

СБОРНИК ДОКЛАДОВ УЧАСТНИКОВ  
XVI МЕЖДУНАРОДНОГО ФОРУМА

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



19-21 СЕНТЯБРЯ 2022 г.,  
МОСКВА, РОССИЯ



СБОРНИК ДОКЛАДОВ УЧАСТНИКОВ  
XVI МЕЖДУНАРОДНОГО ФОРУМА

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

19–21 СЕНТЯБРЯ 2022 г.  
МОСКВА, РОССИЯ

# АННОТАЦИЯ

В сборнике представлена основная часть выступлений участников XVI международного Форума «Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности», проведенного в г. Москве в период с 19 по 21 сентября 2022 г<sup>1</sup>.

Форум, организованный Национальной Ассоциацией международной информационной безопасности (далее — НАМИБ), был посвящен обсуждению приоритетных направлений экспертной проработки проблем сотрудничества государств в использовании ИКТ-среды и путей их решения для обеспечения международного мира, и экономического процветания государств мира. В рамках Форума состоялось пленарное заседание, на котором были рассмотрены современные проблемы обеспечения международного мира и поддержания устойчивого развития в глобальном информационном обществе.

Проведено пять круглых столов, на которых эксперты обсудили следующие вопросы:

- обеспечение суверенитета государств в ИКТ-среде;
- обеспечение безопасности объектов критической информационной инфраструктуры;
- противодействие использованию ИКТ для распространения идеологии неонацизма;
- формирование международного правового режима предотвращения конфликтов и противодействия преступности в ИКТ-среде;
- региональное сотрудничество в системе международной информационной безопасности с ближайшими партнерами, государствами-участниками ОДКБ, СНГ, ШОС, БРИКС и другими международными площадками.

Форум проходил в условиях возрастания риска возникновения масштабной конфронтации в цифровой сфере. Несмотря на огромные усилия, которые прилагает международное сообщество для предметного изучения проблем международной информационной безопасности (МИБ), напряжение в отношениях между государствами в области безопасности использования ИКТ не уменьшается. Сохраняются противоречия в подходах государств к определению приоритетов в противодействии угрозам МИБ.

В представленных в Сборнике докладах участников Форума уделено существенное внимание обсуждению проблем налаживания государственно-частного партнерства при обеспечении безопасности объектов критической инфраструктуры, включая объекты кредитно-финансовой сферы, а также проблем безопасности использования ИКТ-среды коммерческими компаниями. Отмечена важность обсуждения имеющихся в этой области проблем с использованием опыта обеспечения информационной безопасности, накопленного коммерческими организациями. Подтверждена актуальность расширения сотрудничества представителей международного экспертного сообщества в поиске средств противодействия угрозам использования ИКТ в военно-политических целях. Высказана заинтересованность в более широком обсуждении вопросов применения права к обеспечению свободы волеизъявления граждан в процессе национальных выборов. Была подчеркнута важность изучения путей парирования возможного негативного влияния использования ИКТ на сохранение цивилизационных ценностей общества, а также необходимость активизации разъяснения российских подходов к решению проблем МИБ. Отмечена задача совершенствования деятельности высших учебных заведений страны по подготовке кадров в области международной информационной безопасности.

В работе Форума, проходившего в комбинированном формате — онлайн и офлайн — приняли участие 260 экспертов из 43 государств и ряда международных организаций. (ШОС, ООН, Азербайджан, Ангола, Аргентина, Армения, Белоруссия, Бенин, Бразилия, Бурунди, Венесуэла, Вьетнам, Гана, Египет, Индия, Индонезия, Иордания, Иран, Казахстан, Камбоджа, КНДР, КНР, Конго, Куба, Лаос, Мали, Мьянма, Никарагуа, ОАЭ, Пакистан, РФ, Саудовская Аравия, Сейшельские острова, Сербия, Сирия, Судан, США, Тайланд, Того, Узбекистан, Уругвай, Франция, Эфиопия, ЮАР, Южная Осетия). Перевод докладов зарубежных участников на русский язык для сборника осуществлен сотрудником НАМИБ Е. Осечкиным.

*Оргкомитет XVI международного Форума «Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности»*

ISBN 978-5-6044055-4-3

<sup>1</sup> Ряд выступавших участников не представили тезисы своих выступлений



## **ПