрепление международного сотрудничества в деле наращивания потенциала в области искусственного интеллекта» (эта резолюция направлена на укрепление международного сотрудничества и наращивание потенциала в области искусственного интеллекта, она призывает страны к совместной работе над созданием нормативной базы, которая будет учитывать риски и возможности ИИ) от 1 июля 2024 года [7]. В своей совокупности обе резолюции подчеркивают важность международного сотрудничества в области ИИ и необходимость развития потенциала в этой сфере.

Международные инициативы вне системы ООН также не отставали по темпу относительно шагов по выработке регулирования ИИ. Так, например, страны БРИКС внесли свой вклад в глобальную дискуссию по ИИ. В Казанской декларации БРИКС 2024 года были обозначены следующие приоритеты:

– признание ключевой роли ООН в глобальном управлении ИИ;

– создание альянса БРИКС в области ИИ (для регламентации технологий и предотвращения их противоправного использования);

– разработка этических норм и стандартов для использования ИИ [5].

Европейский союз принял первый в мире системный нормативно-правовой акт по регулированию ИИ. Закон о регулировании искусственного интеллекта (AI Act) [1]. Этот закон был предложен Европейской комиссией в апреле 2021 года, принят Европейским парламентом в марте 2024 года и одобрен Советом ЕС в мае 2024 года. Он вступил в силу 1 августа 2024 года. Он устанавливает обязательства для компаний, разрабатывающих и использующих системы ИИ, с акцентом на безопасность и прозрачность.

17 мая 2024 года в Страсбурге на ежегодном министерском заседании Комитета министров Совета Европы была принята Рамочная конвенция Совета Европы об искусственном интеллекте, правах человека, демократии и верховенстве закона, направленная на обеспечение соблюдения прав человека, верховенства закона и демократических стандартов при использовании систем ИИ [2]. Конвенция охватывает весь жизненный цикл систем ИИ и устанавливает правовую основу для их безопасного и ответственного использования, включая меры по снижению рисков для прав человека и демократии). Документ основывается на парадигме рисков для прав человека, выделяя основные угрозы, которые ИИ системы могут представлять для прав человека, демократии и верховенства закона. В этом контексте текст во многом повторяет принятый закон Европейского Союза по искусственному интеллекту и даже адаптирован под него. Особое внимание уделяется

возможности блокировки или введения моратория на развертывание ИИ-систем с высоким риском.

Что касается тенденций в области регулирования ИИ, то, с одной стороны, наблюдается стремление к мультистейкхолдерному подходу с точки зрения выработки глобальных регуляторных рамок и стандартов для ИИ. С другой стороны, мы можем констатировать появление блоковых инициатив. Вероятно увеличение числа международных альянсов и институтов для координации усилий в области ИИ.

В настоящее время отсутствуют всеобъемлющие международные соглашения, регулирующие ИИ. Существующие документы носят рекомендательный характер и представляют собой «мягкое право». Однако говорить о выработке всеобъемлющего договора пока преждевременно. Именно поэтому сохраняется акцент на необходимости разработки этических норм и стандартов безопасности для ИИ, которые выступают гибкой базой, способной адаптироваться к быстро развивающимся технологиям. Особое внимание уделяется развитию компетенций и инфраструктуры в области ИИ, особенно в развивающихся странах.

Заключение. Что касается перспективы глобальной повестки, то стоит отметить усиление роли ООН. Если ранее эта тема была смежной к ключевым вопросам повестки дня, то сегодня Всемирная организация заявила о своих намерениях и готовности играть центральную роль в координации глобальных усилий по регулированию ИИ. Поиск баланса между стимулированием инноваций и обеспечением безопасности и этичности ИИ, его регулированием станет ключевой задачей. Важно не допустить чрезмерной политизации вопросов регулирования ИИ и сохранить эту сферу как поле для конструктивного международного сотрудничества.

А с учетом включения в повестку развивающихся стран важно разработать модельные правовые акты в сфере ИИ, которые могли бы служить ориентиром для национальных законодательств. Важно продолжать работу над гармонизацией нормативных требований и обеспечением совместимости,

в том числе стандартов на международном уровне. Очевидно, что развитие ИИ требует согласования различных национальных правовых норм с международными стандартами. Однако из-за различий в правовых системах стран, таких как различия между прецедентным правом США и континентальным правом России, применение единых стандартов может быть затруднено. Тем не менее, международное сообщество признает необходимость сотрудничества и консенсуса в области регулирования ИИ. Успех в этой области будет зависеть от способности международного сообщества к диалогу, сотрудничеству и выработке общих подходов, учитывающих интересы всех стран. Необходимо также развивать многостороннее сотрудничество, избегая формирования «закрытых клубов».

Список источников и литературы:

1. Artificial Intelligence Act (Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828) [Электронный ресурс] // EUR-Lex. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R1689 (дата обращения: 25.10.2024).

2. Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law [Электронный ресурс] // Council of Europe Treaty Office. URL: https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=225 (дата обращения: 25.10.2024).

3. Global Digital Compact [Электронный ресурс] // Office of the Secretary-General's Envoy on Technology. URL: https://www.un.org/global-digital-compact/sites/default/files/2024-09/Global%20Digital%20Compact%20-%20English_0.pdf (дата обращения: 25.10.2024).

4. Governing AI for Humanity: Final Report [Электронный ресурс] // High-level Advisory Body on Artifcial Intelligence. URL: www.un.org/sites/un2.un.org/files/governing_ai_for_humanity_final_report_en.pdf (дата обращения: 25.10.2024).

5. Казанская декларация БРИКС 23 октября 2024 года [Электронный ресурс] // ЭСВУ БРИКС. URL: https://brics-expert.info/documents/dokumenty-esvu-briks/kazanskaya-deklaratsiya-briks-23-oktyabrya-2024-goda/ (дата обращения: 25.10.2024).

6. Резолюция 78/265 «Использование возможностей безопасных, защищенных и надежных систем искусственного интеллекта в целях устойчивого развития» [Электронный ресурс] // UNDOCS. URL: https://docs.un.org/ru/A/RES/78/265 (дата обращения: 25.10.2024).

7. Резолюция 78/311 «Укрепление международного сотрудничества в деле наращивания потенциала в области искусственного интеллекта» [Электронный ресурс] // UNDOCS. URL: https://docs.un.org/ru/A/RES/78/311 (дата обращения: 25.10.2024).

Артем Алексеевич Олифиренко,
Магистрант, Институт электронной техники и приборостроения,
Саратовский государственный технический
университет им. Гагарина Ю.А.,
E-mail: panolifer@gmail.com

Artem A. Olifirenko,
Master's student, Institute of Electronic Engineering and Instrumentation,
Yuri Gagarin Saratov State Technical University,
E-mail: panolifer@gmail.com

DATA POISONING: НОВЫЕ ГОРИЗОНТЫ УГРОЗ ДЛЯ МОДЕЛЕЙ МАШИННОГО ОБУЧЕНИЯ И СТРАТЕГИИ ПРОТИВОДЕЙСТВИЯ

DATA POISONING: NEW THREAT HORIZONS FOR MACHINE LEARNING MODELS AND COUNTERACTION STRATEGIES

Аннотация. В работе исследуется явление data poisoning как одной из ключевых угроз для систем машинного обучения. Представлена классификация атак и методы их реализации, а также обоснована необходимость разработки комплексных технических и правовых мер защиты. Особое внимание уделено гибридным стратегиям противодействия, включающим предварительную обработку данных и мониторинг модели, а также международному правовому регулированию, направленному на минимизацию трансграничных угроз и укрепление доверия к системам искусственного интеллекта.

Ключевые слова: data poisoning, машинное обучение, безопасность данных, правовое регулирование, гибридные стратегии защиты.

Abstract. The article examines data poisoning as one of the key threats to machine learning systems. It presents a classification of attacks and methods of their implementation, substantiating the need for comprehensive technical and legal protection measures. Special attention is paid to hybrid counteraction strategies, including data preprocessing and model monitoring, as well as international legal

regulation aimed at minimizing cross-border threats and strengthening trust in artificial intelligence systems.

Keywords: data poisoning, machine learning, data security, legal regulation, hybrid protection strategies.

Машинное обучение (machine learning, ML) является ключевым элементом современной технологической инфраструктуры, автоматизируя сложные процессы и позволяя принимать решения на основе анализа больших данных. Оно используется в медицине для диагностики заболеваний и анализа биомедицинских изображений, в финансовой сфере для управления кредитными рисками, выявления мошенничества и оптимизации портфелей [1,2]. Способность ML обрабатывать большие объемы данных и адаптироваться к изменениям делает его важным инструментом в современных экономических и социальных системах [4].

Однако зависимость ML от качества данных делает его уязвимым к атакам типа *data poisoning* (отравление данных). Такие атаки заключаются во внесении вредоносных или искаженных записей в обучающие выборки, что может привести к снижению точности или созданию преднамеренных уязвимостей в модели. Например, в системах компьютерного зрения злоумышленники могут внедрять изображения с триггерами, нарушающими корректность классификации, что особенно опасно в системах обороны и национальной безопасности [3]. В рекомендательных системах такие атаки могут исказить результаты, нанося репутационный и экономический ущерб [2].

Особую сложность представляет скрытность атак data poisoning. Злоумышленники, используя методы маскировки, создают данные, практически неотличимые от легитимных, что затрудняет их обнаружение стандартными алгоритмами. Ошибки, вызванные такими атаками, часто остаются незамеченными, снижая производительность модели на протяжении ее жизненного цикла [1]. Эти риски усиливаются в распределенных системах

обучения, таких как федеративное обучение, где злоумышленники могут контролировать отдельные узлы и внедрять искаженные обновления [6].

Международный аспект данных угроз особенно актуален, поскольку атаки *data poisoning* имеют трансграничный характер. Они могут быть направлены на нарушение доверия между странами, участвующими в совместных технологических проектах. Это требует создания унифицированных стандартов в рамках международного права. Например, протоколы Будапештской конвенции о киберпреступности могли бы быть дополнены положениями об ответственности за манипуляции с обучающими данными. Среди необходимых мер: создание глобального реестра инцидентов, регламентирование обязательного аудита данных и внедрение цифровых сертификатов для верификации источников [3, 7]. Такие меры помогут странам-участникам обмениваться данными и координировать усилия по предотвращению атак [5].

В Российской Федерации целесообразно дополнить ФЗ «О безопасности критической информационной инфраструктуры», включив обязательные требования к проверке целостности данных и установив административную и уголовную ответственность за использование искаженных выборок. Эти меры будут способствовать защите национальных систем и повышению доверия к технологиям [4].

Классификация атак разделяется на целенаправленные (*targeted attacks*), которые ориентированы на конкретные данные, и неизбирательные (*indiscriminate attacks*), направленные на общее снижение точности модели. *Backdoor*-атаки, например, используют триггеры для создания преднамеренных уязвимостей [6]. Такие атаки наиболее опасны для международных систем, где последствия могут быть катастрофическими [2; 6].

Для противодействия атакам типа *data poisoning* предлагается внедрение гибридной модели защиты, сочетающей предварительную обработку данных и мониторинг модели. Предварительная обработка включает очистку данных

с использованием алгоритмов обнаружения аномалий, валидацию источников с применением цифровых сертификатов, а также аугментацию для повышения разнообразия выборок. Эти методы направлены на снижение риска внедрения вредоносных данных на этапе подготовки к обучению. Мониторинг модели предполагает постоянный анализ метрик производительности, выявление аномалий во входных данных и адаптивное обновление моделей с учетом обратной связи.

Преимущества гибридной модели заключаются в ее гибкости, устойчивости к новым типам атак и возможности применения к различным системам. Экспериментальная проверка эффективности включает моделирование атак на тестовых наборах, анализ устойчивости моделей с защитой и без нее. Перспективы дальнейших исследований лежат в автоматизации обнаружения угроз, интеграции гибридной защиты в существующие ML-фреймворки и стандартизации подходов для повышения безопасности.

Таким образом, противодействие атакам *data poisoning* требует интеграции технических и правовых мер, включая международную координацию, мониторинг данных, выявление аномалий и внедрение стандартов. Только комплексный подход позволит минимизировать риски и укрепить доверие к интеллектуальным системам в условиях глобализации.

Список источников и литературы:

1. Данельян А.А. Международно-правовое регулирование киберпространства // Вестник международных организаций. – 2020. – № 1. – С. 140–155. – URL: https://cyberleninka.ru/article/n/mezhdunarodno-pravovoe-regulirovanie-kiberprostranstva (дата обращения: 15.11.2024).

2. Сатканов Р.Т. Деликтные обязательства в международном частном праве // Журнал прикладных исследований. – 2023. – № 7. – С. 116–120. – URL: https://cyberleninka.ru/article/n/deliktnye-obyazatelstva-v-mezhdunarodnom-chastnom-prave (дата обращения: 15.11.2024).

3. Гисель Л., Роденхойзер Т., Дёрманн К. Двадцать лет спустя: международное гуманитарное право и защита гражданских лиц от последствий кибероперациий во время вооруженных конфликтов // Международный обзор Красного Креста. – 2021. – № 913. – URL: https://international-review.icrc.org/ru/articles/twenty-years-ihl-effects-of-cyber-operations-during-armed-conflicts-913 (дата обращения: 15.11.2024).

4. Молодой ученый. Проблема злоупотребления правом в сфере международного частного права // Молодой ученый. – 2021. – № 4 (346). – С. 420–422. – URL: https://moluch.ru/archive/346/77917/ (дата обращения: 15.11.2024).

5. Цифровые платформы и международное частное право, или есть ли будущее у киберправа. // Вестник цифрового права. – 2020. – № 2. – С. 45–60. – URL: https://cyberleninka.ru/article/n/tsifrovye-platformy-i-mezhdunarodnoe-chastnoe-pravo-ili-est-li-buduschee-u-kiberprava (дата обращения: 15.11.2024).

6. Защита персональных данных: международные документы и национальные правовые акты. // Lawtrend. – 2005. – URL: https://www.lawtrend.org/information-access/zashhita-personalnyh-dannyh/mezhdunarodnye-i-natsionalnye-pravovye-akty (дата обращения: 15.11.2024).

7. Источники международного частного права. // Молодой ученый. – 2022. – № 11 (497). – С. 123–126. – URL: https://moluch.ru/archive/497/108952/ (дата обращения: 15.11.2024).

Вероника Ильинична Прошина,
Магистрант факультета международных отношений
СПбГУ,
E-mail: Nickshin004@mail.ru

Veronika I. Proshina,
Master's Degree Student, Faculty of International Relations,
St. Petersburg State University,
E-mail: Nickshin004@mail.ru

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В ВОЕННОЙ СРЕДЕ И РАЗВЕДКЕ США

ARTIFICIAL INTELLIEGENCE IN U.S. MILITARY AND INTELLIEGNCE

Аннотация. В данном исследовании автор стремится охарактеризовать современные цифровые инструментарии, внедрённые в концепты функционала органов безопасности США. Искусственный интеллект, который занимает ведущие позиции в вопросах информационной безопасности, изученный в контексте разведывательного сообщества и военной среды главного оппонента РФ, представляет особый научный интерес. Данное исследование призвано представить основные характеристики технологий искусственного интеллекта как инструмента современного разведывательного сообщества и военной среды США. Исследование было проведено на основе контент-анализа источников разведывательного сообщества США: отчетов Управления Директора национальной разведки США и Директора Центрального разведывательного управления США, а также слушаний 118-го Конгресса США (комитетов по разведке и внешней политике Палаты представителей и Сената).

Ключевые слова: разведка, искусственный интеллект, ИИ в разведке, разведывательное сообщество США, ИИ в военной среде.

Abstract. In this research, the author seeks to characterise modern digital tools embedded in the concepts of US security agencies. Artificial intelligence, which

occupies a leading position in information security issues, studied in the context of the intelligence community and military environment of Russia's main opponent, is of particular interest. This study aims to present the main characteristics of artificial intelligence technologies as a tool of the modern US intelligence community and military environment. The study was conducted on the basis of content analysis of US intelligence community sources: reports of the US Office of the Director of National Intelligence and the Director of the US Central Intelligence Agency, as well as hearings of the 118th US Congress (House and Senate Intelligence and Foreign Policy Committees).

Keywords: artificial intelligence, AI in intelligence, US intelligence community, AI in the military.

Наиболее важным преимуществом ИИ в контексте разведке и военной сферы является возможность быстрого анализа большего объема данных: искусственный интеллект способен обрабатывать и анализировать огромные объемы информации из различных источников, выявляя закономерности, тенденции и связи, которые могут быть незаметны для человека. Нейросети могут автоматически мониторить и фильтровать информацию из различных источников, идентифицируя ключевые события, тренды или угрозы. Одним из наиболее важных проектов в разведывательной среде является документ по эффективизации ИИ в разведке – Стратегия «Повышение эффективности разведдеятельности с помощью машин» (The AIM strategy) от 2019 года [1]. В документе Дэн Коутс, Директор Национальной разведки США с 2017-2019 гг., определил технологии «The AIM» как ключевые элементы преобразований, которые могут помочь аналитикам эффективно использовать растущий объем данных для принятия решений. По мнению экспертов, участвовавших в составлении документа, идеальная система ИИ: «Машина, способная достичь идеального человеческого интеллекта при скорости, мощности и точности компьютера» [1].

Функции ИИ в разведке. В документе выделяется основное различие между AGI (Искусственный интеллект общего назначения) и GenAI (Генеративный ИИ), которые используются в разведке, и в первую очередь оно заключается в объеме их возможностей.

Не мало важной способностью ИИ является его навык выявлять аномальные или необычные паттерны в данных, что может указывать на потенциальные риски или важные события. ИИ применяется для предотвращения кибератак, а также для обнаружения потенциальных угроз, исходящих от конкретных лиц или преступных группировок. Специально выстроенные точечные алгоритмы выявления информации, по конкретным словам, могут предотвращать теракты и различную преступную деятельность. Так, по данным «Ежегодного отчета об угрозах разведывательного сообщества США 2023 года» [2], кибербезопасность является важнейшим направлением в стратегии по обеспечении безопасности страны.

Итак, основными функциями искусственного интеллекта в разведывательном сообществе являются: 1) распознавание и идентификация изображения - системы на базе ИИ могут быстро распознавать и идентифицировать объекты и людей по огромному количеству спутниковых, аэрофотоснимков, сделанных с беспилотников; 2) перевод языков – ИИ может быстро переводить письменные и голосовые сообщения на иностранные языки; 3) геопространственный анализ: то есть, работа ИИ в рамках геопространственной разведки. Немало важной функцией геопространственной разведки является определение, разработка и создание цифровых двойников противника; 4) прогнозирование и предсказание – ИИ позволяет анализировать исторические данные для выявления закономерностей и делать прогнозы относительно текущих и будущих событий; 5) усиленный искусственным интеллектом человеческий интеллект – системы искусственного интеллекта работают вместе с человеком, помогая анализировать огромные массивы данных, обеспечивая автоматизированный анализ и контекстное понимание, а также повышая эффективность принятия

решений человеком. Для административных задач, касаемых внутреннего устройства той или иной спецслужбы и организационных моментов, могут использоваться следующие функции ИИ: виртуальные помощники, ИИ применяется для поддержки базовых задач, таких как составление расписания, поиск информации, предоставление напоминаний и предупреждений; автоматизированная отчетность – ИИ может использоваться для создания автоматических отчетов на основе пользовательских спецификаций и входных параметров.

Главным преимуществом ИИ является его способность выявлять в режиме реального времени или крайне быстро взаимосвязи между наблюдениями и заключениями по всем вышеперечисленным позициям. По каждому из указанных, на первый взгляд тривиальных аспектов, особенностью применения ИИ является его способность не столько повторять выполняемую функцию, сколько на основе такого повторения самообучаться.

ИИ в БПЛА. В период вооруженного конфликта для разведывательных целей активно применяется малозаметная техника, оборудование на основе ИИ. Так, беспилотные летательные аппараты (БПЛА) или дроны, играют ключевую роль в современной военной сфере, предоставляя различные преимущества по сравнению с традиционными средствами боевой техники. На сегодняшний день беспилотник являются наиболее технологичными «бойцами» на военной арене, и имплементация ИИ в их «организм» делает работу дронов еще более эффективной. Эти устройства могут быть использованы для разведки, наблюдения, атаки целей, доставки грузов, электронной борьбы и многих других задач. Современной особенностью использования беспилотников разного рода является их управление ИИ, а не человеком. ИИ, как и оператор обучается, нарабатывает, формирует опыт управления беспилотниками, но делает он это не на основе многократного управления одним беспилотником, а на основе многократного управления множеством беспилотников, аккумулируя получаемый опыт в один массив данных-умений, который постоянно пополняется, таким образом

совершенствуя навык управления беспилотниками. ИИ, в отличие от оператора, при управлении беспилотником способен учитывать значительно больший объем данных, чем способен человек: погодные условия, уже имеющиеся и изменяющиеся разведданные, информация, получаемая от других беспилотников, геопространственные данные о местности, эффекты возможного противодействия и т.п Министерство обороны США планирует предложить финансирование в рамках своего бюджетного запроса на 2026 финансовый год с целью создания «значительно улучшенных» систем противодействия беспилотной обороне в течение двух лет [3].

Заключение. ИИ в разведывательном сообществе США применяется для обработки огромных объемов данных. Это происходит в режиме реального времени, но уже не синхронно с получением данных. Однако ИИ позволяет сократить отставание при обработке и интерпретации информации, вызванное растущим объемом собираемых данных, при обеспечении процесса принятия решений. Ответственные лица, принимающие решения, получают информацию в режиме реального времени, период ее интерпретации и оценки сводится к нескольким часам. Технологии ИИ, которыми оперирует РС США в настоящее время, еще не могут определять и предупреждать о дезинформационных кампаниях. Однако наблюдаются признаки того, что ИИ в настоящее время обучается такому функционалу.

В стратегии по сбору информации из открытых источников 2024-2026 гг. от Управления директора национальной разведки, подчеркивается, что РС должно быть внимательно к рискам в области открытых источников, в том числе к проверке и достоверности получаемой информации [4]. Быстрая добыча данных из открытых источников требует от разведслужб постоянной адаптации своих собственных инструментов и методов работы для поддержания способности предоставлять своевременную и достоверную информацию из открытых источников политикам и военным в быстром и масштабном режиме. Метод OSINT в разведке уже является новатором в использовании искусственного интеллекта, машинного обучения. Для

сохранения конкурентных преимуществ РС ставит перед собой цель расширять и ускорять эти усилия.

Технологии ИИ, которыми оперирует РС США в настоящее время, при сборе информации не могут выявлять признаки проявления применения технологий ИИ в информационных кампаниях в киберпространстве. Нет оснований, чтобы утверждать, что применяемый ИИ разведывательным сообществом США понимает, когда взаимодействует с ИИ контрагента. Открытым остается вопрос, который, вероятно, целенаправленно обходят все отчеты Управления директора национальной разведки, о том, работают ли технологии ИИ, которыми оперирует РС США в настоящее время, только с открытыми данными. Кроме того, нет оснований утверждать, что технологии ИИ, применяемый РС США, не обучены и не применяются для сбора информации также и из закрытых источников.

Список источников и литературы:

1.The AIM initiative: a strategy for augmenting intelligence using machines. Available at: https://www.dni.gov/index.php/newsroom/reports-publications/reports-publications-2019/3286-the-aim-initiative-a-strategy-for-augmenting-intelligence-using-machines (Accessed: 15.10.2024).

2. The 2023 Annual Threat Assessment report. Available at: https://www.dni.gov/files/ODNI/documents/assessments/ATA-2023-Unclassified-Report.pdf (Accessed: 15.10.2024).

3. Office of the Under Secretary of Defense (Comptroller)/Chief Financial Officer March 2024 Defense Budget Overview United States Department of Defense Fiscal Year 2025 Budget Request Revised April 4, 2024. Available at: https://comptroller.defense.gov/Portals/45/Documents/defbudget/FY2025/FY2025_Budget_Request_Overview_Book.pdf (Accessed: 10.10.2024).

4. The OSINT-strategy-2024-2026. Available at: https://www.dni.gov/index.php/newsroom/reports-publications/reports-publications-2024 /3785-the-ic-osint-strategy-2024-2026 (Accessed: 15.10.2024).

Дарья Алексеевна Степовая,
аспирант факультета глобальных процессов,
МГУ имени М.В.Ломоносова,
E-mail: daria.stepovaya@gmail.com

Daria A.Stepovaya,
Ph.D. candidate of the Faculty of Global Studies,
Lomonosov Moscow State University,
E-mail: daria.stepovaya@gmail.com

ВЛИЯНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА НА ДОСТИЖЕНИЕ ЦЕЛЕЙ УСТОЙЧИВОГО РАЗВИТИЯ

THE IMPACT OF ARTIFICIAL INTELLIGENCE ON THE ACHIEVEMENT OF SUSTAINABLE DEVELOPMENT GOALS

Аннотация. Применение искусственного интеллекта (далее - ИИ) в достижении Целей устойчивого развития (далее - ЦУР) открывает новые перспективы в таких сферах, как здравоохранение, образование, экология и экономика. Однако, наряду с положительными эффектами, существуют серьезные риски, включая цифровое неравенство, утечку данных и безработицу. В статье анализируются как возможности, так и угрозы, связанные с ИИ в контексте устойчивого развития. Подчеркивается необходимость комплексного подхода к регулированию и внедрению технологий ИИ для обеспечения справедливого и инклюзивного прогресса.

Ключевые слова: искусственный интеллект, цели устойчивого развития, цифровая трансформация, риски, автоматизация, экология, экономический рост.

Abstract. The application of artificial intelligence (AI) in achieving the Sustainable Development Goals (SDGs) offers new perspectives in areas such as health, education, environment and economy. However, along with positive effects, there are serious risks, including digital inequality, data leakage and unemployment. The article analyzes both opportunities and threats associated with AI in the context of sustainable development. It emphasizes the need for an integrated approach to the

regulation and deployment of AI technologies to ensure equitable and inclusive progress.

Keywords: artificial intelligence, sustainable development goals, digital transformation, risks, automation, ecology, economic growth.

Принятие «Повестки дня в области устойчивого развития на период до 2030 года» обозначило глобальную задачу устранения бедности, сокращения неравенства и защиты окружающей среды. ИИ может ускорить выполнение этих целей за счет автоматизации процессов, анализа больших данных и оптимизации использования ресурсов [5].

В здравоохранении ИИ уже способствует ранней диагностике заболеваний и персонализированному лечению, что помогает достичь ЦУР 3 [3]. В образовании интеллектуальные платформы адаптируют учебный процесс под индивидуальные потребности, повышая качество знаний (ЦУР 4) [3]. В сельском хозяйстве алгоритмы ИИ повышают урожайность и продовольственную безопасность, способствуя выполнению ЦУР 2.

ИИ также активно используется в управлении городами, формируя концепцию «умных городов», что соответствует ЦУР 11 [6]. В области экологии технологии ИИ помогают отслеживать климатические изменения, прогнозировать природные катастрофы и разрабатывать стратегии их предотвращения, что соответствует ЦУР 13 [6]. В экономике автоматизация с помощью ИИ способствует увеличению производительности и экономическому росту (ЦУР 8), однако сопровождается рисками потери рабочих мест в традиционных отраслях [4].

В Российской Федерации также ведется активная работа по внедрению ИИ в рамках национальных программ цифровой трансформации. В 2023 году страна заняла 56 место в глобальном индексе достижения ЦУР, демонстрируя «умеренные улучшения» по ряду показателей. Национальные проекты в сфере цифровой экономики направлены на достижение таких целей, как ликвидация бедности (ЦУР 1), улучшение здравоохранения (ЦУР 3) и создание

устойчивой инфраструктуры (ЦУР 9) [1]. Однако остаются нерешенные вопросы, связанные с доступностью технологий и регулированием рисков ИИ.

Вместе с тем, для ответственного применения ИИ необходимо учесть целый ряд как этических, так и социальных аспектов, которые напрямую влияют на его эффективность и справедливость. Одним из ключевых вопросов является защита конфиденциальности и безопасности данных, поскольку надёжная защита информации является основой для поддержания доверия общества к системам ИИ. Нарушение приватности может привести к утрате доверия граждан к государственным и частным институтам, что подрывает усилия по достижению ЦУР, направленных на обеспечение равенства и социальной справедливости. Важным аспектом является и риск усиления существующего неравенства из-за предвзятости алгоритмов, что может способствовать углублению разрыва между различными социальными группами. Постоянный мониторинг, а также разработка и внедрение мер по минимизации таких рисков становятся необходимыми для того, чтобы технологии ИИ не способствовали усилению несправедливости и неравенства.

Заключение. Таким образом, несмотря на всеобъемлющие возможности, которые искусственный интеллект открывает для ускоренного прогресса в достижении ЦУР, крайне важно уделить должное внимание этическим вопросам, чтобы технологии служили инструментом инклюзивного и справедливого развития. В этом контексте необходимо не только правильно регулировать риски, такие как предвзятость в алгоритмах или доступность технологий для различных групп населения, но и налаживать сотрудничество между государственными структурами, частным сектором и гражданским обществом. Только при условии эффективного взаимодействия всех заинтересованных сторон можно использовать весь потенциал ИИ для улучшения качества жизни людей и продвижения к достижению глобальных целей устойчивого развития.

Список источников и литературы:

1. Указ Президента Российской Федерации от 07.05.2024 г. № 309 «О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года» // Президент России [Электронный ресурс]. URL: http://kremlin.ru/acts/bank/50542 (дата обращения: 10.10.2024).

2. Побочный эффект оценивает такие побочные эффекты по трем параметрам: экологические и социальные последствия, воплощенные в торговле, экономике и финансах, а также безопасности. Более высокий балл означает, что страна вызывает больше положительных и меньше отрицательных побочных эффектов.

3. Fraisl D. [и др.]. Leveraging the collaborative power of AI and citizen science for sustainable development // Nature Sustainability. 2024. С. 1–8.

4. Mehrabi N. [и др.]. A Survey on Bias and Fairness in Machine Learning // arXiv.org [Электронный ресурс]. URL: https://arxiv.org/abs/1908.09635v3 (дата обращения: 10.10.2024).

5. Sustainable Development Report 2024 [Электронный ресурс]. URL: https://dashboards.sdgindex.org/ (дата обращения: 10.10.2024);

6. Times of crisis, times of change. Science for accelerating transformations to sustainable development. Global sustainable development report 2023 // United Nations [Электронный ресурс]. URL: https://sdgs.un.org/sites/default/files/2023-09/FINAL%20GSDR%202023-Digital%20-110923_1.pdf (дата обращения: 10.10.2024).

7. Vinuesa R. [и др.]. The role of artificial intelligence in achieving the Sustainable Development Goals // Nature Communications. 2020. № 1 (11). С. 233.

Марта Винцасовна Стучкайте,
студентка 4 курса факультета международных отношений,
Северо-Кавказский федеральный университет,
E-mail: mstuchkaite@yandex.ru

Marta V. Stuchkaite,
4th year student, Faculty of International Relations,
North Caucasus Federal University,
E-mail: mstuchkaite@yandex.ru

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ – БУДУЩИЙ АКТОР МЕЖДУНАРОДНЫХ ОТНОШЕНИЙ?

IS ARTIFICIAL INTELLIGENCE A FUTURE ACTOR IN INTERNATIONAL RELATIONS?

Аннотация. Данное исследование направлено на проведение анализа роли искусственного интеллекта (ИИ) в современных международных отношениях. Автор приходит к выводу, что на данный момент ИИ трансформируется из инструмента сбора и анализа данных в самостоятельный актор международных отношений.

Ключевые слова: искусственный интеллект, акторы международных отношений, нейросеть, дипфейки, мировая политика.

Abstract. This study is aimed at analyzing the role of artificial intelligence (AI) in modern international relations. The author concludes that at the moment AI is being transformed from a tool for data collection and analysis into an independent actor of international relations.

Keywords: artificial intelligence, actors in international relations, neural network, deepfakes, world politics.

Акторы современных международных отношений. На данный момент наблюдается хаотизация системы международных отношений (МО). Это обусловлено потерей национальными государствами монополии в

инфраструктуре МО. В 1977 году представители неолиберальной школы международных отношений Джозеф Най и Роберт Кеохейн ввели концепцию комплексной взаимозависимости, согласно которой негосударственные акторы («акторы вне суверенитета») играют ключевую роль на международной арене. К «акторам вне суверенитета» относятся транснациональные компании (ТНК), международные правительственные и неправительственные организации, СМИ, частные военные компании, террористические организации, религиозные объединения, отдельные личности и так далее.

В связи с расширением круга субъектов, влияющих на политические процессы, представитель бихевиористской школы МО Дэвид Сингер предложил анализировать поведение всех возможных участников международных отношений, не устанавливая приоритет относительно их роли на мировой арене [5]. Таким образом, в современных международных отношениях сложно выделить ключевого актора, который консолидирует и задает тон процессам, протекающим на мировой арене.

Роль искусственного интеллекта в международных отношениях. 1956 год считается точкой отсчета эпохи искусственного интеллекта (ИИ). Именно в этом году состоялась Дартмутская конференция, на которой был предложен термин «искусственный интеллект». Примерно до 2010-х годов ИИ применялся в качестве инструмента анализа большого объема данных. Так, например, во время президентской кампании Барака Обамы в 2012 году были использованы технологии искусственного интеллекта «для расчета наилучшего дня, штата и аудитории для публичного выступления Б. Обамы. По разным оценкам, это обеспечило преимущество в 10–12% голосов» [2]. Следовательно, ИИ помогал обрабатывать данные, выявлять закономерности и составлять прогнозы.

В последнее время стал активно обсуждаться вопрос о становлении искусственного интеллекта в качестве самостоятельного актора

международных отношений. Речь в первую очередь идет о генеративном ИИ, который представляет собой нейросети ChatGPT, YandexGPT, Pictory и др.

Возникает угроза применения данных технологий с целью манипуляции массового сознания. Подтверждением этому тезису являются дипфейки, использование которых приводит к преднамеренному созданию ложных нарративов. Так, ярким примером выступает дипфейк 2019 года, из-за которого в Габонской Республике возникла большая вероятность государственного переворота [3]. Также в ряде стран отмечены попытки распространять дипфейковые видеоролики для подрыва репутации оппозиционных политиков. «Сегодня дипфейки – это инструмент шантажа, информационных и политических диверсий, способ «легендирования» недостоверных событий и новостей, диффамации и искусственной дестабилизации политической обстановки в отдельно взятой стране или обществе» [1].

Также стоит отметить роль ChatGPT в предвыборных кампаниях. Научно-исследовательская организация OpenAI с начала 2024 года зарегистрировала более 20 попыток использовать ChatGPT для создания контента, предназначенного для оказания влияния на президентские выборы по всему миру [4]. Таким образом, в случае запроса о выборе руководителя страны, искусственный интеллект может преднамеренно выдать ложную информацию, а следовательно, повлиять на исход предвыборной гонки.

Более того, развитие ИИ приводит к кардинальным изменениям характера войны. Речь не только о автоматизации и роботизации войск, но и о планировании военных операций с помощью искусственного интеллекта. Так, в декабре 2023 года ЦАХАЛ, при проведении ударов по объектам, принадлежащим ХАМАС в секторе Газа, использовал системы искусственного интеллекта для выбора целей [6].

Таким образом, ИИ начинает играть роль не только «помощника» в выстраивании курса политики того или иного государства (до 2010-х годов искусственный интеллект использовали для сбора и анализа данных), но и

самостоятельного участника международных отношений. Манипулируя общественным мнением, изменяя характер войны, влияя на принятие военно-стратегических решений, ИИ преобразует систему международных отношений.

Заключение. Главной опасностью развития технологий искусственного интеллекта является тот факт, что существует большая вероятность, что ИИ сможет самостоятельно менять алгоритмы действия, а следовательно, выполнять задачи, на которые его не программировали. Соответственно, в данном случае искусственный интеллект будет выступать не инструментом для дискредитации оппонента в предвыборной гонке или выбора военно-политической стратегии страны, а самостоятельным актором МО. Уже на сегодняшний день в связи с быстротой развития информационных технологий правящие элиты не способны эффективно и своевременно реагировать на усиление роли ИИ в мировой политике.

Список источников и литературы:

1. Дипфейк: невинная технология для развлечения или угроза современному обществу?. // Сайт РСМД. [Электронный ресурс] URL: https://russiancouncil.ru/analytics-and-comments/analytics/dipfeyk-nevinnaya-tekhnologiya-dlya-razvlecheniya-ili-ugroza-sovremennomu-obshchestvu/ (дата обращения: 13.10.2024).

2. Искусственный интеллект идет в политику. // Сайт РСМД. [Электронный ресурс] URL: https://russiancouncil.ru/analytics-and-comments/columns/cybercolumn/iskusstvennyy-intellekt-idet-v-politiku/?ysclid=m26o0o86r190545735 (дата обращения: 13.10.2024).

3. Историк рассказал о возможности дипфейков спровоцировать госпереворот. // Сайт Известия. [Электронный ресурс] URL: istorik-rasskazal-o-vozmozhnosti-dipfeikov-sprovotcirovat-gosperevorot (дата обращения: 13.10.2024).

4. Open AI рассказала, как ChatGPT вмешивается в выборы. // Сайт РБК. [Электронный ресурс] URL: https://www.rbc.ru/technology_and_media/10/10/2024/6706ff919a79473eeedd9178?ysclid=m27maapfa9628829177 (дата обращения: 13.10.2024).

5. Singer D. Quantitative International Politics Insights and Evidence. New York: Free Press, 1978.

6. “The Gospel”: how Israel uses AI to select bombing targets in Gaza. // Website The Guardian. [Electronic resource] URL: https://www.theguardian.com/world/2023/dec/01/the-gospel-how-israel-uses-ai-to-select-bombing-targets (date of application: 13.10.2024).

СЕКЦИЯ 6

«ГЛОБАЛЬНЫЕ АСПЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

Анастасия Владимировна Бурнакина,
аспирант Аспирантской школы по праву,
НИУ ВШЭ,
E-mail: aburnakina@hse.ru

Anastasia V. Burnakina,
Ph.D. Candidate, School of Law,
HSE University
E-mail: aburnakina@hse.ru

РОЛЬ ТОРГОВЫХ ПЕРЕГОВОРОВ В РАМКАХ ВТО В ПРЕОДОЛЕНИИ ЦИФРОВОГО НЕРАВЕНСТВА

THE ROLE OF TRADE NEGOTIATIONS UNDER THE WTO IN OVERCOMING DIGITAL INEQUALITY

Аннотация. Настоящее исследование направлено на анализ подходов, выработанных в рамках ВТО и направленных на преодоление цифрового неравенства как части глобального социального неравенства. В частности, обзорно представлена история торговых переговоров по созданию соглашения о цифровой торговле ВТО, проведен анализ предложенного членами ВТО текста такого соглашения, достигнутого в результате переговоров в рамках Совместной инициативы по электронной торговле, даны его достоинства и недостатки с точки зрения имплементации соглашения в договорную структуру ВТО.

Ключевые слова: цифровое неравенство, ВТО, торговые переговоры, совместная инициатива, международное право.

Abstract. This study aims to analyze the approaches developed within the WTO and aimed at overcoming digital inequality as part of global social inequality. In particular, it provides an overview of the history of trade negotiations on the creation of a WTO digital trade agreement, analyzes the text of such an agreement proposed by WTO members and reached as a result of negotiations within the framework of the Joint Statement Initiative on Electronic Commerce, and presents

its advantages and disadvantages in terms of implementation of the agreement in the WTO treaty structure.

Key words: digital inequality, WTO, trade negotiations, joint statement initiative, international law.

Цифровое неравенство, которое воспринимается как часть более широкого социального и экономического неравенства, не является новой концепцией и активно обсуждается в том числе в правовой литературе. Международное право не остается в стороне от решения этой проблемы. Многочисленные глобальные и региональные международные организации, в числе которых Всемирная торговая организация (ВТО) активно вовлечены в эту тематику.

В договорной структуре ВТО до сих пор нет отдельного соглашения, регулирующего цифровую торговлю. Вместе с тем, обсуждения по вопросам электронной коммерции начались в 1998 году с принятием «Рабочей программы по электронной торговле» [1], направленной на изучение торговых вопросов, связанных с глобальной электронной коммерцией, с учетом потребностей развивающихся стран. В 1999 году Совет по торговле услугами представил отчет о прогрессе [2], в котором были обозначены области согласия и ключевые вопросы, требующие дальнейшего обсуждения, такие как охват и классификация электронных сделок. Однако обсуждения по электронной коммерции существенно не продвинулись. Запуск Дохийского раунда сместил внимание к более широким торговым переговорам, и после того, как они были приостановлены в 2008 году, возможности для продвижения вопросов электронной торговли в рамках ВТО также были утрачены [3].

Несмотря на стремительный рост электронной торговли за последние три десятилетия, лишь на 11-й Министерской конференции ВТО в 2017 году была запущена Совместная инициатива по электронной торговле (*англ.*: Joint Statement on Electronic Commerce) [4] для возможного принятия соглашения о

цифровой торговле в рамках ВТО, что привело в 2019 году к началу переговоров [5]. 26 июля 2024 года участники Совместной инициативы после пяти лет переговоров представили финальный текст соглашения [6].

Преамбула соглашения подчеркивает важность сокращения цифрового разрыва и продвижения электронной коммерции как инструмента для улучшения благосостояния бизнеса, потребителей и работников в глобальной экономике, с особым акцентом на поддержку развивающихся и наименее развитых стран. В соглашении также признается необходимость оказания этим странам помощи в виде технической поддержки и наращивания их потенциала для более эффективного внедрения положений соглашения.

Помимо преамбулы, которая в основном затрагивает общие положения и не налагает конкретных юридических обязательств, в соглашении также есть специальная статья 20, посвященная этому вопросу. В ней уточняется, что устранение цифрового разрыва и создание инклюзивной цифровой экономики требует не только установления правил электронной коммерции, но и активной поддержки развивающихся стран. Эта норма подчеркивает важность улучшения доступа этой группы стран к цифровой инфраструктуре и экосистемам, предоставления технической помощи и помощи в наращивании потенциала для выполнения обязательств по соглашению. При этом признается, что таким странам может потребоваться дополнительное время или ресурсы, и развитые страны, а также развивающиеся страны, располагающие соответствующими возможностями, обязуются оказывать необходимую поддержку, исходя из взаимных договоренностей и потребностей этих государств.

На первый взгляд, новое соглашение ВТО по электронной коммерции кажется важным шагом на пути к сокращению цифрового разрыва в рамках международного экономического права. Однако говорить об успехе пока рано. Сложность заключается в правовой архитектуре соглашения – а именно, как оно будет интегрировано в более широкую договорную структуру ВТО [7]. Для формальной интеграции необходимо достичь консенсуса среди всех

членов ВТО [8], что является непростой задачей, учитывая опыт других плюрилатеральных соглашений, таких как Соглашение по содействию инвестициям для развития (*англ.*: Investment Facilitation for Development, IFDA). Хотя текст IFDA был завершен в 2023 году, попытки включить его в ВТО как отдельное соглашение были заблокированы на 13-й Министерской конференции, где Индия и Южная Африка подали официальные возражения, утверждая, что любые переговоры, проводимые за рамками повестки Дохийского раунда, противоречат многостороннему мандату ВТО и не должны осуществляться в рамках Организации [9].

В переговорах по Совместной инициативе по электронной торговле на текущий момент участвует 91 член ВТО, что составляет более половины от общего числа участников. Эти страны обеспечивают более 90 % мирового товарооборота, включая такие крупные экономические силы, как США, Китай и Европейский союз [10]. Однако некоторые крупные развивающиеся экономики, такие как Индия и Южная Африка, наряду с некоторыми развивающимися странами, воздержались от участия, ссылаясь на возражения против плюрилатеральных переговоров. Участие Африки ограничено девятью странами, а среди наименее развитых стран участвуют только пять, что указывает на значительные региональные пробелы, особенно в Карибском бассейне и на Тихоокеанских островах.

Совместные инициативы, такие как данное соглашение, могут принести ощутимую пользу, оживив переговорную функцию ВТО и сделав деятельность организации более актуальной в условиях изменяющейся глобальной торговли [7]. Однако основной проблемой остается вопрос: как включить эти инициативы в правовую структуру ВТО в юридически корректной форме. Предлагаются различные правовые пути, включая внесение поправок в соглашения ВТО, или включение Совместных инициатив через мягкое право, или модификацию графиков обязательств [7]. Политические и правовые дискуссии вокруг этих вопросов сложны, и пока не ясно, повлияют ли различия между соглашениями, такими как IFDA и

Совместная инициатива по электронной торговле, на их исход. Преодоление этих препятствий будет решающим для будущего Совместных инициатив в рамках ВТО.

Список источников и литературы:

1. WTO. The Geneva Ministerial Declaration on Global Electronic Commerce, 20 May 1998. WT/MIN(98)/DEC/2; WTO. Work Programme on Electronic Commerce.1998. WT/L/274;
2. WTO. Work Programme on Electronic Commerce – Progress Report to the General Council, 1999. S/L/74;
3. UNCTAD. Negotiating liberalization of trade in services for development, 2020. P. 15. URL: https://unctad.org/system/files/official-document/ditctncd2019d2_en.pdf. P. 32 (accessed 30.08.2024);
4. WTO. Joint Statement on Electronic Commerce. 2017. WT/MIN (17)/60;
5. WTO. Joint Statement on Electronic Commerce. 2019. W/T/L/1056;
6. WTO. Joint Statement on Electronic Commerce. 2024. INF/ECOM/87;
7. Boklan D., Starshinova O., Amrita B. Joint Statement Initiatives: A Legitimate End to ‘Until Everything Is Agreed’? // Journal of World Trade. 2023. Vol. 57. №. 2. P. 339-360;
8. Adlung R., Mamdouh H. Plurilateral Trade Agreements: An Escape Route for the WTO? // WTO Staff Working Paper ERSD-2017-03. 2017. P. 1-23;
9. Communication of delegations of India and South Africaю The Legal Status of ‘Joint Statement Initiatives’ and Their Negotiated Outcomes. 2021. WT/GC/W/819. Paras 3, 38;
10. WTO. E-commerce. Joint Statement Initiative on E-commerce. URL: https://www.wto.org/english/tratop_e/ecom_e/joint_statement_e.htm#___(accessed 30.08.2024).

Арина Евгеньевна Варламова,
студентка факультета глобальных процессов,
МГУ имени М.В. Ломоносова,
E-mail: vorobyshekarina2019@gmail.com

Arina E. Varlamova,
Student, Faculty of Global Studies,
Lomonosov Moscow State University,
E-mail: vorobyshekarina2019@gmail.com

СОТРУДНИЧЕСТВО РОССИИ И АСЕАН В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. СРАВНЕНИЕ РОССИЙСКОГО И КИТАЙСКОГО ПОДХОДОВ

COOPERATION BETWEEN RUSSIA AND ASEAN IN THE FIELD OF INFORMATION SECURITY. COMPARISON OF THE RUSSIAN AND CHINESE APPROACHES

Аннотация. В настоящей статье рассматривается специфика отношений России и АСЕАН, анализируется взаимодействие сторон в сфере информационной безопасности и ИКТ. Приводится попытка проведения сравнительного анализа внешнеполитических стратегий России и Китая в данной области по отношению к АСЕАН, характеризуются их слабые и сильные стороны. Проведя сопоставление двух подходов, автор делает выводы и оценивает перспективы дальнейшего развития отношений по линии Россия-АСЕАН в области цифровых технологий.

Ключевые слова: Россия, АСЕАН, Китай, кибербезопасность, информационная безопасность, информационно-коммуникационные технологии.

Abstract. This article examines the specifics of relations between Russia and ASEAN, analyses the interaction between the parties in the sphere of information security and ICT. It attempts to carry out a comparative analysis of Russia's and China's foreign policy strategies in this area in relation to ASEAN, characterising

their weak and strong points. By comparing the two approaches, the author draws conclusions and assesses the prospects for further development of Russia-ASEAN relations in the field of digital technologies.

Keywords: Russia, ASEAN, China, cyber security, information security, information and communication technologies.

Динамика сотрудничества России и АСЕАН в области информационной безопасности и информационно-коммуникационных технологий (ИКТ). Эта тема не теряет своей актуальности еще и потому, что масштабы двусторонних взаимоотношений между АСЕАН и Российской Федерацией постепенно набирают обороты, о чем говорит постоянное участие Москвы в работе Восточноазиатского саммита и проведение односторонних переговоров со странами-участницами. Россия активно поддерживает «асеановский» тип построения регионального объединения. В 2023 году Россия выпустила обновленную Концепцию внешней политики, в которой впервые акцентируется внимание на намерении наращивать сотрудничество с АСЕАН [5].

Первые серьезные обсуждения основ сотрудничества в области информационной безопасности и торговли информационными технологиями были начаты в 2013 году при поддержке Центра АСЕАН при МГИМО [4, с. 77]. Уже в 2015 году переговоры получили продолжение и превратились в рабочий план по безопасности и использованию информационно-телекоммуникационных технологий, что предполагало создание специальной рабочей группы и мер по укреплению доверия между ее участниками, а также предотвращение использования ИКТ в террористических целях [2, с. 62].

Россия и АСЕАН смогли выработать широкую договорную базу, состоящую из соглашений и инициатив в сфере ИКТ. Тем не менее, стоит отметить и большой вклад российских ИТ-компаний в торговлю цифровой продукцией. В частности, российская компания «Лаборатория Касперского» открыла офисы в странах странах-членах АСЕАН и активно сотрудничает с

правительственными группами этих стран [6, с. 86-87]. В 2015 году был разработан рабочий план по безопасности и использованию информационно-телекоммуникационных технологий [2, с. 62]. Россия и АСЕАН в 2018 году сделали совместное заявление о «сотрудничестве в области обеспечения безопасности использования информационно-коммуникационных технологий, что стало новой вехой диалоге между двумя акторами [3]. Через 3 года была реализована инициатива Российской Федерации в проведении специальных встреч Диалога Россия-АСЕАН по вопросам, связанным с обеспечением безопасности и ИКТ.

Сравнение китайского и российского подходов по сотрудничеству в области информационной безопасности и ИКТ по линии АСЕАН. Почему китайский подход оказался более эффективным и на основании чего мы можем судить о том, что Россия не является приоритетным партнером стран АСЕАН? Во-первых, практическое сотрудничество Россия-АСЕАН на деле так и не было реализовано. В целом, присутствие товаров российских ИТ-компаний не велико на мировом рынке. В свою очередь, было отмечено, что финансирование ИТ-технологий в России скромно уступает аналогичному в Китае без преувеличения в 100 раз [6, с. 89]. Во-вторых, Китай активно внедряется в проекты стран-членов АСЕАН по цифровому управлению, кибербезопасности и развитию умных городов. Для Китая сотрудничество с АСЕАН является одной из первостепенных задач по успешному продвижению своих геополитических проектов, таких как, например, «Один пояс – один путь», было создано специальное направление Цифрового Шелкового пути Китая, которое прямо заявляет о намерениях Пекина удержать лидирующие позиции в сфере искусственного интеллекта [1, с. 60-62]. Китай углубляет рыночно-ориентированное сотрудничество в сфере цифровых технологий, создает многоуровневые механизмы сотрудничества с законодательной базой. Однако в данном случае АСЕАН ценит сотрудничество с российскими представителями, так как для него важно сохранять внеблоковый статус и оградить себя от возможной зависимости от ресурсов как Китая, так и США.

Поэтому Россия остается важным участником в экономических и политических процессах АСЕАН.

Заключение. Как показывает практика, Россия-АСЕАН на данный момент не стало приоритетным направлением сотрудничества для самого объединения. Необходимо усовершенствовать инструментарий для постоянного сотрудничества, чтобы активизировать взаимодействие и сотрудничество между Россией и странами-членами АСЕАН [7, с. 25-28].

Список источников и литературы:

1. Ван Вэй, Цветов П.Ю., Сотрудничество Китая и России с АСЕАН: основные формы, направления, результаты // Обозреватель − Observer. 2021. № 1 (372). С.56-68.

2. Горян Э.В., Сотрудничество России и АСЕАН в сфере кибербезопасности: промежуточные результаты и перспективы дальнейшего развития // Вопросы безопасности. 2018. № 6. С. 56-70.

3. Заявление Российской Федерации и АСЕАН о сотрудничестве в области обеспечения безопасности использования информационно-коммуникационных технологий и самих информационно-коммуникационных технологий от 14 ноября 2018 года. [Электронный ресурс] URL: http://www.kremlin.ru/supplement/5361 (дата обращения: 16.10.2024)

4. Материалы круглого стола «Общая повестка дня России и АСЕАН в киберпространстве: противодействие глобальным угрозам, укрепление кибербезопасности и развитие сотрудничества» // ИНДЕКС БЕЗОПАСНОСТИ. 2013. № 4 (111), Том 20, С.77-92.

5. Указ Президента РФ от 31 марта 2023 г. № 229 "Об утверждении Концепции внешней политики Российской Федерации". [Электронный ресурс] URL: https://mid.ru/ru/detail-material-page/1860586/ (дата обращения: 15.10.2024)

6. Шкирмонтова Е.А., Шульман В.Д., Возможности и перспективы продвижения российских IT-технологий, искусственного интеллекта и кибербезопасности в страны АСЕАН // Kant. 2022. № 1 (42). С. 83-90.

7. Kanaev Evgeny A. ASEAN-Russia cooperation: the digital dimension // ЮВА: актуальные проблемы развития. 2022. № 3 (56). С. 18-29.

Радмир Радикович Гайнанов,
к.п.н.
E-mail: radmirgaynanov@yandex.ru

Radmir R.Gaynanov,
Ph.D. in Political Science
E-mail: radmirgaynanov@yandex.ru

МЕЖДУНАРОДНОЕ ИЗМЕРЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. СИТУАЦИЯ В ТУРЦИИ И ВОЗМОЖНОСТИ РОССИИ

INTERNATIONAL DIMENSION OF INFORMATION SECURITY. SITUATION IN TÜRKIYE AND RUSSIA'S OPPORTUNITIES

Аннотация. В статье рассматриваются проблемы информационной безопасности Турции, а также возможные шаги России по активизации «кибердипломатии».

Abstract. The article is focusing on problems of the information security of Türkiye as well as possible Russia's moves to enhance her cyberdiplomacy.

Ключевые слова: информационная безопасность, Турция, Россия, кибердипломатия.

Keywords: information security, Türkiye, Russia, cyberdiplomacy

Дайте недругам контроль над провайдером
и они слепят из вас нужное им общество.
Современная кибермудрость

Внимание к вопросам обеспечения информационной безопасности в Турции за последние несколько лет существенно возросло [1]. Продиктовано это не только усложняющимся характером угроз в сфере ИКТ, но и пониманием того, что стране, претендующей на роль одного из влиятельных центров формирующегося многополярного миропорядка, необходимо

развивать собственные цифровые решения, а не полагаться на транснациональные корпорации и ближайших союзников по НАТО. Конечно, в узком смысле кибербезопасности Анкара верна обязательствам по североатлантическому альянсу и соблюдает «блоковую дисциплину». Однако в более широком плане турецкое правительство осознает необходимость достижения цифрового суверенитета, прежде всего, от Запада.

На данном направлении местными властями принимается целый ряд мер: разрабатываются стратегии в области ИКТ, искусственного интеллекта (ИИ) [3] и кибербезопасности с акцентом на наращивание собственных компетенций и потенциала, ведется законотворческая деятельность, инвестируются немалые средства в разработку национального программного обеспечения и компонентной базы, расширяются образовательные программы для подготовки профессиональных кадров и повышения общего уровня цифровой грамотности населения. Хорошим тоном для руководителей министерств и ведомств стало освещение работы возглавляемых ими структур по внедрению современных цифровых технологий, особенно ИИ.

На этом пути у Анкары уже есть свои достижения, которые вполне можно заимствовать в качестве передового опыта (например, система межведомственной координации для быстрого вывода готового продукта на международные рынки, а значит, и оперативной монетизации своих разработок). Впрочем, получается пока не всё. Судя по заявлениям властей, беспокойство у Анкары вызывает ограниченность средств противодействия отрицательному информационному влиянию, которому местные жители регулярно подвергаются через социальные сети и иные популярные онлайн-платформы. Как правило, речь идет о скрытом планомерном навязывании чуждых традиционным исламским ценностям неолиберальных нарративов с задействованием для этого специальных алгоритмов и обученных в нужном ключе нейросетей [2]. В Турции понимают, что если уже сейчас не принять меры по обеспечению своих национальных интересов в этой сфере, то через

одно-два поколения в цивилизационные основы нации будет, говоря языком хакеров, внедрен зловредный код.

Как представляется, Россия с уникальным опытом обеспечения собственной информационной безопасности и с опорой на наш частный сектор могла бы внести свой вклад в дело недопущения киберколониализма и цифрового закабаления, причем не только Турции, но и многих государств мирового большинства. Речь, разумеется, не идет о мессианстве или благотворительности. Здесь требуется здравый расчет с тем, чтобы интересы нашего государства, народа и хозяйствующих субъектов были учтены, а в качестве элементов возможного плана действий российской «кибердипломатии» можно было бы обозначить следующие:

1. Достижение с фокусной страной на политическом уровне договоренностей о развитии сотрудничества, т. к. на фоне антироссийских санкций местным компаниям важно видеть готовность собственного правительства взаимодействовать с Россией.

2. Проведение с участием российских профильных ведомств и представителей сектора выездных «цифровых миссий» в страну назначения.

3. Повышение эффективности горизонтальной координации по линии частный сектор/регионы – ведомства экономического блока – МИД (диппредставительства).

4. Подключение к совместной работе постоянно проживающих в потенциальной стране-партнере и знающих местную специфику росграждан-специалистов в области ИКТ с возможным назначением их представителями крупных российских компаний или ассоциаций.

5. С учетом внедрения ИКТ фактически во все сферы международной жизни востребовано прохождение сотрудниками МИД стажировки по основам функционирования данного сектора. Наступит время, когда для дипломатов, работающих по данному профилю, станет нормой указание в графе «языки» не только условного русского, английского, китайского, арабского и т.п., но и

что-то вроде C++, QASM, Python, MASM. Хорошо бы именно нашей стране стать законодателем моды на этом пути.

Список источников и литературы:

1. National Cybersecurity Strategy 2024-2028. (Adopted on September 6, 2024) Available at: https://www.uab.gov.tr/uploads/pages/siber-guvenligin-yol-haritasi-yerli-ve-milli-tekno/ulusal-siber-guvenlik-stratejisi-2024-2028.pdf (Accessed 10.10.2024).

2. Commission on Digital Media of the Grand National Assembly of Türkiye. Available at: https://www5.tbmm.gov.tr/develop/owa/komisyon_tutanaklari.goruntule?pTutanakId=3309 (Accessed 10.10.2024).

3. National Artificial Intelligence Strategy 2021-2025 (Adopted on August 19, 2021). Available at: https://cbddo.gov.tr/uyzs (Accessed 10.10.2024).

Елена Евгеньевна Гуляева,
к.ю.н., доцент кафедры международного права,
Дипломатическая академия МИД России
E-mail: gulya-eva@yandex.ru

Elena E. Gulyaeva,
Ph.D. in Law, Associate Professor, Department of International Law,
Diplomatic Academy of the Ministry of Foreign Affairs of Russia
E-mail: gulya-eva@yandex.ru

СОВРЕМЕННЫЕ ТЕНДЕНЦИИ РАЗВИТИЯ ЗАКОНОДАТЕЛЬСТВА В ОБЛАСТИ ЗАЩИТЫ ПРАВА НА ИДЕНТИЧНОСТЬ ЛИЧНОСТИ В СВЯЗИ С ЗАРОЖДЕНИЕМ НЕЙРОПРАВА

MODERN TRENDS IN THE DEVELOPMENT OF LEGISLATION IN THE FIELD OF PROTECTING THE RIGHT TO PERSONAL IDENTITY IN CONNECTION WITH THE EMERGENCE OF NEUROLAW

Аннотация. Настоящая статья посвящена рассмотрению вопроса о современных тенденциях развития законодательства в области защиты права на идентичность личности в связи с зарождением нейроправа. В результате исследования автор обращает внимание на то, что во многих Западных странах и странах Латинской Америки активно принимаются нормативно-правовые акты, направленные на защиту персональных данных, конфиденциальности, психической неприкосновенность, когнитивной автономии и необходимости информированного согласия на использование данных о нейронной деятельности мозга человека. Данные нововведения в законодательным акты имеют также важное значение для защиты частной жизни и предотвращения кражи личных данных и киберзапугивания. Право на идентичность личности является одним из основных прав человека и приобрело характер права *erga omnes*, которое не допускает отступлений или приостановления договорных обязательств со стороны любого государства. При этом, следует подчеркнуть

роль правового регулирования при соблюдении баланса прав человека и интересов государства.

Ключевые слова: нейротехнологии, психическая неприкосновенность, когнитивная автономия, erga omnes, права человека, искусственный интеллект, право на идентичность, право на неприкосновенность частной жизни.

Abstract. This article is devoted to consideration of the issue of modern trends in the development of legislation in the field of protecting the right to personal identity in connection with the emergence of neurolaw. As a result of the study, the author draws attention to the fact that many Western countries and Latin American countries are actively adopting regulations aimed at protecting personal data, confidentiality, mental integrity, cognitive autonomy and the need for informed consent for the use of data on the neural activity of the human brain.These legislative changes are also important for protecting privacy and preventing identity theft and cyberbullying.The right to personal identity is a fundamental human right and has acquired the character of an erga omnes right, which does not allow derogation or suspension of treaty obligations on the part of any state. At the same time, it is necessary to emphasize the role of legal regulation while maintaining the balance of human rights and state interests.

Keywords: neurotechnology, mental integrity, cognitive autonomy, erga omnes, human rights, artificial intelligence, right to identity, right to privacy.

Стремительное развитие нейротехнологий требует переосмысления и принятия новых законодательных актов в Западных странах. Сегодня наблюдается зарождение новой отрасли права – нейроправа [3]. В связи с этим проблема идентичности личности выходит на новый уровень. Законодательные органы штатов США принимают законы о защите конфиденциальности умственной деятельности и нейронных данных. Ниже приводится краткое изложение недавних законодательных актов штатов, касающихся нейроправа. Так, Губернатор штата Колорадо одобрил новый

закон, направленный на защиту нейронной активности человека. Новый закон вносит изменения в Закон о конфиденциальности Колорадо (Colorado Privacy Act (CPA) [4, 11], комплексный закон штата о защите персональных данных потребителей. Поправки расширяют существующее определение «конфиденциальных данных» и включают в него «биологические данные» − информацию, полученную в результате анализа биологических, генетических, биохимических, физиологических или нейронных характеристик человека, а также его жизнедеятельности. Биологические данные также включают «нейронные данные» − данные, полученные в результате измерения активности центральной или периферической нервной системы человека, которые можно обрабатывать с помощью специального оборудования или без него. Более того, в законодательное собрание штата Миннесота внесен законопроект, предусматривающий защиту права человека на конфиденциальность умственной деятельности и когнитивную свободу, а также запрет государственным организациям на сбор и транскрибирование нейронных данных без информированного согласия [6, 7]. Законопроект также устанавливает, что правительственные структуры не должны вмешиваться в процесс принятия человеком самостоятельного и осознанного решения в связи с использованием нейротехнологий. Кроме того, законопроект устанавливает, что компания, записывающая и хранящая нейронные данные, в обязательном порядке должна уведомлять и получать согласие на потенциальное использование и распространение нейронных данных [6, 7].

Еще одним примером является Калифорнийский законопроект SB 1223, который устанавливает права потребителей на конфиденциальность, чтобы защитить их нейронные данные от технологий сканирования мозга. Законопроект похож на законопроект Колорадо о нейроправах, поскольку он расширит определение «чувствительные персональные данные», включив в него «нейронные данные» [10, 8]. В Калифорнии в законодательство внесены [10] положения о защите нейроправ. Поправки касаются действующего *Акта о защите прав потребителей*. Изменения происходят в контексте

распространения устройств, накапливающих информацию о мозговой активности. Новый закон в Калифорнии направлен на защиту нейроданных (*информации о мозговой активности, эмоциях, реакциях и предпочтениях человека*), которые теперь официально признаются частью личной информации. Это включает любую информацию, полученную при измерении активности центральной или периферической нервной системы, не основанную на других внешних данных. Закон запрещает компаниям продавать или передавать нейроданные без согласия владельца и обязывает их принимать меры по анонимизации таких данных. Кроме того, пользователи получают право узнать, какие данные собираются, и могут потребовать их удаление.

В теме остаётся много пробелов, например, не регламентирован используемый в тексте нормы термин «*ненейронная информация*», что создает вероятность злоупотребления данными. Ряд исследователей полагают, что требуется расширение понятия нейроданных до более широкого определения, которое будет включать не только данные мозга, но и другие биометрические показатели, такие как сердцебиение или движения глаз, которые также могут раскрывать информацию о психическом состоянии человека.

В дополнение к действиям, предпринятым законодательными органами штатов в США, многие страны Латинской Америки предложили законопроекты или приняли законы, касающиеся нейроправа и конфиденциальности умственной деятельности [9]. Например, в 2021 году президент Чили подписал поправку к конституции, предусматривающую право на жизнь, физическое и психическое здоровье. Новое положение гласит, что «научно-техническое развитие должно быть направлено на благо людей и осуществляться с уважением к жизни, физическому и психическому здоровью». В нем также говорится, что «закон должен регулировать требования, условия и ограничения для его использования на людях и должен особенно защищать, в частности, нейронную деятельность, а также информацию, полученную на ее основе». В Бразилии были внесены два

законопроекта, направленные на защиту конфиденциальности умственной деятельности и нейроправа. Законопроект 29/2023 направлен на внесение поправок в Конституцию Бразилии с целью включения в нее положений о защите ментальной целостности и прозрачности алгоритмов. Предложение было представлено в Сенат в июне 2023 года и находится на рассмотрении до назначения эксперта-докладчика для изучения законопроекта. Законопроект 522/2022 направлен на внесение поправок в бразильский Общий закон о защите данных (LGPD) для регулирования нейронных данных как категории конфиденциальных данных. Законопроект также добавляет новый раздел, регулирующий обработку нейроданных, подчеркивая, что запрос на согласие должен «четко и ясно указывать на возможные физические, когнитивные и эмоциональные последствия» обработки нейроданных. Законопроект был одобрен докладчиком Комиссии по здравоохранению в октябре 2023 года и ожидает дальнейшего рассмотрения [1, 2].

В Мексиканских Соединенных Штатах на рассмотрении находятся два законопроекта о нейроприватности, которые должны внести поправки в Конституцию Мексики. Первый законопроект включает в себя право на психологическую неприкосновенность, а также формулировку, обязывающую Мексику уважать конфиденциальность и неприкосновенность умственной деятельности. Второй законопроект позволит конгрессу принимать федеральное законодательство, связанное с нейроправами. Таким образом, конгресс сможет принимать законы, защищающие психическую неприкосновенность, когнитивную автономию и требующие информированного согласия на использование данных о нейронной деятельности [5, 9].

Список источников и литературы:

1. Законопроект 29/2023 Proposta de Emenda à Constituição n° 29, de 2023. URL: https://www25.senado.leg.br/web/atividade/materias/-/materia/158095 (дата обращения: 20.09.2024).

2. Законопроект 522/2022 в Бразилии. − URL: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2317524 (дата обращения: 20.09.2024).

3. Farinella F., Gulyaeva E.E. Neurorights: Time to Discuss Rights to Mental Privacy and Integrity. *Lex Genetica*. 2024; 3(3):44-61. https://doi.org/10.17803/lexgen-2024-3-3-44-61

4. HOUSE BILL 24-1058. – URL: https://leg.colorado.gov/sites/default/files/2024a_1058_signed.pdf (дата обращения: 20.09.2024).

5. Iniciativa con proyecto de Decreto por la que se adiciona un noveno parrafo y se recorren los subsecuentes del artículo 4°; de la Constitución Política de los Estados Unidos Mexicanos. − URL: http://sil.gobernacion.gob.mx/Archivos/Documentos/2023/08/asun_4588906_20230808_1690903141.pdf (дата обращения: 20.09.2024).

6. Minnesota House Bill 1904 . – URL: https://www.revisor.mn.gov/bills/text.php?number=HF1904&type=bill&version=0&session=ls93&session_year=2023&session_number=0 (дата обращения: 20.09.2024).

7. Minnesota's HF 4522 seeks to protect individuals' neurodata and regulate its collection and use. // URL: https://www.dataguidance.com/news/minnesota-bill-establishing-neurodata-rights-0 (дата обращения: 20.09.2024).

8. Privacy & Data Security Law News. − URL: https://www.bloomberglaw.com/bloomberglawnews/privacy-and-data-security/X7CO1M8G000000?bna_news_filter=privacy-and-data-security#jcite (дата обращения: 20.09.2024).

9. Privacy and the Rise of “Neurorights” in Latin America. URL: https://fpf.org/blog/privacy-and-the-rise-of-neurorights-in-latin-america/ (дата обращения: 20.09.2024).

10. SB-1223 Consumer privacy: sensitive personal information: neural data. – URL: https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=202320240SB1223 (дата обращения: 20.09.2024)

11. Your Brain Waves Are Up for Sale. A New Law Wants to Change That. // The New York Times. – URL: https://www.nytimes.com/2024/04/17/science/colorado-brain-data-privacy.html i. (дата обращения: 20.09.2024).

Артем Михайлович Жбанов,
Аспирант, кафедра международных отношений и интеграционных процессов факультета политологии,
МГУ им. М.В. Ломоносова,
E-mail: norvejsky@gmail.com

Artem M. Zhbanov,
Postgraduate researcher, Department of International Relations and Integration Processes, Faculty of Political Science,
Lomonosov Moscow State University,
E-mail: norvejsky@gmail.com

ТЕНДЕНЦИИ ПОЛИТИКИ КЛЮЧЕВЫХ АКТОРОВ МЕЖДУНАРОДНОЙ СИСТЕМЫ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И РЕГУЛИРОВАНИЯ ИНТЕРНЕТА

CYBERSECURITY POLICY AND INTERNET REGULATION TRENDS OF MAJOR POWERS AND KEY ACTORS IN INTERNATIONAL SYSTEM

Аннотация: В исследовании рассмотрены тенденции ключевых акторов международной системы в области информационной безопасности и регулирования интернета. Отдельное внимание уделяется проблеме милитаризации интернета и аспектам предотвращения вмешательства во внутренние дела государств посредством интернет-технологий.

Abstract: The study examines the trends of the key actors of the international system in the realm of information security and Internet regulation. Article focuses on the problem of the militarization of the internet and aspects of preventing interference in the internal affairs of states through internet technologies.

Ключевые слова: информационная безопасность, кибербезопасность, цифровой суверенитет, международная информационная безопасность, регулирование интернета, национальный сегмент сети интернет.

Keywords: information security, cybersecurity, digital sovereignty, international information security, Internet regulation, national internet network.

Анализ тенденций политики ключевых акторов международной системы в области информационной безопасности и регулирования интернета осуществляется на основе критериев, выявленных в качестве значимых факторов и атрибутов национальных политик в области информационной безопасности. Анализ политики кибербезопасности США и Китая позволяют выделить тенденции общего вектора движения государств в отношении регулирования сети интернет, которые имеют схожие характеристики, но также обусловлены спецификой положения государств в международной системе и особенностями политических режимов государств. Общие для большинства самостоятельных акторов международной системы тенденции представлены формированием политики, направленной на создание конкурентной технологической базы и развитие человеческого капитала в целях осуществления как можно большего контроля сети интернет как в пределах национальных границ, так и за рубежом. Контроль также осуществляется постепенным формированием соответствующей нормативно-правовой базы и законодательных рамок, позволяющих регулировать действия в сети. В подтверждение данной гипотезы выступает всё более активное ужесточение законодательства и усиление контроля за возможным иностранным вмешательством во внутренние дела государств, которое сопровождает теперь, пожалуй, все избирательные кампании в США, Российской Федерации и странах Европейского Союза и других странах. Предыдущие этапы укрепления власти государств в сети интернет сопровождались постепенным формированием регулирующей законодательной базы в отношении операторов связи и данных их клиентов, а также постепенным формированием специализированных подразделений правоохранительных органов, направленных на предотвращение правонарушений в интернете. По мере расширения академических исследований в области возможности использования интернета и ИКТ-среды (киберпространства) в качестве потенциального пространства реализации национальных интересов, а также осознания потенциала использования

интернет-инструментов для воздействия на общественное мнение, государства стали укреплять национальную экспертизу в области информационной работы с населением собственных и зарубежных стран, формировать национальные подразделения специальных служб и вооруженных сил для проведения информационных операций и операций вмешательства в национальные сети государств-соперников. Параллельно шел процесс усиления национального законодательства и надзорных и регулирующих органов для предотвращения подобной активности иностранных государств. По мере развития интернет-технологий и сервисов гражданского пользования, всё большее значение приобрел контроль за мировыми потоками данных, который определяется через доминирующее положение ИТ-корпораций на рынках данных. Крупные международные акторы, обладающие самостоятельными решениями в области программного обеспечения, социальных сетей, интернет-технологий и сервисов, представленных национальными ИТ-компаниями используют проблемы цифрового и технологического неравенства малых государств, приобретая на них огромное влияние посредством монополии цифровых сервисов и технологического доминирования. Ряд процессов данного направления можно отнести к процессам гибридного противостояния государств. При этом, на текущий момент аспекты применения отдельных инструментов гибридного противостояния в ИКТ-среде никак не регулируются международным законодательством, а использование трансграничных сервисов по работе с сетью интернет, таких как социальные сети, браузеры для поиска информации, видеохостинги и т.д. позволяют проводить информационные операции на конкретную аудиторию без правовых последствий. Особенности уклада современного рынка программного обеспечения и интернет-сервисов практически ограничивают страны, способные обладать существенным преимуществом в реализации инструментов гибридного противостояния в информационной сфере и киберпространстве до нескольких единиц. Отсутствие возможностей контроля за информацией и невозможность

ограничения доступа к ряду социальных сетей без проведения политики ограничений или использования широкой системы фильтрации сети Интернет по аналогии с китайской моделью «Золотой щит» [1, с.91] является проблемой реализации суверенитета в киберпространстве. Для обозначения возможностей государств контролировать информацию в интернете, обладать технологическим потенциалом для осуществления независимой политики в рамках сетей в собственной юрисдикции в академическом сообществе, а также на уровне принимающих решения лиц применяется термин «цифровой суверенитет». Концепция «цифрового суверенитета» является иерархически взаимосвязанной с общей концепцией суверенитета. На текущий момент в академическом сообществе нет однозначной позиции относительно концепции суверенитета, среди исследователей ведутся споры относительно содержания и наполнения термина [2]. Традиционным для реалистской школы международных отношений является определение суверенитета как независимости проведения политики государства по отношению к другим государствам (внешний суверенитет), а также верховную и исключительную власть государства над процессами и полномочиями на своей территории (внутренний суверенитет). По мнению ряда авторов, преимущественно представителей неолиберальной школы международных отношений, с увеличением роли транснациональных корпораций и негосударственных акторов международной политики традиционная вестфальская концепция суверенитета более неприменима в отношении международных отношений. Данный подход к суверенитету присутствует в работах Д.Ная, Р.Кохейна [4], Д.Слотера [3]. Противоречивой является и природа цифрового суверенитета, относительно которой в научном сообществе нет единого подхода. Концепция цифрового суверенитета берет начало с 1996 года, в котором ряд западных исследователей рассмотрели проблемы имплементации права в рамках киберпространства. Д.Джонсон и Д.Пост рассматривают проблему отсутствия и практической сложности определения национальных границ и границ применения законодательства в рамках киберпространства [5]. Вопросы

правоприменения и работы судебной власти в отношении правонарушений в киберпространстве также получили освещение в статье Р.В. Свита, Д. Эвана Ван Хука и Э.В. Дилелло [6]. В это же время политический активист либертарианских взглядов из США Д.Барлоу публикует резонансный материал «декларации независимости киберпространства», в котором отмечает, что киберпространство является местом, на которое не распространяется концепция суверенитета и отдельных положений законодательства [7]. Впоследствии, с развитием государственных механизмов контроля за нежелательной и опасной для государственной безопасности информации в интернете, а также активным созданием инструментов киберразведки вопрос цифрового суверенитета и реализации государственной власти в киберпространстве получил новое измерение.

Мнения современных исследователей в отношении цифрового суверенитета разделились: ряд авторов рассматривают цифровой суверенитет лишь как онлайн-версию принципа суверенитета, которая распространяется исключительно на вопросы контроля информации в интернете и телекоммуникационных сетях. Содержание данного термина совпадает с понятием «информационный суверенитет». Расширенное понимание цифрового суверенитета в данной оптике рассматривает его как новую версию классического понятия суверенитета, адаптированную к новому цифровому пространству. По мнению китайских исследователей Л.Хуэй и Я.Син, проблемой распространения суверенитета в киберпространстве является сложность восприятия того, где именно располагаются национальные границы в виртуальном мире, в котором границы сети невидимы, а пространственный охват неясен [8]. Кроме того, сама возможность обеспечения цифрового суверенитета в сети предполагает наличие технических возможностей у государства для реализации данного суверенитета. Помимо этого, государство должно иметь возможность развивать технологии по реализации контроля, поскольку пространство сети постоянно расширяется и приобретает новые сервисы, приложения, домены и

принципы связи. Этот аспект рассматривается другой группой авторов, которая делает акцент на вопросах реализации цифрового суверенитета через обладание полностью самостоятельной и автономной технологической базой для обеспечения суверенитета в киберпространстве. По мнению С.В. Володенкова «цифровой суверенитет одновременно включает в себя две ключевые компоненты: возможность независимого применения цифровых технологий в собственных интересах и способность их использования», которое включает в себя защиту цифрового пространства государства и граждан от негативных информационных воздействий [9].

В связи с ростом возможностей информационных технологий, содержание концепции цифрового суверенитета постоянно меняется и корректируется. На сегодняшний день цифровой суверенитет является заключительным этапом в эволюции концепции суверенитета. Проблемы цифрового суверенитета тесно пересекаются с вопросами как правового регулирования, так и технологических компетенций, которыми обладает государство. Вопросы международной безопасности в условиях возрастающей напряженности международной системы напрямую связаны с проблемой реализации цифрового суверенитета. С развитием возможностей применения киберинструментов для реализации национальных интересов, а также применения силы в отношении потенциального противника, современность ставит точку в представлении интернета как глобальной сети, в которой нет государственных границ, распространенном в 1990-ых годах. В целях осуществления межгосударственного взаимодействия и создания базовой категории для реализации ряда международных соглашений по регулированию киберпространства Российская Федерации использует категорию «национальный сегмент сети Интернет» и неоднократно предлагала ее в качестве основы для формирования системы международной информационной безопасности. Термин, в частности, использовался в ряде инициатив российской стороны по созданию базовых понятий для формирования системы международной безопасности в конвенции ООН,

которые не были в итоге приняты, в частности, в концепции конвенции 2017 года и 2023 года. Основная цель этих инициатив заключалась в формировании правовых основ для международного управления интернет-пространством, которое бы соответствовало интересам государства и обеспечивало его суверенитет в ИКТ-среде. Согласно определению, используемому в концепции конвенции 2017 года, национальный сегмент сети Интернет является совокупностью информационно-коммуникационных сетей, систем, ресурсов сети Интернет, размещённых на территории государства и зарегистрированных в установленном порядке в соответствии с внутренним законодательством данного государства, и национальной доменной зоны, а также ресурсов, отнесённых к национальным сегментам государств в рамках соответствующих международных договоров [10]. Современные глобальные тенденции политики кибербезопасности характеризуются увеличением контроля государств над национальными сегментами киберпространства. Как видно из политики государств, стремящихся достичь максимально возможного уровня цифрового суверенитета, в данных целях используются такие практики как цифровой протекционизм, представленный барьерами для иностранных цифровых сервисов и компаний, включающий в себя требования к локализации, ограничения на трансграничную передачу данных, фильтрации, блокировки, интернет-цензуру, ограничения в отношении электронных платежных систем или методов шифрования, а также принудительную передачу технологий или ключей шифрования в интересах национальной безопасности. По мере дальнейшего роста экономик стран, занимающих вторые и третьи роли в международной системе, предполагается, что они также будут использовать цифровой протекционизм для уменьшения возможности иностранного влияния на свои общественные и политические процессы в интернете. Указанные тенденции отражают логику процесса деглобализации и постепенного снижения влияния США в международной системе. В долгосрочной перспективе прогнозируется обособление глобальных цифровых макрорегионов, аналогичных существующим

экономическим макрорегионам, при этом «границы» цифрового пространства будут определяться цивилизационными связями между государствами и уровнем их экономической интеграции.

С учетом текущих тенденций в развитии интернета и телекоммуникационных технологий, а также постепенного перехода к интернету четвертого поколения, или Web 4.0, основанному на новых принципах скорости передачи данных, искусственном интеллекте и, прежде всего, технологии «интернета вещей», возникает необходимость в повышенных требованиях к безопасности и полной прозрачности сети для контролирующих органов, правоохранительных структур и специальных служб. Углубленная интеграция производственных процессов и информационного обеспечения объектов критической инфраструктуры, также дальнейшее расширение человеко-машинного взаимодействия подчеркивают, что риски потенциальных кибератак и деструктивных действий со стороны злоумышленников становятся крайне высокими. Речь идет не только о экономических потерях, но и о физической безопасности значительного числа граждан.

Учитывая вышеперечисленное, можно констатировать, что общие для ключевых акторов международной системы тенденции в области информационной безопасности и регулирования интернета можно обобщить в следующих положениях:

- увеличение государственного контроля за пользователями интернета в пределах национальных границ;

- расширение государственного сотрудничества с частным сектором в вопросах предоставления данных, а также информационной политики в рамках платформ, сервисов и социальных сетей в интернете;

- расширение возможностей вооруженных сил и национальных разведок в области военного и разведывательного использования сети интернет;

- расширение требований по защите данных и безопасности операторов данных и частный сектор в целях обеспечения защиты критической

инфраструктуры и чувствительных гражданских отраслей, которые будут всё больше сталкиваться с возможным влиянием и кибератаками извне.

Заключение. Выявленные тенденции становятся особенно актуальными в условиях роста международной напряженности, милитаризации интернет-технологий, а также стремительного развития технологий искусственного интеллекта, которые, с высокой долей вероятности, станут определяющими в повестке информационной безопасности и регулирования интернета в ближайшее десятилетие.

Список источников и литературы:

1. Goldsmith, Jack L.; Wu, Tim (2006). Who Controls the Internet?: Illusions of a Borderless World. New York: Oxford University Press. p. 91. ISBN 0-19-515266

2. Соловьев Э. Суверенитет в XXI веке // РСМД, 2012. URL: https://russiancouncil.ru/analytics-and-comments/analytics/suverenitet-v-xxi-veke/ (Дата обращения 16.10.24)

3. Slaughter A.-M. A New World Order. Princeton and Oxford: Princeton University Press, 2004. P. 267.

4. Най Дж. мл. и Кохэйн Р. О Транснациональные отношения и мировая политика./ Теория международных отношений: Хрестоматия// Сост. и науч. Редактор П.А. Цыганков: М, 2003 стр. 147-152

5. Johnson, D. R., & Post, D. Law and Borders: The Rise of Law in Cyberspace // Stanford Law Review, 48, 1996

6. Robert W. Sweet, D. Evan van Hook, and Edward V. Di Lello, Towards a Common Law of Sentencing: Developing Judicial Precedent in Cyberspace , 65 Fordham L. Rev. 927 1996. URL: https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=3319&context=flr (Дата обращения 17.10.24)

7. Barlow, J. P. Declaration of the Independence of Cyberspace. 1996 URL: https://www.eff.org/cyberspace-independence (Дата обращения 17.10.24)

8. Li, H., Yang, X. Sovereignty and Network Sovereignty. In: Co-governed Sovereignty Network. Springer, Singapore 2021

9. Володенков С.В. Феномен цифрового суверенитета современного государства в условиях глобальных технологических трансформаций: содержание и особенности // Журнал политических исследований. 2020. № 4. С. 3–11.

10. Как Россия предлагает ООН обезопасить интернет // ТАСС 01.11.2017 URL: https://tass.ru/ekonomika/4672302 (Дата обращения 17.10.24)

Павел Александрович Карасев,
к.полит.н.,с.н.с.,
Национальный исследовательский институт мировой экономики
и международных отношений имени Е. М. Примакова
Российской академии наук,
E-mail: karpaul@iisi.msu.ru

Pavel A. Karasev,
Ph.D. in Political Science, Senior Researcher,
Primakov National Research Institute
of World Economy and International Relations
Russian Academy of Sciences,
E-mail: karpaul@iisi.msu.ru

УПРАВЛЕНИЕ ИНТЕРНЕТОМ В КОНТЕКСТЕ ГЛОБАЛЬНОГО ЦИФРОВОГО ДОГОВОРА

INTERNET GOVERNANCE IN THE CONTEXT OF GLOBAL DIGITAL COMPACT

Аннотация. Глобальный цифровой договор направлен на решение задач, связанных со старыми и новыми вызовами массового освоения ИКТ-среды, в том числе управлением Интернетом. На фоне существования различных взглядов на развитие глобальной сети необходимо рассмотреть, что предлагает ГЦД, и может ли он способствовать интернационализации управления Интернетом.

Ключевые слова: международная информационная безопасность, управление Интернетом, Пакт во имя будущего, Глобальный цифровой договор.

Abstract. The Global Digital Compact aims to address the old and new challenges of mass use of the ICT-environment, including Internet governance. Given the different views on the development of the global network, it is necessary to consider what the GDC offers and whether it can contribute to internationalization of Internet governance.

Key words: international information security, Internet governance, Pact for the Future, Global Digital Compact.

В сентябре 2024 г. на Саммите будущего Генеральная Ассамблея ООН приняла резолюцию, содержащую «Пакт во имя будущего» и приложения к нему, в том числе Глобальный цифровой договор (ГЦД) [7]. В сущности, Пакт созвучен таким инициативам, как Цели развития тысячелетия 2001 г. [9] и Цели устойчивого развития 2015 г. [8], и во многом развивает их положения. В то же время, Россия дистанцировалась от консенсуса по этому документу и его приложениям, поскольку их подготовка проходила вразрез с согласованными процедурами, и нормальной переговорной работы не велось [1].

Глобальный цифровой договор рассматривает большой спектр задач, связанных со старыми и новыми вызовами массового освоения ИКТ-среды, в том числе регулированием искусственного интеллекта, преодолением цифрового разрыва, расширением возможностей участия в цифровой экономике, развитием подходов к управлению данными. В рамках задачи по формированию инклюзивного, открытого, безопасного и защищенного цифрового пространства рассматривается и проблема управления Интернетом. В контексте центробежных тенденций развития глобальной информационной инфраструктуры, которые можно наблюдать последние несколько лет, и существования различных подходов к этому вопросу, таких, как американская «Декларация о будущем Интернета» и предложенная Китаем концепция сообщества единой судьбы в киберпространстве [3], представляется немаловажным рассмотреть, какой вектор развития задается ГЦД, и сделать соответствующие выводы.

На данный момент значительная часть функций по управлению Интернетом осуществляется Международной корпорацией по распределению номеров и имён (ICANN), созданной в 1998 г. Несмотря на формально некоммерческий, неправительственный статус этой структуры, до 2016 г. правительство США напрямую участвовало в её работе через меморандум о взаимопонимании между ICANN и Министерством торговли США [11]. Впоследствии и по сей день этот контроль сохраняется опосредованно – через

широкое участие в её управляющих структурах заинтересованных сторон с западноцентричным взглядом на развитие глобальной сети. Правительственный консультативный комитет, который должен предоставить право голоса государствам, на деле обеспечивает только номинальное участие представителей стран, так как, в соответствии с его принципами работы, он не является органом принятия решений и не имеет полномочий действовать от имени ICANN [6, принцип 2].

Противоречивость ГЦД начинается со «сквозных и взаимоукрепляющих» принципов, на которых строится этот документ. С одной стороны, указано, что «всеохватное участие всех государств и других заинтересованных сторон является краеугольным камнем» договора [7, прил. I, п.8(a)]. С другой – что «участие правительств… *в рамках их соответствующих функций и обязанностей*[10], существенно необходимо для продвижения навстречу всеохватному, открытому, безопасному и защищенному цифровому будущему» [там же, п.8(k)]. Этот тезис дублируется в подразделе «Регулирование Интернета», где признается, что оно «должно оставаться по своей природе глобальным и учитывающим интересы многих заинтересованных сторон и должно осуществляться при полноценном участии правительств… *согласно их соответствующим функциями и обязанностями*» [там же, п.27].

Пункт 28 ГЦД говорит о важности Форума по вопросам управления Интернетом как основной многосторонней платформы для обсуждения вопросов регулирования Интернета [там же, п.28], а пункт 68 утверждает, что для содействия осуществлению ГЦД страны будут «опираться на процессы и форумы, созданные по итогам Всемирной встречи на высшем уровне по вопросам информационного общества, в частности на Форум по вопросам управления Интернетом и его национальные и региональные инициативы, а также на Форум ВВУИО» [там же, п.68]. В то же время, на официальном сайте

[10] Здесь и далее курсив автора.

Форума ООН по управлению Интернетом (IGF) указано, что он способствует обсуждению вопросов государственной политики в отношении Интернета, но при этом не вырабатывает согласованных результатов, а только «информирует и вдохновляет тех, кто обладает полномочиями по формированию политики, как в государственном, так и в частном секторе [5].

Таким образом, совокупность положений ГЦД закрепляет за государствами их роль в рамках соответствующих функций и обязанностей, которые фактически не выходят за пределы национальных границ, и объявляет удовлетворенность текущей системой, которая строится вокруг ICANN. Важно отметить, что это противоречит другим основам, упомянутым в ГЦД. Так, говорится, что регулирование Интернета следует по-прежнему осуществлять в соответствии с положениями итоговых документов встреч на высшем уровне (ВВУИО), проведенных в Женеве и Тунисе [7, прил. I, п.27]. Однако, если обратиться к «Тунисской программе для информационного общества», можно обнаружить пункт, который гласит, что «организация использования Интернет на международном уровне должна иметь многосторонний, прозрачный и демократический характер *при полном участии правительств*, частного сектора, гражданского общества и международных организаций» [10, п.29]. Процесс управления глобальной сетью, как единым целым, должен находиться в руках мирового сообщества, а не в руках одного государства.

Очевидно, что по итогам ВВУИО была сформирована в целом позитивная программа, предусматривавшая участие всех сторон, а также намечены соответствующие практические шаги, значимая часть которых, тем не менее, не была в полной мере реализована. Рассмотрение положений ГЦД позволяет сделать неутешительный вывод – заявляя о роли государств, его составители, напротив, фиксируют существующую систему, в которой государства, по сути, отстранены от международного управления Интернетом, и не предложены альтернативные пути развития. Более того, поощрение международного сотрудничества между всеми заинтересованными сторонами

«в интересах своевременного предупреждения, выявления и устранения рисков фрагментации Интернета» [7, прил. I, п.29(c)] можно рассматривать как превентивную меру против появления подобных альтернатив.

В этом контексте весьма показательны тезисы, которые содержаться в Казанской декларации БРИКС 2024 г.[4] Страны признали, «что устойчивая, безопасная, инклюзивная и интероперабельная общественная цифровая инфраструктура способна обеспечить масштабное предоставление услуг и расширить социально- экономические возможности для всех», а также заявили «о своей поддержке работы Института БРИКС по изучению сетей будущего» и отметили «продолжающиеся усилия Целевой группы по созданию платформы БРИКС по цифровым общественным благам». Представляется, что в случае отсутствия прогресса по интернационализации текущей модели управления Интернетом, БРИКС обладает достаточным потенциалом для создания и продвижения собственной значимой альтернативы, которая будет отражать дух объединения, в основе которого взаимоуважение и взаимопонимание, суверенное равенство, солидарность, демократия, открытость, инклюзивность, взаимодействие и консенсус.

Список источников и литературы:

1. В МИД рассказали о нарушениях при принятии «Пакта будущего» // РИА новости [Официальный сайт] https://ria.ru/20240926/pakt_buduschego-1974747339.html (Дата обращения 17.10.24)

2. Доклад рабочей группы по управлению Интернетом // Working Group on Internet Governance [Official website] Систем. требования: Microsoft Word URL: http://www.wgig.org/docs/WGIGReport-Russian.doc (Дата обращения 17.10.24)

3. *Карасев П. А.* Управление интернетом – тенденции и перспективы // International Journal of Open Information Technologies. − 2023. − Т. 11, № 9. − С. 59–65.

4. Казанская декларация // Председательство Российской Федерации в объединении БРИКС в 2024 году [Официальный сайт] URL: https://cdn.brics-

russia2024.ru/upload/docs/Казанская_декларация.pdf (Дата обращения 17.10.24)

5. О нас // Форум по управлению Интернетом (IGF) [Официальный сайт] URL: https://www.intgovforum.org/ru/about (Дата обращения 17.10.24)

6. Принципы работы Правительственного консультативного комитета (GAC) // ICANN [Официальный сайт] URL:https://gac.icann.org/operating-principles/operating-principles (Дата обращения 17.10.24)

7. Резолюция, принятая Генеральной Ассамблеей 22 сентября 2024 года 79/1. Пакт во имя будущего // ООН [Официальный сайт] URL: https://documents.un.org/doc/undoc/gen/n24/272/24/pdf/n2427224.pdf (Дата обращения 17.10.24)

8. Резолюция, принятая Генеральной Ассамблеей 25 сентября 2015 года 70/1. Преобразование нашего мира: Повестка дня в области устойчивого развития на период до 2030 года // ООН [Официальный сайт] URL: https://documents.un.org/doc/undoc/gen/n15/291/92/pdf/n1529192.pdf (Дата обращения 17.10.24)

9. Резолюция, принятая Генеральной Ассамблеей 8 сентября 2000 года 55/2. Декларация тысячелетия ООН // ООН [Официальный сайт] URL: https://www.un.org/ru/documents/decl_conv/declarations/summitdecl.shtml (Дата обращения 17.10.24)

10. Тунисская программа для информационного общества // ООН [Официальный сайт] URL: https://www.un.org/ru/events/pastevents/pdf/agenda_wsis.pdf (Дата обращения 17.10.24)

11. Memorandum of Understanding between the U.S. Department of Commerce and Internet Corporation for Assigned Names and Numbers // ICANN [Official website] URL: https://www.icann.org/resources/unthemed-pages/icann-mou-1998-11-25-en (Дата обращения 17.10.24).

Анастасия Михайловна Кучина,
к.ю.н., преподаватель кафедры международного права,
Дипломатическая академия МИД России,
E-mail: anastasia.kuchina@mail.ru

Anastasia M. Kuchina,
Ph.D. in Law, Lecturer, Department of International Law,
Diplomatic Academy of the Russian Ministry of Foreign Affairs,
E-mail: anastasia.kuchina@mail.ru

ЦИФРОВАЯ СОЛИДАРНОСТЬ И ЦИФРОВОЙ СУВЕРЕНИТЕТ В КОНТЕКСТЕ РАЗВИТИЯ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

DIGITAL SOLIDARITY AND DIGITAL SOVEREIGNTY IN THE CONTEXT OF THE DEVELOPMENT OF INTERNATIONAL INFORMATION SECURITY

Аннотация. Настоящее исследование посвящено анализу двух конкурирующих между собой концепций в сфере информационной безопасности: цифровой солидарности и цифрового суверенитета. Определены ключевые компоненты, основные различия, а также влияние на национальные и международные стратегии обеспечения кибербезопасности указанных подходов в условиях современной геополитической обстановки.

Ключевые слова: цифровая солидарность, цифровой суверенитет, кибербезопасность, информационная безопасность, международное сотрудничество, проект конвенции ООН против киберпреступности.

Abstract. The present article focuses on the analysis of two competing with each other concepts in the field of information security: digital solidarity and digital sovereignty. The key components, main differences and the impact of these approaches on national and international strategies for ensuring cybersecurity in the current geopolitical environment are identified.

Keywords: digital solidarity, digital sovereignty, cybersecurity, information security, international cooperation, Draft United Nations convention against cybercrime.

Понятия цифрового суверенитета и цифровой солидарности. Значимость «цифрового» или «информационного» суверенитета обуславливается тем, что от уровня цифровизации, влияющей на ключевые сферы жизнедеятельности государства, в частности, экономику, технологии, общественные и международные отношения, зависят и статус государства на международной арене, и его внешнеполитические возможности.

Цифровой суверенитет понимается как право государства определять свою информационную политику самостоятельно, распоряжаться инфраструктурой, ресурсами, обеспечивать информационную безопасность. [2] Наиболее «популярным» признаком цифрового суверенитета стало право на независимое управление цифровыми ресурсами, действующими в национальных сегментах цифрового пространства. Такого рода право предполагает возможности регулирования, надзора и контроля за деятельностью цифровых платформ, а также блокировки размещаемой на них информации уполномоченными на это государством органами и организациями [5].

Нет причин, по которым принцип суверенитета не должен применяться в киберконтексте также как он применяется в любой другой сфере деятельности государства, как это признала Группа правительственных экспертов ООН в своих докладах за 2013 г. [9] и 2015 г. [10]

6 мая 2024 года во время Конференции RSA в Сан-Франциско (штат Калифорния) Государственный департамент США представил Стратегию Соединенных Штатов в области международного киберпространства и цифровой политики: на пути к инновационному, безопасному и уважающему права цифровому будущему [6], которая основана на концепции цифровой солидарности. *Цифровая солидарность* предполагает тесное сотрудничество

с международными партнерами, частным сектором, развивающимися экономиками для согласования нормативных актов, обмена передовым опытом, совместного реагирования на кибератаки, обеспечения открытой и независимой исследовательской среды.

Коллизия двух концепций. Приверженцы концепции цифровой солидарности полагают, что, отдавая предпочтение национальному контролю, государства могут оказаться изолированными в своих усилиях по борьбе с киберугрозами, что может облегчить осуществление безнаказанных кибератак злоумышленниками [12].

Вместе с тем в настоящее время увеличиваются случаи несанкционированного вторжения в информационное пространство государств другими государствами и негосударственными субъектами.

Подобная ситуация способствует дестабилизации международной безопасности, усиливая взаимное недоверие государств и подталкивая их к односторонним действиям в информационной сфере, что, в свою очередь, актуализирует необходимость международного сотрудничества в области информационной безопасности, основанного на принципах уважения государственного суверенитета [4].

Более того, доктрина цифровой солидарности, в которой подчеркивается технологическое сотрудничество США с их союзниками и провозглашается идея глобального свободного подключения, в противовес понятию цифрового суверенитета, в то же время блокирует возможности для подлинного сотрудничества с геополитическими соперниками.

Вопросы практического международного сотрудничества в области информационной безопасности. Взаимовыгодное международное партнерство государств в области кибербезопасности, включающее элементы цифровой солидарности, наблюдается в практике региональных объединений. В Европейском союзе завершена процедура предварительного согласования законопроекта о киберсолидарности [3]. В рамках БРИКС осуществляется взаимодействие по таким приоритетным направлениям, основанным на

уважении государственного суверенитета, как: развитие цифровой инфраструктуры и передовых отраслей, включая коммуникации, облачные вычисления, искусственный интеллект и т.д., а также сотрудничество в борьбе с терроризмом и экстремизмом в цифровом пространстве [11], принципы которого были заложены в Антитеррористической стратегии БРИКС, принятой в 2020 году [1].

Тем не менее, инициативы в области сотрудничества по вопросам международной информационной безопасности не ограничиваются их региональной повесткой. Так, специальный межправительственный комитет Организации Объединенных Наций 7 августа 2024 года принял проект Конвенции ООН против киберпреступности [8], инициированный Российской Федерацией в 2021 году [7], однако отличающийся от первоначально предложенного более узким охватом распространения (криминализированы только 10 видов нарушений из 23 предложенных). Несмотря на тот факт, что принятый на основании консенсуса проект новой конвенции не достигает желаемого в полной мере, данная конвенция претендует на статус первого международного договора универсального характера в области информационной безопасности.

Заключение. Новые геополитические вызовы влияют на эффективность межгосударственного сотрудничества в сфере кибербезопасности. Необходимо подчеркнуть, что обеспечение цифрового суверенитета и сотрудничество в области международной информационной безопасности не противоречат, а дополняют друг друга. Стандартизация мер защиты и обмен опытом в рамках региональных и глобальных международных организаций сказываются на эффективности и повышают уровень информационной безопасности, которая, в свою очередь, является неотъемлемой частью цифрового суверенитета.

Принципы, заложенные в концепцию цифровой солидарности, могут выступать в качестве ориентира для дальнейшего сотрудничества по вопросам международной информационной безопасности, при этом не умаляя

суверенных прав государств и ориентируясь на осуществление деполитизации процессов развития отрасли информационных технологий.

Список источников и литературы:

1. Антитеррористическая стратегия БРИКС за 2020 год [Электронный ресурс]. – URL: https://brics-russia2020.ru/images/114/81/1148163.pdf (дата обращения – 01.10.2024).

2. Бухарин В.В. Компоненты цифрового суверенитета Российской Федерации как техническая основа информационной безопасности [Текст] / В.В. Бухарин // Вестник МГИМО-Университета. – 2016. – № 6 (51). – С. 76-91.

3. Законодатели ЕС предварительно согласовали положения законопроекта о киберсолидарности [Электронный ресурс]. – URL: https://d-russia.ru/zakonodateli-es-predvaritelno-soglasovali-polozhenija-zakonoproekta-o-kibersolidarnosti.html (дата обращения – 16.09.2024).

4. Зиновьева Е. С. Цифровой суверенитет в практике международных отношений / Е. С. Зиновьева, С. В. Шитьков // Международная жизнь. – 2023. – № 3. – С. 38-51. – EDN HBTQYT.

5. Никонов В.В., Воронов А.С., Сажина В.А., Володенков С.В., Рыбакова М.В. Цифровой суверенитет современного государства: содержание и структурные компоненты (по материалам экспертного исследования) // Вестн. Том. гос. ун-та. Философия. Социология. Политология. – 2021. – № 60. – С. 206-216.

6. Обнародование Стратегии США в области международного киберпространства и цифровой политики [Электронный ресурс]. – URL: https://ru.usembassy.gov/ru/release-of-united-states-international-cyberspace-and-digital-policy-strategy-ru/ (дата обращения – 18.09.2024).

7. О внесении в Спецкомитет ООН российского проекта универсальной международной конвенции по противодействию использованию информационно-коммуникационных технологий в преступных целях [Электронный ресурс]. – URL:

https://archive.mid.ru/foreign_policy/news/-/asset_publisher/cKNonkJE02Bw/content/id/4831832 (дата обращения – 01.10.2024).

8. Проект конвенции Организации Объединенных Наций против киберпреступности [Электронный ресурс]. – URL: https://documents.un.org/doc/undoc/gen/v24/055/08/pdf/v2405508.pdf (дата обращения – 01.10.2024).

9. A/68/98 [Электронный ресурс]. – URL: https://documents.un.org/doc/undoc/gen/n13/371/68/pdf/n1337168.pdf (дата обращения – 18.09.2024).

10. A/70/174 [Электронный ресурс]. – URL: https://documents.un.org/doc/undoc/gen/n15/228/37/pdf/n1522837.pdf (дата обращения – 18.09.2024).

11. BRICS Agenda for Digital Sovereignty [Электронный ресурс]. – URL: https://russiancouncil.ru/en/analytics-and-comments/analytics/brics-agenda-for-digital-sovereignty/ (дата обращения – 01.10.2024).

12. Digital solidarity vs. digital sovereignty: Which side are you on? [Электронный ресурс]. – URL: https://securityintelligence.com/articles/digital-solidarity-vs-digital-sovereignty/ (дата обращения – 18.09.2024).

Анна Гарегиновна Меликсетян,
Аспирант, кафедра международного права,
Дипломатическая академия МИД России,
E-mail: anna-meliksetyan1@yandex.ru

Anna G. Meliksetyan,
Postgraduate student
Department of International Public Law,
Diplomatic Academy of the Russian Ministry of Foreign Affairs,
E-mail: anna-meliksetyan1@yandex.ru

ЦИФРОВИЗАЦИЯ РЫНКА ТРУДА ЕВРАЗИЙСКОГО ЭКОНОМИЧЕСКОГО СОЮЗА

DIGITALIZATION OF THE LABOR MARKET OF THE EURASIAN ECONOMIC UNION

Аннотация. Настоящее исследование направлено на проведение анализа правового регулирования общего рынка трудовых ресурсов ЕАЭС в контексте цифровизации. Цифровизация создает возможности для так называемых виртуальных мигрантов трудоустроиться в отличном от государства проживания государстве-члене Союза. Суть мировой экономики в процессе виртуальной трудовой мобильности заключается в том, что мировая экономика переходит из физического пространства в информационное. Это создает широкий спектр возможностей как для работников, так и для работодателей. Однако этот процесс сопряжен с рядом препятствий. Цифровизация рынка труда становится неотъемлемой частью современных трудовых отношений, что обусловлено стремительным развитием и внедрением цифровых технологий во все сферы жизни. Данный процесс требует адекватного правового регулирования, особенно в контексте единого рынка труда ЕАЭС.

Ключевые слова: правовое регулирование новых форм занятости, безопасность персональных данных, виртуальная трудовая мобильность, цифровизация.

Abstract. This study focuses on analyzing the legal regulation of the common labor market within the EAEU in the context of digitalization. Digitalization creates opportunities for so-called virtual migrants to gain employment in a member state of the Union different from their country of residence. The essence of the global economy in the process of virtual labor mobility lies in its transition from the physical space to the informational one. This shift offers a wide range of opportunities for both employees and employers. However, this process is accompanied by a number of challenges. Digitalization of the labor market is becoming an integral part of modern labor relations due to the rapid development and integration of digital technologies into all spheres of life. This process necessitates adequate legal regulation, especially in the context of the unified labor market of the EAEU.

Key words: legal regulation of new forms of employment, personal data security, virtual labor mobility, digitalization.

Цифровизация рынка труда представляет собой комплексное и многогранное направление, требующее тщательного правового регулирования для обеспечения эффективной и безопасной реализации свободы передвижения трудовых ресурсов в рамках ЕАЭС. В данном контексте виртуальные трудовые мигранты пересекают национальные границы в режиме онлайн, оставаясь при этом на своих местах.

На сегодняшний день сама модель интеграции трансформируется под влиянием цифровизации. ЕАЭС стремится создать на своей территории единой цифровое пространство, в перспективе подключиться к которому смогут и иные государств, не входящие в состав интеграционного объединения. Цифровая трансформация оказывает постепенное влияние на все социально-экономические сферы и рынки в рамках ЕАЭС: производство, рынок труда, рынок товаров и услуг, финансовый рынок, рынок информации, бизнес-среда.

На уровне ЕАЭС было создано уже два цифровых продукта, которые облегчали процесс свободы передвижения и трудоустройства в рамках Союза.

С 2021 года под эгидой ЕЭК функционирует унифицированная система поиска «Работа без границ», которая, в сущности, является аналогом общеевропейской сети обмена вакансиями EURES, которая поддерживает свободное передвижение работников между странами интеграционного объединения.

В системе «Работа без границ» зарегистрировано на 2024 год 2 млн. резюме и 500 тысяч вакансий [3].

Второй цифровой продукт ЕАЭС был создан в период распространения коронавирусной инфекции под эгидой Фонда цифровых инициатив Евразийского банка развития «Путешествую без COVID-19» [2], задачей которого было обеспечение свободного и безопасного передвижения граждан между странами. Приложение позволяло находить ближайшие лаборатории для сдачи анализов на Covid-19 перед путешествием между Российской Федерацией, Республикой Армения, Республикой Беларусь, Республикой Узбекистан, Республикой Казахстан, Кыргызской Республикой и Республикой Таджикистан.

Цифровизация выступает не просто технологическим трендом, а фундаментальным процессом, определяющим облик современной экономики и общества. Именно впоследствии цифровизации появились новые формы занятости, в частности такие формы занятости как дистанционная и платформенная занятость, аутсорсинг, фриланс, совместное использование сотрудников и т.д. Изменение жизненного уклада людей в связи с информационными технологиями стало радикально влиять на сферу трудовой деятельности человека.

Заключение. Подводя итог, можно отметить, что, несмотря на прогрессирующий характер тенденции цифровизации рынка труда ЕАЭС, государства-члены могут столкнуться с рядом рисков, в частности в вопросах переоценки цифрового суверенитета отдельных государств-членов, в том

числе угрозы его нарушения, угрозы нарушения прав граждан на неприкосновенность частной жизни, перетока трудовых ресурсов в цифровые экономики третьих стран [4], утечки персональных данных работников в процессе трансграничного обмена данными, обесценивания ряда профессий и возникновения других, что может привести к дисбалансу на едином рынке труда.

Следовательно, при развитии цифровой интеграции ЕАЭС должен исходить из цели поиска баланса интересов между обеспечением и сохранением государственного суверенитета, в том числе цифрового, и развитием цифровых продуктов [2].

Список источников и литературы:

1. «Путешествую без COVID-19» // Официальный сайт МИД России [Электронный ресурс] − URL: https://www.mid.ru/ru/diverse/bezcovid/?TSPD_101_R0=08765fb817ab2000acea5c8d281fcda4114100c8ea8a2473c46072a40b6f5aaccadd7a2948e1d974086c7a8da7143000347e5894edf58fb77185b1ab87811fcc5eebc6a37be8f1dffa6738d0658dd5ac846f03ce6c67feca75f7780f52051cd4 (дата обращения: 19.12.2024).

2. Меликсетян А.Г. Правовые аспекты цифровизации рынка труда ЕАЭС: перспективы и вызовы// Электронное сетевое издание Международный правовой курьер/ 2024 год.

3. Проект «Работа без границ» стартовал в ЕАЭС // Официальный сайт Евразийской экономической комиссии [Электронный ресурс] − URL: https://eec.eaeunion.org/news/proekt-rabota-bez-granic-startoval-v-eaes/ (дата обращения: 19.12.2024).

4. Томашевский К.Л. Цифровизация и ее влияние на рынок труда и трудовые отношения (теоретический и сравнительно-правовой аспекты)// Вестник СПбГУ. Серия 14. Право. 2020. №2.

Лидия Николаевна Осауленко,
кандидат юридических наук, начальник отдела по защите прав потребителей, Евразийская экономическая комиссия,
E-mail: lidiyaosaulenko@yandex.ru

Lidiya N. Osaulenko,
Ph.D. in Law, Head of the Section,
Eurasian Economic Commission,
E-mail: lidiyaosaulenko@yandex.ru

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ПОТРЕБИТЕЛЯ В ЭЛЕКТРОННОЙ ТОРГОВЛЕ ЕАЭС: СОСТОЯНИЕ, ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ

ELECTRONIC COMMERCE AND CONSUMER RIGHTS IN THE EURASIAN ECONOMIC UNION: STATE, PROBLEMS AND PROSPECTS

Аннотация. Настоящее исследование направлено на проведение анализа проблематики информационной безопасности потребителей в контексте развития цифровых технологий и трансформации экономических процессов в рамках Евразийского экономического союза. Дана характеристика состояния защиты потребительских прав граждан, а также представлен краткий обзор законодательной базы в данной сфере, выявлены ключевые риски для информационной безопасности потребителей, сформулированы предложения по дальнейшему развитию политики ЕАЭС в сфере защиты прав потребителей.

Ключевые слова: безопасность данных, правовое регулирование безопасности данных, евразийская интеграция, ЕАЭС, право, интеллектуальные сервисы, международные отношения, права потребителей, цифровые технологии, электронная торговля.

Abstract. The article is aimed at analyzing the issues of consumer protection in the context of the development of digital technologies and the transformation of economic processes within the framework of the Eurasian Economic Union. The characteristics of the state of consumer rights protection

of citizens are given, as well as a brief overview of the legislative framework in this area is presented, key risks to consumer safety are identified, proposals for further development of the EAEU policy in the field of consumer protection are formulated.

Keywords: data security, legal regulation of data security, Eurasian integration, EAEU, law, artificial intelligence, intelligent services, international relations, consumer rights, digital technologies, electronic commerce.

Тенденции и состояние защиты потребителей в ЕАЭС. В Евразийском экономическом союзе (далее — ЕАЭС) проживают 183 миллиона человек. Более 90% населения пользуются возможностями электронной торговли, при этом 20% потребителей приобретают товар онлайн несколько раз в месяц, 19% — один раз в месяц[3]. Активные пользователи электронных торговых сервисов —покупатели в возрасте от 26 до 40 лет (45 %) и от 41 до 55 лет (37 %) [2]. Массовый переход потребительских правоотношений в онлайн формат повышает вероятность возникновения проблем для защиты интересов покупателей, что особенно актуально для обеспечения безопасности данных потребителей.

В ЕАЭС вопросы регулирования защиты интересов граждан, как потребителей, а также обеспечения безопасности их данных, до сих пор остаются на уровне национального законодательства. Попытки разработать международный акт по защите персональных данных ведутся с 2015 года, до настоящего времени не увенчались успехом [4].

Выработка общих механизмов безопасности данных должна выстраиваться с учетом имеющихся интеграционных возможностей ЕАЭС и в тех сферах, где такая работа наиболее востребована. Договором о ЕАЭС закреплены гарантии прав потребителей, а также обязательства государств-членов по формированию равных условий для защиты таких прав в ЕАЭС [1]. Создание международного правового поля ЕАЭС в данной сфере не предусмотрено.

Важным шагом вперед стало принятие программы совместных действий государств-членов ЕАЭС в сфере защиты прав потребителей [5]. Это решение объединило усилия стран для решения локальных проблем, но не дало возможности установить единые обязательные механизмы защиты потребителей и их данных в ЕАЭС.

Страны ЕАЭС проводят согласованную политику в сфере защиты прав потребителей, которая подразумевает сближение национального регулирования на основе рекомендаций Евразийской экономической комиссии. Степень сближения национального законодательства в сфере защиты прав потребителей определяется каждым государством-членом самостоятельно.

Гармонизации подходов по защите персональных данных граждан в рамках электронной торговли содержатся в рекомендации Евразийской экономической комиссии по защите потребителей при дистанционной торговле [6]. Документ принят в 2017 году, но актуален до настоящего времени.

В соответствии с указанными рекомендациями, обработка персональных данных потребителя должна соответствовать следующим ключевым аспектам: потребитель должен заранее дать своё согласие на обработку данных, причем такое согласие должно быть осознанным, чётким и однозначным; если это согласие было отозвано, оператор обязан прекратить обработку данных. Меры по защите данных должны приниматься с момента их получения оператором, которые должны нести ответственность за и сохранность. Передача данных, включая трансграничную, возможна только с согласия потребителя и в соответствии с законодательно установленными требованиям.

Обзор правовой базы и последних инициатив в области защиты прав потребителей в ЕАЭС. В странах ЕАЭС сформирована правовая и институциональная основа для защиты прав потребителей на национальном уровне, которая имеет сходства и различия.

Сходство заключается в том, что системы защиты прав потребителей, созданные в странах ЕАЭС, обладают в целом, общей структурой, состоящей из специальных правовых норм и правоприменительных институтов. Программные документы по защите прав потребителей существуют только в Российской Федерации [7].

Различия между правовыми системами стран ЕАЭС проявляются в степени детализации законодательства, а также в полномочиях и сферах компетенции национальных институтов защиты прав потребителей, структура, полномочия и количество которых существенно различаются. Постоянная корректировка норм национального права приводит к увеличению их разрозненности.

Проблематика, влияющая на защиту прав потребителей. В числе аспектов, влияющих на защиту интересов граждан и обеспечения безопасности их данных в электронной торговле, можно выделить сложности контроля и регулирования онлайн-рынка, недостаток прозрачности и доступности информации, высокие риски мошенничества. Ключевой проблемой для регуляторов является ограничение возможностей применения национального законодательства к трансграничным потребительским взаимоотношениям.

Очевидна проблема отсутствия механизмов разрешения трансграничных потребительских споров, в том числе связанных с обеспечением безопасности данных потребителей. Отраслевое законодательство ориентировано на национальные суды, но потребители редко используют судебные системы других стран для защиты своих прав. Решением этой проблемы может стать международный опыт в этой области: от создания международной сети по защите прав потребителей, в которой взаимодействуют государственные и общественные органы стран ЕАЭС, до создания единой онлайн-платформы по разрешению потребительских споров с обеспечением обезличивания данных.

Заключение: Условия развития единого рынка ЕАЭС связаны с отсутствием общих наднациональных стандартов и правил, гарантирующих равные условия для обеспечения и защиты потребительских прав граждан, а также безопасности их данных в электронной торговле. Расхождения между национальными законодательными актами в данной сфере неуклонно растет. Решение этой задачи возможно посредством создания комплексной правовой системы ЕАЭС к защите интересов граждан в цифровом пространстве.

Список источников и литературы:

1. Договор о Евразийском экономическом союзе (Астана, 29 мая 2014 г.) Правовой портал Евразийского экономического союза. Официальный сайт. [Электронный ресурс]. – URL: https://docs.eaeunion.org/docs/ru-ru/0003610/itia_05062014 (дата обращения 07.10.2024).

2. Общественное мнение населения стран ЕАЭС о правах потребителей в электронной торговле. Сайт Евразийской экономической комиссии. – URL: https://potrebitel.eaeunion.org/ru-ru/Pages/Obschestvennoe-mnenie-naseleniya-stran-EAES-o-pravah-potrebitelej-v-elektronnoj-torgovle.aspx (дата обращения 07.10.2024).

3. Комиссия подвела итоги масштабного социологического исследования для оценки защиты прав потребителей в странах ЕАЭС. Официальный сайт Евразийской экономической комиссии https://potrebitel.eaeunion.org/ru-ru/Pages/Komissiya-podvela-itogi-masshtabnogo-sociologicheskogo-issledovaniya-dlya-ocenki-zaschiti-prav-potrebitelej-v-stranah-EAES.aspx (дата обращения 07.10.2024).

4. Рабочая группа высокого уровня определит механизмы обеспечения безопасности данных в ЕАЭС. Официальный сайт Евразийской экономической комиссии https://eec.eaeunion.org/news/rabochaya-gruppa-vysokogo-urovnya-opredelit-mehanizmy-obespecheniya-bezopasnosti-dannyh-v-eaes/ (дата обращения 07.10.2024).

5. Распоряжение Евразийского межправительственного совета от 21.06.2022 № 12 «О Программе совместных действий государств - членов Евразийского экономического союза в сфере защиты прав потребителей» — Доступ из справочно-правовой системы «КонсультантПлюс» (дата обращения: 07.10.2024).

6. Рекомендаций Коллегии Евразийской экономической комиссии от 21 ноября 2017 г. № 27 «Об Общих подходах к проведению государствами – членами Евразийского экономического союза согласованной политики в сфере защиты прав потребителей при реализации товаров (работ, услуг) дистанционным способом» — Доступ из справочно-правовой системы «КонсультантПлюс» (дата обращения: 07.10.2024).

7. Стратегия государственной политики Российской Федерации в области защиты прав потребителей на период до 2030 года: Распоряжение Правительства Российской Федерации от 28 августа 2017 г. № 1837-р – Доступ из справочно-правовой системы «КонсультантПлюс» (дата обращения: 07.10.2024).

Мария Владимировна Стрелкова,
студент направления «Юриспруденция»,
Военный университет имени князя Александра Невского,
E-mail: strelkova-88@list.ru

Mariya V.Strelkova,
Student, Faculty of Law,
Prince Alexander Nevsky Military University,
E-mail: strelkova-88@list.ru

РОЛЬ РОССИИ В ОБЛАСТИ МЕЖДУНАРОДНОГО СОТРУДНИЧЕСТВА ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

THE ROLE OF RUSSIA IN THE FIELD OF INTERNATIONAL COOPERATION IN ENSURING INFORMATION SECURITY

Аннотация. Настоящее исследование направлено на анализ текущей ситуации вокруг решения проблемы формирования международного режима информационной безопасности. Дана характеристика позиций России и Запада в отношении дальнейшего пути к противодействию киберпреступности, а также обозначена роль России в создании честного баланса законных национальных интересов всех стран.

Ключевые слова: информационная безопасность, Россия и Запад, международные инициативы в рамках ООН, национальный суверенитет, киберсфера.

Abstract. The article is aimed at analyzing the current situation around solving the problem of forming an international information security regime. The article characterizes the positions of Russia and the West regarding the further path to countering information crime, and also outlines Russia's role in creating an honest balance of legitimate national interests of all countries.

Keywords: information security, Russia and the West, international initiatives within the UN, national sovereignty, cybersphere.

Пути взаимодействия стран по обеспечению информационной безопасности. Одним из приоритетов мирового сообщества является формирование международного режима информационной безопасности. По словам Генерального секретаря ООН Антониу Гутерриша, «десятки международных организаций в мире сегодня не являются членами семьи ООН, например БРИКС, ШОС, Африканский союз или Организация исламского сотрудничества. Однако они должны быть фундаментальными партнерами» [1]. С конца XX века Россия выдвигает инициативы по взаимодействию между странами в интересах формирования международного режима в области информационной безопасности и предотвращению конфликтов в цифровой среде. По словам Министра иностранных дел Российской Федерации Сергея Викторовича Лаврова, «в 1998 году Россия − с трибуны ООН − первой предупредила мир о рисках, которые таила в себе тогда еще зарождающаяся киберсфера, и предложила конкретные пути противодействия им» [2, с. 8]. На текущий момент ситуация в этой области остается сложной.

Информационно-коммуникационные технологии используются в целях вмешательства во внутренние дела суверенных государств. Некоторые страны открыто заявляют о своем праве наносить превентивные кибердары по потенциальным противникам, в том числе по объектам их критической инфраструктуры. Конвенция Совета Европы по борьбе с киберпреступностью (Будапештская конвенция) разрешает ее участникам без согласования действовать на территории иностранного государства.

Позиции России и Запада по противодействию информпреступности. Противоречия в позициях России и Запада по противодействию информпреступности заключаются в том, что Запад ищет защиту гражданских прав от механизмов универсальной конвенции, а Россия призывает к обеспечению интересов граждан и бизнеса от посягательств киберпреступников на их деньги и имущество через механизмы конвенции, к необходимости защиты национального суверенитета, территориальной целостности и невмешательстве во внутренние дела государств. Создание

универсального международного «кодекса поведения» в киберсфере станет гарантом устойчивого социально-экономического и научно-технического развития всех без исключения стран.

Создание единого универсального механизма по тематике информбезопасности. 9 августа 2024 года в Нью-Йорке Специальный межправительственный комитет ООН по разработке всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях под председательством Алжира завершил начатые в феврале 2022 года переговоры принятием проекта универсального договора.

На 79-й сессии Генеральной Ассамблеи ООН, прошедшей с 22 по 27 сентября 2024 года, Россия выступила за сохранение центральной роли ООН и, в частности, ее Рабочей группы открытого состава по международной информбезопасности. «Необходимо обеспечить выполнение достигнутой по итогам восьмой сессии РГОС договоренности о создании в ООН – по завершении деятельности нынешней Группы в 2025 г. – единого универсального механизма по тематике информбезопасности, действующего на основе принципа консенсуса и уполномоченного на выработку юридически обязывающих норм в цифровой сфере» [3]. Россия также выступила с инициативой проведения Форума по управлению Интернетом в России в 2025 году, за формирование справедливых международных технических стандартов и требований в области ИИ.

Заключение. Россия стоит на стороне коллективной работы в пользу формирования честного баланса законных национальных интересов всех стран. Таким образом воплощается в жизнь записанное в Уставе предназначение ООН: «Быть центром для согласования действий наций» [4].

Список источников и литературы:

1. Антониу Гутерриш: на Земле нет мира, работа ООН должна быть лучше. URL: https://tass.ru/interviews/21218783 (дата обращения: 12.09.2024).

2. Лавров С. В. Глобальные проблемы кибербезопасности и международные инициативы России по борьбе с киберпреступностью // Внешнеэкономические связи. 2020. №38. С. 6—11.

3. О позиции России на 79-й сессии Генеральной Ассамблеи ООН. URL: https://mid.ru/ru/foreign_policy/un/1966480/ (дата обращения: 14.09.2024).

4. United Nations Charter (full text). Available at: www.un.org/ru/about-us/un-charter/full-text (Accessed: 15.10.2024).

Анастасия Владимировна Щербань,
Аспирант, Факультет международных отношений,
СПбГУ,
E-mail: n.shche@mail.ru

Anastasia V. Shcherban,
PhD student, Faculty of International Relations,
St. Petersburg State University,
E-mail: n.shche@mail.ru

ФОРМИРОВАНИЕ ПОЛИТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РАМКАХ ОДКБ

FORMATION OF INFORMATION SECURITY POLICY WITHIN THE FRAMEWORK OF THE CSTO

Аннотация. Работа посвящена анализу политики в области обеспечения информационной безопасности стран-участниц ОДКБ. Представлены данные о реализации инициатив государств-участников Договора на региональном уровне, а также дальнейших планах развития усовершенствования сферы информационной безопасности.

Ключевые слова. ОДКБ, Российская Федерация, политика в области обеспечения информационной безопасности, информационный суверенитет.

Annotation. The work is devoted to the analysis of the information security policy of the CSTO member states. The data on the implementation of initiatives of the States parties to the Treaty at the regional level, as well as further plans for the development and improvement of the field of information security are presented.

Keywords. The CSTO, the Russian Federation, information security policy, information sovereignty.

Начало формирования политики информационной безопасности на уровне ОДКБ было положено в 2006 году. В Минске, на заседании Комитета секретарей советов безопасности, была создана Рабочая группа по вопросам информационной политики и безопасности. Перед Рабочей группой ставились следующие задачи: выявление угроз в области информационной

безопасности, а также координация совместных усилий государств-участников ОДКБ для их преодоления [2].

В декабре 2010 года в Москве состоялось заседание Совета коллективной безопасности. Среди итогов заседания можно отметить утверждение Положения о сотрудничестве стран-участниц ОДКБ в сфере обеспечения информационной безопасности. В Положении давалось определение «системы информационной безопасности», под которой понимается усилия политического, правового, научно-технического, финансового, кадрового и организационного характера, которые направлены на регулирование системы информационной безопасности в зоне ответственности ОДКБ [5].

Можно предположить, что еще в 2010 году государства-участники понимали важность формирования своей системы информационной безопасности. К тому времени наблюдалась дестабилизация политической обстановки на постсоветском пространстве. В качестве примера, можно привести Революцию роз в Грузии (2003 г.) и Оранжевую революцию в Украине (2004 г.), основными инструментами реализации которых стали СМИ, а также лидеры мнений, которые активно агитировали людей выйти на протесты.

В 2017 году, на очередном заседании стран-участниц ОДКБ в Минске, было подписано Соглашение о сотрудничестве государств-членов ОДКБ в области обеспечения информационной безопасности. В документе отмечено, что государства будут выстраивать систему информационной безопасности по принципам межгосударственного и межведомственного сотрудничества. Кроме этого, отмечена необходимость проведения совместных мероприятий, целью которых является укрепление системы информационной безопасности [6].

В Статье 2 Соглашения, государства дали определения терминологии, в частности: «деструктивное информационной воздействие», «защита информации», «информационная безопасность», «информационное

пространство», «компьютерная атака», «компьютерный инцидент», «критически важные структуры», «система информационной безопасности», «угроза информационной безопасности».

Среди главных угроз Соглашение определяет: осуществление деструктивного воздействия, под которым понимается использование ИКТ для нарушения действия органов власти, нанесения ущерба ИКТ системам, сетям и ресурсам, создание внутреннего социально-политического кризиса, а также разрушение духовно-нравственного стержня граждан государств-участников ОДКБ; использование ИКТ террористическими и экстремистскими организациями, а также осуществление преступной деятельности в глобальной сети Интернет [4].

Сотрудничество Сторон должно быть направлено на разработку правовых и практических механизмов совместного реагирования на угрозы информационной безопасности, совершенствование технологий, а также создание условий для компетентных органов Сторон.

Исходя из основных положений документа, можно отметить, что информационная безопасность имеет два измерения. Первое – это защита критически важной технологической инфраструктуры. Второе – безопасность и контроль самой информации, которая в этом понимании выступает самостоятельным субъектом.

В ноябре 2021 года Парламентской ассамблеей ОДКБ (г. Санкт-Петербург) был принят Модельный закон, опирающийся на положения предыдущих документов «Об информационной безопасности» [3]. В ходе анализа документа прослеживается, что информационная безопасность государства – это защита конституционного строя, территориальной целостности с использованием информационных средств. Отдельно акцентируется внимание на деструктивном влиянии социальных сетей, СМИ, которые размывают понятия граждан, что способствует разрушению целостности личности. К таким действиям можно отнести: дестабилизацию внутреннего устройства государства, разжигание политической,

национальной, этнической и религиозной ненависти, а также фальсификацию исторической памяти и подмену ценностей. В этой связи, отечественная наука отмечает необходимость обеспечения информационно-психологической, а иногда и в целом когнитивной безопасности [1].

Заключение. Сложное геополитическое положение разделило мир на два лагеря. В этой связи стремительная информатизация и цифровизация на международном уровне не была урегулирована в полном объеме. Альтернативой этому, может послужить регулирование сферы информационной безопасности в рамках национальных государств, а также региональных организаций или объединений. Ярким примером формирования собственной системы информационной безопасности на постсоветском пространстве может послужить ОДКБ. После начала активной информационной кампании Западом, направленной на подрыв мировой репутации России, а также дестабилизацию политической ситуации среди граждан, формирование системы информационной безопасности в рамках ОДКБ является одной из альтернатив защитить граждан постсоветского пространства от «перепрошивки мозгов», изменения ценностей, фальсификации истории.

Список источников и литературы:

1. Выходец Р.С. Политика ОДКБ в сфере информационно-психологической безопасности /СПб: «Фонд РМГК», 2024 – 432 с.

2. В ОДКБ создана рабочая группа по вопросам информационной политики и безопасности [Электронный ресурс] // Новости ВПК (сайт). 27.12.2006. URL: https://vpk.name/news/2126_v_odkb_sozdana_rabochaya_gruppa_po_voprosam_informacionnoi_politiki_i_bezopasnosti.html (дата обращения: 15.10.2024).

3. Модельный закон ОДКБ «Об информационной безопасности» [Электронный ресурс] // Парламентская Ассамблея Организации Договора о коллективной безопасности (ПА ОДКБ) (сайт). 29.11.2021. URL:

https://paodkb.org/events/assambleya-prinyala-modelnyy-zakon-obinformatsionnoy-bezopasnosti (дата обращения: 15.10.2024).

4. Пролегомены когнитивной безопасности. Коллективная монография / Под редакцией И. Ф. Кефели. СПб.: ИД «Петрополис», 2023. − 488 с.

5. Решение Совета коллективной безопасности Организации Договора о коллективной безопасности от 10 декабря 2010 года «О Положении о сотрудничестве государств-членов Организации Договора о коллективной безопасности в сфере обеспечения информационной безопасности» [Электронный ресурс] // Предпринимательское право (сайт). URL: http://businesspravo.ru/Docum/DocumShow_DocumID_181116.html (дата обращения: 15.10.2024).

6. Соглашение о сотрудничестве государств − членов Организации Договора о коллективной безопасности в области обеспечения информационной безопасности от 30 ноября 2017 года [Электронный ресурс] // Официальный интернет-портал правовой информации. URL: http:// publication.pravo.gov.ru/Document/View/0001201904260001 (дата обращения: 15.10.2024).

СЕКЦИЯ 7

«ЦИФРОВОЕ ПРОСТРАНСТВО КАК ТОЧКАПЕРЕСЕЧЕНИЯ ПОЛИТИКИ И ТЕХНОЛОГИЙ» ОРГАНИЗОВАНА СОВМЕСТНО С МОЛОДЕЖНЫМ СОВЕТОМ КООРДИНАЦИОННОГО ЦЕНТРА ДОМЕНОВ .RU/.РФ

Александр Александрович Игнатов,
к.п.н., с.н.с., Центр исследований международных институтов Института прикладных экономических исследований РАНХиГС (ЦИМИ ИПЭИ РАНХиГС), Член Молодежного совета при Координационном центре национального домена сети Интернет,
Email: ignatov-aa@ranepa.ru

Alexander A. Ignatov,
Ph.D. in Political Science, Senior Research Fellow,
Center for International Institutions Research, Institute for Applied Economic Research, RANEPA,
Member of The Youth Council of the Coordination Center for TLD .RU/.РФ
Email: ignatov-aa@ranepa.ru

ПОЛИТИКА УПРАВЛЕНИЯ ДАННЫМИ НОВЫХ СТРАН-ЧЛЕНОВ БРИКС И ПЕРСПЕКТИВЫ МНОГОСТОРОННЕГО СОТРУДНИЧЕСТВА В РАМКАХ ОБЪЕДИНЕНИЯ

DATA MANAGEMENT POLICY OF THE NEW BRICS STATES AND PROSPECTS FOR MULTILATERAL COOPERATION

Аннотация. В работе рассмотрены особенности формирования и развития национальных правовых режимов управления пользовательскими данными в новых странах-членах БРИКС, а также перспективы их многостороннего взаимодействия в этой сфере. Анализ включает изучение законов и инициатив по защите и локализации персональных данных, а также их трансграничной передаче. Подчеркивается важность дальнейшего сближения подходов к регулированию и взаимного признания национальных юрисдикций как безопасных, что откроет возможности для развития цифрового бизнеса и укрепления сотрудничества внутри БРИКС.

Ключевые слова: БРИКС, управление данными, персональные данные, кибербезопасность, трансграничная передача, локализация, международное сотрудничество.

Abstract. This paper examines the formation and development of national legal frameworks for user data management in the new BRICS member states, as

well as the prospects for their multilateral cooperation in this field. The analysis covers the examination of laws and initiatives on data protection and localization, as well as cross-border data transfers. The paper highlights the importance of further aligning regulatory approaches and mutually recognizing national jurisdictions as secure, thus opening up opportunities for the growth of digital business and the strengthening of cooperation within BRICS.

Key words: BRICS, data management, personal data, cybersecurity, cross-border transfer, data localization, international cooperation.

Введение. Управление пользовательскими данными становится одним из ключевых направлений цифровой политики в современном мире. Новые страны-участницы БРИКС — ОАЭ, Саудовская Аравия[11], Египет, Эфиопия и Иран — активно совершенствуют правовую базу в этой сфере, во многом опираясь на опыт Общего регламента по защите данных Европейского союза (GDPR). При этом каждая из этих стран учитывает национальные особенности, включая культурно-правовой контекст и приоритеты развития цифровой экономики. Анализ сравнительных преимуществ и различий в подходах к управлению данными позволяет оценить потенциал многостороннего сотрудничества в рамках БРИКС и способствует формированию единых принципов регулирования.

Обзор общих тенденций и отличий. Для всех новых стран-членов БРИКС актуален вопрос защиты персональных данных, включая аспекты сбора, обработки, хранения и трансграничной передачи. В ОАЭ [6] и Саудовской Аравии [3] приняты законы о защите данных, основанные на опыте GDPR, имеющие экстерриториальное действие и предусматривающие значительные штрафы за нарушения (до 2,5 млн долларов США в ОАЭ). В Египте [1] закон о защите данных, принятый в 2020 году, практически полностью соответствует основным положениям GDPR, однако расширяет понятие

[11] После саммита БРИКС в Казани в октябре 2024 года Саудовская Аравия получила статус «приглашенной страны», а процесс полноценного присоединения к БРИКС был формально приостановлен.

«чувствительных данных» и требует получения лицензии на трансграничную передачу данных. Эфиопия в 2024 году приняла закон о защите данных (Постановление 1321 / 2024) [7], стремясь максимизировать выгоды трансграничной передачи и защитить интересы пользователей в соответствии с международными стандартами. Особенностями эфиопского законодательства являются более низкие по сравнению с GDPR штрафы и обязательная локализация данных. Иран пока не имеет специального закона о защите персональных данных, но регулирует эти вопросы в соответствии с положениями Конституции [4] и уголовного кодекса [5], Законом об электронной коммерции [2] и постановлениями Верховного совета по киберпространству и Верховоного совета по культурной революции. Уже введено требование локализации пользовательских данных для иностранных социальных сетей, а также подготовлен проект Закона о защите персональных данных, хотя сроки его принятия не определены.

Большинство новых стран БРИКС допускают трансграничный обмен пользовательскими данными при условии, что принимающая юрисдикция обеспечивает эквивалентный или адекватный уровень защиты. Дополнительно могут действовать механизмы лицензирования, двусторонние или многосторонние соглашения, а в отдельных случаях допускается передача с согласия субъекта данных. Требования о локализации данных введены в Эфиопии и Иране, что отражает стремление государств контролировать поток данных и снижать риски несанкционированного доступа.

Перспективы многостороннего сотрудничества в рамках БРИКС. Укрепление сотрудничества в области управления данными среди новых стран-членов БРИКС открывает возможности для цифрового бизнеса и инноваций. Взаимное признание национальных правовых режимов в качестве «надежных» с т.з. обеспечения безопасности персональных данных, а также сближение подходов к обеспечению кибербезопасности могут облегчить трансграничный обмен информацией и способствовать развитию единых цифровых платформ. Гармонизация законодательств в сфере конкурентного

права позитивно скажется на инвестиционном климате и послужит стимулом для появления новых игроков на рынке. Совместная работа над общими стандартами будет способствовать интеграции цифровых рынков и формированию новых форматов делового сотрудничества.

Заключение. Анализ национальных политик управления данными в новых странах БРИКС показывает доминирование модели, близкой к GDPR, но с учетом локальных особенностей и приоритетов. Сферы трансграничной передачи и локализации данных регулируются по-разному, однако в целом наблюдается стремление к ужесточению мер защиты пользовательских данных. Перспективы многостороннего сотрудничества в области управления данными в рамках БРИКС выглядят весьма благоприятными, поскольку существует значительный потенциал для взаимного признания национальных режимов «адекватной» защиты данных. Его реализация будет способствовать развитию цифрового бизнеса, улучшению инвестиционного климата и углублению интеграции в сегменте платформенных услуг. Дальнейшая работа в данном направлении позволит создать более гармоничную среду для обмена информацией и укрепит роль БРИКС в формировании глобальной цифровой повестки.

Список источников и литературы:

1. Egypt – Data Protection Overview [Электронный ресурс] / DataGuidance. 30.07.2024. URL: https://www.dataguidance.com/notes/egypt-data-protection-overview (дата обращения: 15.10.2024).

2. Electronic Commerce Law of the Islamic Republic of Iran [Электронный ресурс] / WIPO. URL: https://wipolex-res.wipo.int/edocs/lexdocs/laws/en/ir/ir008en.html (дата обращения: 15.10.2024)

3. Introduction to the Saudi Arabia Personal Data Protection Law [Электронный ресурс] / UserCentric. 18.08.2023. URL: https://usercentrics.com/knowledge-hub/saudi-arabia-personal-data-protection-law-pdpl/ (дата обращения: 15.10.2024).

4. Iran (Islamic Republic of) 1979 (rev. 1989) [Электронный ресурс] / Constitute. URL: https://www.constituteproject.org/constitution/Iran_1989 (дата обращения: 15.10.2024).

5. Islamic Penal Code [Электронный ресурс] / United Nations Office on Drugs and Crime SHERLOCK. URL: https://sherloc.unodc.org/cld/uploads/res/islamic-penal-code_html/Islamic_Penal_Code.pdf (дата обращения: 15.10.2024).

6. Personal Data Protection Law [Электронный ресурс] / Saudi Data & AI Authority. URL: https://sdaia.gov.sa/en/SDAIA/about/Documents/Personal%20Data%20English%20V2-23April2023-%20Reviewed-.pdf (дата обращения: 15.10.2024).

7. Personal Data Protection Proclamation 1321 / 2024 [Электронный ресурс] / BonelliErede. 7.05.2024. URL: https://www.belex.com/en/case_study/personal-data-protection-proclamation-1321-2024/ (дата обращения: 15.10.2024).

Дарья Александровна Мальцева,
к. полит. наук, доцент кафедры теории и философии политики,
заместитель декана по молодежной политике факультета политологии
СПбГУ, Доцент кафедры сравнительной политологии РУДН им. П.Лумумбы,
E-mail: buenafiesta@mail.ru

Карина Евгеньевна Стребкова,
магистр психологии, член Молодежного совета при Координационном
центре национального домена сети Интернет,
E-mail: streb.karina@gmail.com

Darya A. Maltseva,
Ph.D. in Political Science, Associate Professor of the Department of Theory
and Philosophy of Politics, Deputy Dean for Youth Policy of the Faculty of
Political Science at St. Petersburg State University, Associate Professor of the
Department of Comparative Political Science at the Peoples' Friendship University
of Russia named after P. Lumumba,
E-mail: buenafiesta@mail.ru

Karina E.Strebkova,
Master in Psychology, Member of The Youth Council of the Coordination
Center for TLD .RU/.РФ,
E-mail: streb.karina@gmail.com

ПРАКТИКИ ИСПОЛЬЗОВАНИЯ НЕЙРОСЕТЕЙ ДЛЯ АНАЛИЗА УГРОЗ И РИСКОВ ДЛЯ МОЛОДЕЖИ В ЦИФРОВОМ ПРОСТРАНСТВЕ: ОПЫТ США[12]

AI-DRIVEN THREAT AND RISK ANALYSIS FOR YOUTH IN THE DIGITAL WORLD: USA CASE STUDIES

Аннотация. Настоящая работа исследует актуальные практики использования нейросетей в США для анализа угроз и рисков для молодежи в

[12] Исследование выполнено в рамках проекта №124102900048-1 «Технологии геймификации и искусственного интеллекта как инновационный инструмент реализации государственной молодежной политики РФ: стратегии, механизмы и практики», который реализован в Институте научной информации по общественным наукам РАН по итогам отбора научных проектов, поддержанных Министерством науки и высшего образования РФ и Экспертным институтом социальных исследований.

цифровом пространстве. На основе изучения 40 крупных проектов были выделены три ключевых направления: 1) мониторинг медиа и социальных сетей для предупреждения вреда психическому здоровью молодежи; 2) поддержка специалистов в области психического здоровья и социальной работы для более эффективной помощи жертвам насилия; 3) прогнозирование и анализ потенциальных угроз правоохранительными органами с целью выявления и пресечения девиантного поведения. Подчеркиваются методологические и этические ограничения использования данных технологий.

Ключевые слова: нейронные сети, США, молодежь, потенциальные угрозы и риски, психическое здоровье, социальные сети.

Abstract. This study examines current practices in the USA of utilizing neural networks to analyze threats and risks to youth in the digital space. A review of 40 major projects identified three key areas of focus: 1) monitoring media and social networks to prevent harm to youth mental health; 2) supporting mental health and social work professionals to provide more effective assistance to victims of violence; and 3) forecasting and analyzing potential threats by law enforcement agencies to identify and deter deviant behavior. The paper explores recent advances in the application of neural networks for threat and risk analysis of youth in the online environment, while highlighting methodological and ethical considerations associated with the use of these technologies.

Keywords: neural networks, USA, youth, potential threats and risks, mental health, social media.

В цифровом обществе молодежь сталкивается с возрастающим количеством рисков и угроз. Так, в интернет-пространстве молодые американцы все чаще встречаются с такими опасностями, как кибербуллинг, домогательства, сексуализированное насилие, торговля наркотиками, неконтролируемая продажа оружия, финансовые махинации, а также дезинформация [18]. В этом контексте критически важно раннее выявление

рисков, уменьшающее вероятность развития кризисных ситуаций. Современные технологии, в особенности нейронные сети, обладают значительным потенциалом для решения этих задач. Нейросети способны обрабатывать огромные массивы данных, обнаруживая скрытые закономерности и аномалии, которые могут указывать на потенциальные опасности для молодого поколения [35]. Тем не менее, внедрение таких технологий находится на начальной стадии в различных странах, что делает актуальным изучение текущих инициатив для лучшего понимания тенденций в данной сфере. В рамках настоящей статьи рассматриваются подходы, реализуемые в США, где нейросети используются для анализа угроз и рисков в цифровом пространстве.

На основе контент-анализа 40 крупных проектов в США (см. Таблица 1), информация о которых есть в открытом доступе, было выделено три ведущих тренда по использованию нейросетей для анализа угроз и рисков для молодежи: 1) мониторинг медиа и социальных сетей для предупреждения вреда психическому здоровью молодежи (28 проектов); 2) поддержка специалистов в области психического здоровья и социальной работы для более эффективной помощи жертвам насилия (3 проекта); 3) прогнозирование и анализ потенциальных угроз правоохранительными органами с целью выявления и пресечения девиантного поведения (9 проектов).

Таблица 1

Результаты поиска проектов с использованием ключевых слов

Поисковая система	Google
Ключевые слова	machine learning, risk, youth, young people, AI, neural network, threats, USA
Количество документов поисковой выдачи	920 (были изучены все страницы)
Количество релевантных проектов	40

Тренд **«Мониторинг медиа и социальных сетей для предупреждения вреда психическому здоровью молодежи»** выражается в создании систем анализа контента на основе машинного обучения для выявления и предотвращения случаев психологического насилия [1; 3; 11; 14; 15; 30; 39]. Нейросети изучают текстовые и голосовые сообщения, изображения и видео в социальных сетях [2] с целью распознавания языка вражды [19], кибербуллинга [2; 14; 22; 23; 24; 40; 34; 36], экстремизма [9] и других форм насилия. В этом контексте часто рассматривается борьба с дезинформацией [19]. Некоторая часть проектов направлена на использование анализа больших данных для определения потенциальных случаев самоубийства или идентификации неотложных психических кризисов среди молодежи путем мониторинга социальных медиа и запуск чат-ботов [5; 6; 8; 17; 20; 26; 29; 33; 38].

В тренд **«Поддержка специалистов в области психического здоровья и социальной работы для более эффективной помощи жертвам насилия»** входят исследования, проводимые при помощи машинного обучения с целью выявления повторяющихся паттернов у лиц, обращающихся за помощью [13; 25]. Разрабатываются сервисы, которые предлагают рекомендации в реальном времени, основываясь на сведениях о клиентах и возможностях обучения и развития навыков в преодолении негативного опыта [10; 37]. Рекомендательные системы на основе данных о клиентах могут предлагать чтение статей и книг на определенные темы, физические упражнения, которые адекватно встраиваются в образ жизни молодых людей, а также запускать короткие курсы по тренировке коммуникативных навыков.

Тренд **«Прогнозирование и анализ потенциальных угроз правоохранительными органами с целью выявления и пресечения девиантного поведения»** проявляется в проектах, где нейросети используются государственными структурами для предотвращения преступлений, в которые может быть вовлечена молодёжь [35]. Так, статистические расчеты и алгоритмы машинного обучения применяются для

мониторинга социальных сетей и построения прогностических моделей для выявления потенциальных случаев «скулшутинга» [32]. Остро стоит вопрос радикализации молодёжи с целью присоединения последней к террористическим организациям, поэтому ведутся исследования в области использования нейросетей для поиска контента, ассоциированного с международным терроризмом [12; 27; 28]. На защиту молодежи также направлены проекты, которые обеспечивают конфиденциальность личной информации в социальных сетях [21].

Заключение. Подводя итоги, важно отметить, что проекты в области цифровых технологий сталкиваются с этическими и методологическими ограничениями. Нейросетевые инструменты требуют экспертной оценки социологов, политологов, психологов и других специалистов по работе с молодежью для корректной интерпретации данных. Кроме того, цифровые данные часто нерепрезентативны и могут содержать предвзятости, ведущие к дискриминации [4; 31]. Помимо прочего, описанные потенциальные и существующие проекты поднимают вопросы приватности и безопасности личной информации [5]. Это означает, что разработчикам цифровых решений необходимо найти трудноосуществимый баланс между безопасностью и сохранением принципов свободы слова и доступа к информации и технологиям.

Список источников и литературы:

1. Как Facebook [13] использует искусственный интеллект для модерации контента? Available at: https://www.facebook.com/help/1584908458516247

2. AI-powered content moderation is Twitch's AutoMod system. Available at: https://www.linkedin.com/pulse/leveraging-ai-combat-cyberbullying-andre-ripla-pgcert-avsbe (Accessed: 15.10.2024).

[13] Организация Meta, а также её продукты Instagram и Facebook, упомянутые в тезисах, признаны экстремистскими на территории РФ.

3. American Psychological Association. Potential risks of content, features, and functions: The science of how social media affects youth. Available at: https://www.apa.org/topics/social-media-internet/youth-social-media-2024 (Accessed: 15.10.2024).

4. Blank G. & Groselj D. Dimension of Internet Use: Amount, Variety, and Types // Information, Communication & Society. №17, 2014. pp. 417-435.

5. Boyd D. & Crawford K. Critical Questions for Big Data: Provocations for a Cultural, Technological, and Scholarly Phenomenon // Information, Communication, & Society. №15, 2012. pp. 662-679.

6. Can AI Support Youth Mental Health? Available at: https://news.utexas.edu/2020/02/11/can-ai-support-youth-mental-health (Accessed: 15.10.2024).

7. Centers for Disease Control and Prevention. Suicide Prevention. Available at: https://www.cdc.gov/suicide/index.html (Accessed: 15.10.2024).

8. Character.ai: Young people turning to AI therapist bots. Available at: https://www.bbc.com/news/technology-67872693 (Accessed: 15.10.2024).

9. Cherney A., Belton E., Norham S. A. B. & Milts, J. Understanding youth radicalisation: an analysis of Australian data // Behavioral Sciences of Terrorism and Political Aggression, 2020. 14(2), pp. 97–119.

10. Common Sense Media. Available at: https://www.commonsensemedia.org/research (Accessed: 15.10.2024).

11. Comulada W.S., Goldbeck C., Almirol E. et al. Using Machine Learning to Predict Young People's Internet Health and Social Service Information Seeking // Prev Sci. 2021. Nov 22(8). pp. 1173-1184.

12. Criezis M. AI Caliphate: The Creation of Pro-Islamic State Propaganda Using Generative AI // The Global Network on Extremism and Technology (GNET). 2024. Available at: https://gnet-research.org/2024/02/05/ai-caliphate-pro-islamic-state-propaganda-and-generative-ai/# (Accessed: 15.10.2024).

13. Crisis Text Line. Available at: https://www.crisistextline.org (Accessed: 15.10.2024).

14. Cyberbullying.AI. Available at: https://solve.mit.edu/challenges/gender-equity-in-stem-challenge/solutions/75546 (Accessed: 15.10.2024).

15. Daneshvar H., Boursalie O., Samavi R. et al. Chapter 9 – SOK: Application of machine learning models in child and youth mental health decision-making // Advanced Studies in Complex Systems: Theory and Applications, Artificial Intelligence for Medicine. Academic Press, 2024. pp. 113-132.

16. Drew Barvir, MBA ’23: Harnessing AI to Support Youth Mental Health and Safety. Available at: https://www.gsb.stanford.edu/experience/news-history/drew-barvir-mba-23-harnessing-ai-support-youth-mental-health-safety (Accessed: 15.10.2024).

17. Facebook's AI Tools for Suicide Prevention Facebook. Available at: https://www.facebook.com/safety/resources (Accessed: 15.10.2024)[14].

18. Freed D., Bazarova N. N., Consolvo S. et al. Understanding Digital-Safety Experiences of Youth in the U.S. // In Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems (CHI '23). Association for Computing Machinery. New York, USA. Article 191, 2023. pp. 1–15.

19. Google's Jigsaw. Available at: https://jigsaw.google.com/ (Accessed: 15.10.2024).

20. Götzl C., Hiller S., Rauschenberg C. et al. Artificial intelligence-informed mobile mental health apps for young people: a mixed-methods approach on users’ and stakeholders’ perspectives // Child Adolesc Psychiatry Ment Health. Available at: https://doi.org/10.1186/s13034-022-00522-6 (Accessed: 15.10.2024).

21. How AI can help give teens protection and privacy on social media. Available at: https://www.fastcompany.com/91021866/how-ai-can-help-give-teens-protection-and-privacy-on-social-media (Accessed: 15.10.2024).

[14] Сервис признан экстремистским и запрещен в России.

22. Instagram brings on DeepText AI in effort to eradicate cyberbullying // Outside Insight. Available at: https://outsideinsight.com/insights/instagram-brings-on-deeptext-ai-in-effort-to-eradicate-cyberbullying (Accessed: 15.10.2024)[15].

23. Kumar Y.; Huang K.; Perez A. et al. Bias and Cyberbullying Detection and Data Generation Using Transformer Artificial Intelligence Models and Top Large Language Models. Available at: https://doi.org/10.3390/electronics13173431 (Accessed: 15.10.2024).

24. Leveraging AI to Combat Cyberbullying. Available at: https://www.linkedin.com/pulse/leveraging-ai-combat-cyberbullying-andre-ripla-pgcert-avsbe (Accessed: 15.10.2024).

25. Levine A. S. Suicide hotline shares data with for-profit spinoff, raising ethical questions // Politico. 2022. Available at: https://www.politico.com/news/2022/01/28/suicide-hotline-silicon-valley-privacy-debates-00002617 (Accessed: 15.10.2024).

26. Lockett A., Zhang J., Borji S. et al. Health Insurance Literacy Among Young Adults: The Role of Search Generative Experience and AI. Proceedings of the Association for Information Science and Technology. Vol. 61, 2024. pp. 1005-1007.

27. Macdonald S. & Mattheis A. Using Artificial Intelligence and Machine Learning to Identify Terrorist Content Online. Available at: http://dx.doi.org/10.13140/RG.2.2.24800.46084 (Accessed: 15.10.2024).

28. Macdonald S., Correia S.G. & Watkin A.-L. Regulating terrorist content on social media: automation and the rule of law // International Journal of Law in Context. 15(2), 2019. pp. 183–197.

29. McHugh C.M., Ho N., Iorfino F. et al. Predictive modelling of deliberate self-harm and suicide attempts in young people accessing primary care: a machine learning analysis of a longitudinal study // Soc Psychiatry Psychiatr Epidemiol. №58, 2023. pp. 893–905.

[15] Организация Meta, а также её продукты Instagram и Facebook, упомянутые в тезисах, признаны экстремистскими на территории РФ.

30. Mindwise Innovations. Available at: https://www.mindwise.org/ (Accessed: 15.10.2024).

31. O'Neil C. Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy // New York: Crown Publishers, 2016. 272 p.

32. Police Surveillance in Chicago. Predictive Policing. Available at: https://chicagopolicesurveillance.com/tactics/predictive-policing.html (Accessed: 15.10.2024).

33. Project Violet. Available at: https://www.cdc.gov/suicide/facts/index.html (Accessed: 15.10.2024).

34. Reynolds K., Kontostathis A. & Edwards L. Using Machine Learning to Detect Cyberbullying // Proceedings of the 2011 10th International Conference on Machine Learning and Applications and Workshops – Vol. 02. IEEE Computer Society, USA, 2011, pp. 241–244.

35. Rigano C. Using Artificial Intelligence to Address Criminal Justice Needs // National Institute of Justice. Available at: https://nij.ojp.gov/topics/articles/using-artificial-intelligence-address-criminal-justice-needs (Accessed: 15.10.2024).

36. Snapchat Launches Anti-Bullying Tools On World Mental Health Day. B&D. Available at: https://www.bandt.com.au/snapchat-launches-anti-bullying-tools-on-world-mental-health-day/ (Accessed: 15.10.2024).

37. The Trevor Project Launches New AI Tool To Support Crisis Counselor Training. Available at: https://www.thetrevorproject.org/blog/the-trevor-project-launches-new-ai-tool-to-support-crisis-counselor-training/ (Accessed: 15.10.2024).

38. UT Austin, Cornell Researchers Developing AI Interventions to Address Suicide Rates Among Black Youth. Available at: https://news.utexas.edu/2024/01/31/ut-austin-cornell-researchers-developing-ai-interventions-to-address-suicide-rates-among-black-youth (Accessed: 15.10.2024).

39. Wysa. Available at: https://www.wysa.com/children-and-young-people (Accessed: 15.10.2024).

40. Yan W., Yuan Y., Yang M. et al. Detecting the risk of bullying victimization among adolescents: A large-scale machine learning approach // Computers in Human Behavior. Volume 147, 2023. Available at: https://doi.org/10.1016/j.chb.2023.107817 (Accessed: 15.10.2024).

Марина Владиславовна Моисеева,
студентка 3 курса, факультет глобальных процессов,
МГУ им. Ломоносова,
член Исполнительной дирекции Школы МИБ ДА МИД
и Молодёжного совета Координационного центра доменов .RU/.РФ
E-mail: marina-mareev@yandex.ru

Marina V. Moiseeva,
3rd year student, the Faculty of Global Studies,
Lomonosov Moscow State University,
Member of the Executive Board of the School of IIS
of the Diplomatic Academy of the Russian MFA and the Youth Council of the
Coordination Center for TLD .RU/.РФ
E-mail: marina-mareev@yandex.ru

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В СОВРЕМЕННОЙ ПОВЕСТКЕ БРИКС

CYBERSECURITY IN CONTEMPORARY BRICS AGENDA

Аннотация. Данная статья обозначает прогнозируемо успешные векторы обсуждений внутри объединения, препятствия на пути к принятию компромиссных решений, а также перспективы для присоединившихся членов.

Ключевые слова: информационная безопасность, БРИКС, ИКТ и терроризм, кибератаки, цифровая валюта, контентные угрозы, управление интернетом.

Abstract. The article is aimed at outlining the anticipatedly successful vectors of the discussions within the organization, obstacles on the way to the decision-making and opportunities for the newly joined members.

Keywords: cybersecurity, BRICS, ICT and terrorism, cyberattacks, digital currency, content threats, Internet governance.

Введение. Изучение современной повестки информационной безопасности БРИКС и цифрового развития объединения в целом стоит начать с рассмотрения перечня целей председательства Российской Федерации [10]. Обозреваемая тематика напрямую коррелирует с I (о безопасности) и II (об экономике) разделами, затрагивающими политическую и экономическую стороны использования ИКТ[16]. Именно в год председательства России к объединению присоединились четыре значимых актора[17]. Это открывает новые возможности и перед объединением, и перед присоединившимися странами, и потому требует детального изучения.

Уроки встречи министров связи стран БРИКС. В БРИКС ожидается появление органов и реестров для обмена данными об угрозах кибербезопасности, финансирования терроризма и отмывания денег [1]. По сути, это является кооперацией групп реагирования профильных ведомств, которая могла бы произойти и без участия в объединении, тем не менее оно ускорило налаживание связей.

Вслед за работой ЕС и ООН, затрагивающей ИИ, БРИКС тоже вносит его в повестку. Главы делегаций признают важность создания кодекса этики, уже представленного российской стороной, а также поощряют запуск Инициативы БРИКС по защите детей в цифровой среде [3].

Перспективные направления развития полилога. Пожалуй, самая проработанная и широко освещаемая в БРИКС с самого основания тема – необходимость борьбы с терроризмом и экстремизмом с помощью ИКТ. Ожидается, что работа продолжится, т.к. для новоприбывших арабских государств это болевая точка. Те же страны выступают против милитаризации киберпространства, т.к. подвергаются негативным эффектам проявления этого феномена в регионе и сами участвуют в его формировании [2]. Из новых направлений развития сотрудничества можно назвать диалог по поводу

[16] Подразумеваются пункты про недопущение киберконфликтов, милитаризации информационного пространства, использование платежных систем и финансовых технологий, рост производительности труда и цифровизации.
[17] ОАЭ, Эфиопия, Египет, Иран (Саудовская Аравия так и не стала полноформатным участником).

технологий умного города под эгидой ОАЭ, дипфейков[18]. Тема именно контентной, а не «физической»[19] информационной безопасности будет активно продвигаться в повестку, так как многие страны уже имеют подобные инициативы на национальном уровне [18] [15] [9, с. 71]. Т.е. нельзя утверждать, что работа будет вестись только над инфраструктурной базой информационной безопасности, которая более актуальна для ЮАР, Бразилии и Эфиопии [5]. Определённую долю внимания забирает вопрос кибератак; можно предположить, что работу возглавит Россия, так как она оценивается как наиболее подверженная воздействию вредоносного ПО. У остальных стран тоже есть подобные проблемы, например, Бразилия лидирует по атакуемости троянами [7], а африканский континент всё чаще используется как «тренировочный полигон» для хакеров [19]. В дальнейшем может быть разобран кейс Индии, которая является и объектом угроз [9, с. 234], и их источником[20].

Возможные разногласия. Некоторые члены объединения взяли вектор на запреты в сфере ИКТ: так можно сказать, например, об IP-телефонии в Эфиопии [12] и VPN-сервисах в Китае. Могут возникнуть разногласия и в деле обмена данными, управления интернетом. Россия и Китай (и частично Индия) выступают за мультилатеральный подход, а Бразилия и ЮАР – за мультистейкхолдерный [5], и ожидается, что ввиду особенностей политического устройства новые члены присоединятся скорее к первому лагерю. Разнятся и позиции по поводу ратификации европейских соглашений и внедрения соответствующих стандартов[21]. Неоднозначно также будущее в плане конфронтации, сотрудничества с Западом или просто построения альтернативы ему в регуляторике ИКТ, учитывая «антиблоковый» характер объединения.

[18] У Китая, например, есть отдельное Положение о контроле распространения дипфейков от 2022 г., регулирующее их.
[19] Имеется в виду материальная, технологическая база киберзащиты.
[20] Имеется в виду, например, мошеннический бизнес, задействующий серые колл-центры.
[21] Например, в плане подписания Будапештской конвенции, поддержки Парижского призыва, Конвенции и киберпреступности ЕС и стандартов трансграничной передачи данных.

Шансы для новых членов. Вступление в БРИКС для развивающихся стран – шаг навстречу дедолларизации и расчёту в национальных валютах, в том числе цифровых. У БРИКС очевидно больше возможностей и ресурсов для внедрения ликвидного блокчейн-SWIFT-аналога, чем у национальных объединений. Однако несмотря на распространённое до недавнего времени мнение, что платформа уже в разработке [14], В.В. Путин опроверг запуск процесса на пресс-конференции после саммита БРИКС в Казани, при этом подчеркнув, что это «очень важный вопрос» [11]. Неоднозначный ответ объясняется тем, что на Западе опасаются инициативы из-за долгосрочного риска финансовой фрагментации и возможной утери технологического преимущества. Вопрос о реальном положении дел остаётся подвешенным.

Вступление в БРИКС и участие в освещении повестки по информационной безопасности – отличный шанс заявить о себе политически для ОАЭ, которые играют значимую роль в мировой экономике, но не были до этого вовлечены в работу Рабочей группы открытого состава и Группы неправительственных экспертов. Для Эфиопии и всего африканского континента членство в BRICS – ещё один шаг на пути к достижению Agenda 2063, где заявлено не только устойчивое развитие с помощью технологий, но и превращение Африки в значимого игрока на мировой арене [13]. Эфиопия, являясь давним дипломатическим «хабом», может сыграть даже большую роль, чем ЮАР. Возможно, она вдохновит другие развивающиеся страны, преодолев разрыв в развитии ИКТ[22] путём получения доступа к инвестициям Нового банка развития.

Что примечательно, большинство стран нового состава объединения согласно Global Cybersecurity Index 2024 [16] входят в Тир 1 (Role Modeling или «Подающие пример») [23] . Ещё три – в Тир 2 (Advancing,

[22] Если градировать страны БРИКС по ICT Development Index 2024 от высшего к низшему значению, то Эфиопия окажется на последнем месте с отрывом от ЮАР почти в 50 очков: ОАЭ – 97.5, Китай – 85.8, ЮАР – 83.6, Иран – 82.2, Бразилия – 82, Египет – 76.8, Эфиопия – 39.8. Данных об Индии нет. Источник – https://www.itu.int/itu-d/reports/statistics/IDI2024/.

[23] Индия, ОАЭ, Египет, Бразилия.

«Развивающиеся»)[24] и Эфиопия – в Тир 3 (Establishing, «Формирующиеся»). Сообщество членов, более активных и успешных в попытках обеспечить кибербезопасность, в перспективе действительно может помочь остальным участникам в достижении более впечатляющих показателей.

Результаты саммита БРИКС 22-24 октября. Говоря о Заседании, можно отметить три характера высказываний: о достижениях стран, достижениях БРИКС и планах на будущее[25]. При этом сразу несколько акторов – особенно на этом акцент сделала Бразилия – высказались о необходимости окончательного формирования новой независимой и равноправной финансово-банковской системы БРИКС. Учитывая слова В.В. Путина о неготовности цифровых модификаций для неё, интересно, во что выльется имеющаяся потребность.

Переходя к Казанской декларации [6], важно учесть, что странами вынесен в отдельный пункт комментарий о террористическом акте с использованием ИКТ в Бейруте 17.09.2024, который был назван нарушением международного права. Является ли это маркером будущей работы БРИКС над чётко оформленным запретом на использование ИКТ в военных целях, пока неизвестно, однако позиция ясна. В п. 54 отмечаются важность ИКТ в преодолении цифрового разрыва и социально-экономических проблем и

[24] Китай, ЮАР, Россия.

[25] Краткий обзор релевантных тезисов на Заседании по странам и департаментам БРИКС (те, которые не были выделены, не делали фокус на конкретных пунктах повестки кибербезопасности и развития ИКТ):
Россия. Из инновативных предложений России можно выделить стабилизацию совместного информирования о запуске цифровых сервисов по урегулированию споров в электронной коммерции и инициативу о создании альянса БРИКС в области искусственного интеллекта, регламентирующего его легальное использование.
КНР. Из результатов работы была упомянуты создание центра БРИКС по сотрудничеству в сфере развития технологий искусственного интеллекта, а в секции планов – инициатива, касающаяся сотрудничества по вопросу цифрового образования. С последней связаны перспективы обмена, что существенно повысит качество человеческого капитала, задействованного в постиндустриальной экономике (и потенциально уровень информационной безопасности). Высказано желание строительства сети сотрудничества БРИКС в области цифровых экосистем.
Индия. Ставится в заслугу разработка унифицированного интерфейса для платежей, уже имплементированного в ОАЭ и готового для внедрения в других странах БРИКС, а также выражается готовность делиться опытом в сфере цифрового здоровья
Деловой совет БРИКС. Сказано о действиях по созданию единой цифровой инфраструктуры, совместному использованию биометрических систем идентификации, развитию информационной безопасности и цифровой инклюзивности.
Полная стенограмма см. Заседание саммита БРИКС в расширенном составе // Официальный сайт Президента Российской Федерации. URL: http://www.kremlin.ru/events/president/transcripts/75375.

одновременная опасность этих технологий; говорится о ведущей роли органов ООН в определении правил ответственного пользования ИКТ. В пп. 55 и 69 подчёркнуты достижения сотрудничества стран БРИКС в обеспечении информационной безопасности [26] . П. 56 делает акцент на контентном компоненте информационной безопасности, упоминая важность целостности и свободы потока информации, подчёркивает неприемлемость распространения фейков и агрессивных высказываний и вместе с этим необходимость обеспечения свободы слова. Два последних явления как будто конкурируют между собой и потому интересен способ обеспечения выполнения обоих на нормативной основе. Тем не менее, сам вектор на контентные угрозы подтверждает гипотезу о превалировании мнения Китая, России и арабского мира на этот счёт. П. 77 посвящён важности обеспечения устойчивости и безопасности управления Интернетом и функционирования цифровой экономики в условиях внедрения инновативных технологий. В вопросе ИИ опять выделяется роль ООН (п. 78) и Института БРИКС по изучению сетей будущего, в том числе в контексте помощи развивающимся странам в укреплении потенциала ИИ (пп. 78-79).

Заключение. Как следует из обзора недавних мероприятий выше, у БРИКС существует достаточное количество активных профильных структур, касающихся ИКТ. Они не обладают законодательными полномочиями (да и в целом характер объединения БРИКС пока не подразумевает таковых), но являются центрами научно-технологического сотрудничества в соответствующей сфере, а в каких-то случаях и помощи. Казанская декларация, отводит много места рассмотрению проблем ИКТ, что делает тематику актуальной и перспективной для последующего взаимодействия стран БРИКС. Гипотезы о векторах этого взаимодействия подтверждаются, однако реализация мер и их жёсткость, а также конкретизация отношений с

[26] В частности, работа Реестра контактных пунктов и Рабочей группы БРИКС по вопросам безопасности в сфере использования ИКТ и Канала оперативного обмена данными в сфере информационной безопасности БРИКС.

Западом – элементы будущей повестки. Остаётся лишь наблюдать за развитием событий.

Список источников и литературы:

1. БРИКС объединились во благо кибербезопасности // COMNEWS от 13.09.2024. URL: https://www.comnews.ru/content/235179/2024-09-13/2024-w37/1007/briks-obedinilis-vo-blago-kiberbezopasnosti??utm_source=telegram&utm_medium=general&utm_campaign=general (дата обращения: 16.10.2024).

2. Валиахметова Г. Н., Цуканов Л. В. Цифровой вызов для арабского мира: фактор интеграции или дифференциации? // Вестник Российского университета дружбы народов. Серия: Международные отношения. 2022. Т. 22, № 2. С. 303-319.

3. Встреча министров связи стран БРИКС прошла в Иннополисе // BRICS RUSSIA 2024 от 02.10.2024. URL: https://brics-russia2024.ru/news/vstrecha-ministrov-svyazi-stran-briks-proshla-v-innopolise/ (дата обращения: 16.10.2024).

4. Заседание саммита БРИКС в расширенном составе // Официальный сайт Президента России. URL: http://www.kremlin.ru/events/president/transcripts/75375 (дата обращения: 09.11.2024).

5. Игнатов А. А., Зиновьева Е. С. «Цифровой суверенитет» в повестке объединения БРИКС // РСМД. 2024. URL: https://russiancouncil.ru/analytics-and-comments/analytics/tsifrovoy-suverenitet-v-povestke-obedineniya-briks/ (дата обрщения: 16.10.2024).

6. Казанская декларация XVI Саммита БРИКС // Официальный сайт Президента Российской Федерации. URL: http://static.kremlin.ru/media/events/files/ru/MUCfWDg0QRs3xfMUiCAmF3LEh02OL3Hk.pdf (дата обращения: 15.11.2024).

7. Коротков С. В. Формирование механизма противодействия угрозам информационной безопасности БРИКС – объективная потребность для суверенитета государств-участников межгосударственного объединения [Эл. ресурс] // Международная жизнь. 2024. URL: https://interaffairs.ru/news/show/45745?ysclid=ly8nlczzbz729242806 (дата обращения: 16.10.2024).

8. Минфин сообщил о работе над платформой для расчетов в нацвалютах в БРИКС // РБК от 26.06.2024 URL: https://www.rbc.ru/finances/26/06/2024/667b4c5f9a7947478a28de7f (дата обращения: 09.11.2024).

9. Особенности политики государств-участников БРИКС в сфере развития ИКТ, обеспечения национальной и международной информационной безопасности: сборник / Под общ. ред. Б. Н. Мирошникова. М.: НАМИБ, 2024, 402 с.

10. Приоритеты председательства Российской Федерации в объединении БРИКС в 2024 году // BRICS RUSSIA 2024 Official Website. URL: https://brics-russia2024.ru/russia-and-brics/priorities/?ysclid=m0uqdxt85p396228688 (дата обращения: 16.10.2024).

11. Путин опроверг создание в БРИКС альтернативы SWIFT // РБК от 24.10.2024. URL: https://www.rbc.ru/finances/24/10/2024/671a68a79a794736c04b1b8c (дата обращения: 09.10.2024).

12. Эфиопия объявила Skype вне закона // Lenta.ru от 15.06.20212 URL: https://lenta.ru/news/2012/06/15/novoip/ (дата обращения: 16.10.2024).

13. Agenda 2063: The Africa We Want. // African Union Official Website. URL: https://au.int/en/agenda2063/overview (дата обращения: 15.10.2024).

14. BRICS Confirms 159 Participants Will Adopt New Payment System // Watcher.Guru от 10.09.2024. URL: https://watcher.guru/news/brics-confirms-159-participants-will-adopt-new-payment-system (дата обращения 16.10.2024).

15. Cyber safety and digital security // The Official Portal of the UAE Government. URL: https://u.ae/en/information-and-services/justice-safety-and-the-law/cyber-safety-and-digital-security (дата обращения: 16.10.2024).

16. Global Cybersecurity Index // ITU Official Website. URL: https://www.itu.int/hub/publication/d-hdb-gci-01-2024/ (дата обращения: 10.10.2024).

17. ICT Development Index 2024 // ITU Official Website. URL: https://www.itu.int/itu-d/reports/statistics/IDI2024/ (дата обращения: 16.10.2024).

18. Law No. 180/2018 regulating the press and the media and the Supreme Council for Media // International Labour Organisation Natlex official website. URL: https://wwwex.ilo.org/dyn/natlex2/natlex2/files/download/111247/EGY111247.pdf (дата обращения: 16.10.2024).

19. New research suggests that Africa is being used as a 'testing ground' for nation state cyber warfare // Performanta от 29.04.2024. URL: https://www.performanta.com/post/new-research-suggests-africa-is-being-used-as-a-testing-ground-for-nation-state-cyber-warfare (дата обращения: 16.10.2024).

Никита Евгеньевич Соловьев,
член Исполнительной дирекции Школы МИБ ИАМП
Дипломатической академии МИД России,
Член Молодёжного совета Координационного центра доменов .RU/.РФ,
E-mail: info@mibschool.ru

Nikita E.Solovev,
Member of the Executive Board
of the School of International Information Security
of the Institute of Contemporary International Problems
of the Diplomatic Academy of the Russian Foreign Ministry,
Member of Youth Council of the Coordination Center for TLD .RU/.РФ,
E-mail: info@mibschool.ru

ЭКСПЛУАТАЦИЯ УЯЗВИМОСТЕЙ ГЕНЕРАТИВНЫХ МОДЕЛЕЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В КОНТЕКСТЕ ГЕНЕРАЦИИ ВРЕДОНОСНОГО КОНТЕНТА

EXPLOITATION OF VULNERABILITIES IN GENERATIVE ARTIFICIAL INTELLIGENCE MODELS FOR MALICIOUS CONTENT GENERATION

Аннотация. Настоящий доклад посвящен анализу эксплуатации уязвимостей генеративных моделей искусственного интеллекта в контексте генерации вредоносной информации, а также дана оценка влияния злонамеренного применения генеративных моделей на международную информационную безопасность.

Ключевые слова: международная информационная безопасность, терроризм, информационная угроза, искусственный интеллект, уязвимости, генерация, промпт, ChatGPT, YandexGPT, Шедеврум, Кандинский, ООН, OpenAI, Yandex, SberAI.

Abstract. The present report is dedicated to the analysis of the exploitation of vulnerabilities in generative artificial intelligence models in the context of malicious information generation. Furthermore, it evaluates the impact of the malicious use of generative models on international information security.

Keywords: international information security, terrorism, information threat, artificial intelligence, vulnerabilities, generation, prompt, ChatGPT, YandexGPT, Shedvrum, Kandinsky, UN, OpenAI, Yandex, SberAI.

Модель текущего технологического прогресса характеризуется высокой степенью развития и проникновения передовых технологий искусственного интеллекта (ИИ), который способен решать широкий спектр возложенных на него задач. Обладая значительным преимуществом перед когнитивными возможностями человека при обработке, анализе и принятии решений, ИИ способен усиливать потенциал оператора в достижении поставленных целей при существенном сокращении временных затрат.

Являясь технологиями двойного назначения, генеративные модели искусственного интеллекта, наряду с их прогрессивным потенциалом, существенно усилили деструктивные возможности злоумышленных акторов, расширив спектр информационных угроз. В частности, их применение включает как создание вредоносного программного обеспечения, используемого для взлома IT-систем, так и генерацию контента, способного оказывать негативное влияние на психологическое состояние человека.

В своем исследовании, посвящённом анализу влияния выявленных уязвимостей в ГМИИ компаний OpenAI, Sber и Yandex на международную информационную безопасность, автор применял метод маскировки слов-триггеров, содержащихся в запросах, используя HTML-теги для форматирования текста. В результате обработки таких запросов защитные механизмы ГМИИ не смогли корректно распознать деструктивные намерения, что позволяло генерировать потенциально опасный контент.

ChatGPT от компании OpenAI, выступающая флагманом на рынке текстовых ГМИИ, продемонстрировала значительные успехи в обработке текстов и нахождении применения в самых разных отраслях. Однако при проведении исследования была выявлена уязвимость в защитных механизмах моделей ChatGPT-3.5, ChatGPT-4o и ChatGPT-4. С помощью промпт-инъекций

был получен доступ к опасной информации, такой как рецепты изготовления взрывных устройств и описание их применения в школьных учреждениях, инструкции по организации террористических актов, рекомендации для постов в социальных сетях, побуждающих к вождению в состоянии алкогольного опьянения, а также списки активационных ключей для Windows 10.

YandexGPT, разработанная российской компанией Yandex, проявила лучшую устойчивость к промпт-атакам по сравнению с ChatGPT. Например, при атаке, направленной на создание поста в социальных сетях, побуждающего к вождению в нетрезвом состоянии, YandexGPT продемонстрировал частичное сопротивление и в ряде случаев отказывался генерировать вредоносный контент. Однако модель всё же поддавалась атакам с применением специфических техник, что подтверждает необходимость дальнейшего совершенствования её защитных механизмов.

Графические генеративные модели также сталкиваются с аналогичными проблемами. Например, «Шедеврум» от Yandex показал устойчивость к прямым запросам на создание изображений, содержащих вирусную дезинформацию, таких как изображение Дональда Трампа в тюрьме, однако промпт-атаки с использованием HTML-тегов позволили обойти защитные механизмы, что привело к успешной генерации подобных изображений. В другом примере «Шедеврум» сгенерировал изображение террориста Ближнего Востока при запросе на теракт в школе, что потенциально может привести к выдвижению ближневосточными странами обвинений в предвзятости. В свою очередь, Kandinsky от компании Sber также показал свою уязвимость к промпт-атакам, например, при запросах на создание изображений с направленным на ребёнка оружием, сцен террористичнского акта 11 сентября или девочки с оружием в руках и кровью, модель смогла сгенерировать необходимые изображения лишь после применения промпт-атак.

Заключение. Таким образом, с целью снижения вероятности злонамеренного применения ГМИИ компаниям-разработчикам крайне рекомендуется значительно нарастить свои усилия в контексте предотвращения нецелевого использования своих продуктов, что в свою очередь, с одной стороны, неизбежно приведет к замедлению темпов и повышению стоимости разработки программных средств, но с другой – данный более ответственный подход способен многократно сократить потенциальный ущерб от действий злонамеренных акторов для всего мирового сообщества.

В то же время стратегия по обеспечению безопасной эксплуатации ИИ-продуктов представляет собой комплексную задачу, решение которой требует интеграции как технических, так и междисциплинарных подходов на локальном и глобальном уровнях. И компаниям-разработчикам, и международному сообществу в контексте обеспечения безопасности ИИ-решений необходимо проводить комплексную работу, основанную на принципах сотрудничества, что позволит минимизировать связанные с использованием ИИ риски и угрозы, а также создать безопасные и устойчивые системы, которые будут соответствовать интересам как конечного пользователя, так и мировой общественности в целом. Только синергия скоординированных усилий всех участников глобального диалога способна обеспечить защиту как от настоящих, так и будущих угроз, которые могут возникнуть в процессе использования ИИ-продуктов в условиях динамично изменяющейся ИКТ-среды.

Софья Андреевна Тюлякова,
Член Молодёжного совета Координационного центра доменов .RU/.РФ,
E-mail: sofya.tyulyakova@yandex.ru

Sofya A. Tyulyakova,
Member of Youth Council of the Coordination Center for TLD .RU/.РФ,
E-mail: sofya.tyulyakova@yandex.ru

СУВЕРЕНИТЕТ ДАННЫХ КАК ФАКТОР ФОРМИРОВАНИЯ ЦИФРОВОГО СУВЕРЕНИТЕТА ГОСУДАРСТВ

DATA SOVEREIGNTY AS A FACTOR IN THE FORMATION OF DIGITAL SOVEREIGNTY OF COUNTRIES

Аннотация. Суверенитет данных является значимым фактором обеспечения информационной безопасности государств. Такие переменные, как глобальная база пользователей, удаленные работники и облачные центры хранения данных, делают первоначальную концепцию намного более сложной. Из-за этого такие факторы, как местонахождение данных, где они собираются и как они собираются, имеют важное значение для обеспечения информационного суверенитета как части национальной безопасности.

Abstract. Data sovereignty is a significant factor in ensuring the information security of States. Variables such as the global user base, remote workers, and cloud storage centers make the initial concept much more complex. In this regard, factors such as the location of data, where it is collected and how it is collected are important to ensure information sovereignty as part of national security.

Ключевые слова: информационный суверенитет, цифровизация, цифровой суверенитет, данные, управление интернетом, национальная безопасность.

Key words: information sovereignty, digitalization, digital sovereignty, data, Internet governance, national security.

Концепция суверенитета данных находится в стадии формирования, однако уже играет значительную роль в формировании цифрового

суверенитета государств. Суверенитет данных можно определить как концепцию, согласно которой обеспечение сохранности данных подчиняется законам и правилам юрисдикции, в которой находятся их субъекты. В целом правила суверенитета данных возлагают ответственность за управление и защиту пользовательских данных на организацию, которая их собирает и обрабатывает.

Основой суверенитета данных как части технологического суверенитета является концепция контроля, в рамках которой правительства заботятся о защите конфиденциальных личных и деловых данных, а также о сохранении контроля над данными, которые могут иметь последствия для национальной безопасности. Перечень таких данных в каждой юрисдикции различен, в частности к ним относятся сведения о государственной тайне, военной и правоохранительной деятельности, профессиональной, коммерческой деятельности, персональные данные граждан.

Говоря об обеспечении суверенитета данных важно учитывать резиденцию и локализацию данных (таблица 1).

Таблица 1 – Разграничение основных понятий регулирования оборота данных

Суверенитет данных	**Локализация данных**	**Резиденция данных**
Правовой надзор за данными на основе нормативных актов страны, где они генерируются и/или обрабатываются.	Концепция, согласно которой данные, полученные гражданами региона, должны храниться в этой юрисдикции до их внешнего использования	Физическое место, где организация хранит и/или обрабатывает свои данные.

Все компании, выступающие операторами персональных данных граждан РФ, обязаны хранить персональных данные только на файловых серверах, физически расположенных на территории России [2]. К тому же, российское законодательство предусматривает особый порядок трансграничной передачи персональных данных. Согласно нему, оператор может осуществить передачу таких данных иностранным лицам только с уведомлением уполномоченного органа государственной власти.

Компании, которые собирают и хранят данные, должны учитывать законы о суверенитете данных всех стран, в которых они работают, и эта работа может включать хранение данных в определенных местах, реализацию мер безопасности и контроль за тем, чтобы данные обрабатывались в соответствии с местными правилами. Это может быть сложным и трудным процессом, особенно для многонациональных компаний, которые работают в нескольких юрисдикциях.

Набирающие популярность облачные вычисления позволяют организациям хранить и обрабатывать данные на удаленных серверах, поддерживаемых сторонними поставщиками. Однако именно здесь возникают проблемы с суверенитетом данных из-за возможности хранения данных в разных географических точках в соответствии с законами и правилами юрисдикций.

Многие национальные юрисдикции описывают меры по обеспечению суверенитета данных в своих стратегиях кибербезопасности (информационной безопасности). Организациям предлагается разрабатывать архитектуру безопасности, направленную на поддержание высокой доступности сервисов, внедрять защитные меры контроля доступа: многофакторную аутентификацию и управление привилегированным доступом, а также использовать SaaS-решения, адаптированных к киберландшафту региона.

В рамках управления глобальным Интернетом значимым документом в формировании суверенитета данных стал Общий регламент по защите данных

ЕС [3], установивший, что организации должны собирать и обрабатывать персональные данные только юридически разрешенными способами, включая согласие субъекта, договорные обязательства или общественный интерес в официальном органе власти. Аналогичные требования были включены в регулирование большинства юрисдикций, что потребовало пересмотра политик конфиденциальности онлайн-сервисов.

Одним из ключевых последствий формирования суверенитета данных является затруднение глобального потока данных и обмена информацией, что создаёт негативный эффект для развития международной торговли, бизнеса и противодействия интернациональной киберпреступности.

Несмотря на данное значимое последствие, концепция суверенитета данных будет развиваться в силу растущей деглобализации и ускоренного формирования цифрового суверенитета государств. Несомненно, на физическом уровне происходят утечки, регистрируются факты кибершпионажа, однако рассматриваемая концепция позволяет государствам охранять критически значимую информацию и персональные данные в правовой плоскости.

Утекшая информация может представлять по истине катастрофические последствия для национальной безопасности. Иностранным спецслужбам необязательно получать полную информацию, чтобы составить представления об экономический, политической или военной обстановке. Зачастую хватает фрагментированных данных об отдельных социальных стратах, чтобы образовать серьёзную угрозу противнику [1]. В этой связи государствам необходимо:

— проводить гигиену и защиту собираемых государством данных;

— уменьшать сбор и накопление данных в одном месте (в противном случае это позволит, атаковав одно место, получить массивы необходимых данных);

— контролировать потоки данных, отправляемых «наружу» (визы, билеты, страховки и т.п.)

— организовать просветительскую деятельность среди граждан в области цифровой гигиены

— классифицировать данные в новом формате (не присваивая всей важной информации принятые грифы секретности), а выстаивать из них цепочки данных и измерять вес в зависимости от их положения;

— методы разведки по открытым источникам (OSINT) трансформировать в сторону защиты данных. Если наш специалист ходит по определенной цепочке сбора данных и строит по ним портрет личности, тоже самое может сделать и противник, поэтому необходимо изменить логику организации информации в информационном поле.

Список источников и литературы:

1. Стратегия [Текст] / А. Свечин. − Москва : Государственное военное издательство, 1926. – С. 216.

2. Федеральный закон от 27 июля 2006 г. N 152-ФЗ «О персональных данных». Формат доступа: http://www.kremlin.ru/acts/bank/24154 (дата обращения: 11.10.2024).

3. General Data Protection Regulation. Regulation (EU) 2016/679. Available at: https://gdpr-info.eu/ (Access: 11.10.2024).

Научное издание

БЮЛЛЕТЕНЬ
II МЕЖДУНАРОДНОЙ МОЛОДЕЖНОЙ КОНФЕРЕНЦИИ
ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Сборник тезисов

Научный руководитель:
Карпович Олег Геннадьевич
доктор юридических наук, доктор политических наук, профессор,
и.о. проректора по экспертно-аналитической работе – руководитель Института актуальных международных проблем Дипломатической академии МИД России

Ответственные редакторы:
Мартиросян Аревик Жораевна *– кандидат юридических наук, мл.научный сотрудник Института актуальных международных проблем Дипломатической академии МИД России, член Совета молодых ученых Дипломатической академии МИД России, Российской Ассоциации международного права и Молодежного совета Координационного центра доменов.RU/.РФ*

Шангараев Руслан Насимович *– доктор политических наук, кандидат экономических наук, доцент, профессор кафедры стратегических коммуникаций и государственного управления Дипломатической академии МИД России, профессор Академии военных наук, главный редактор журнала «Вестник ученых-международников»*

ISBN-978-5-6052665-5-6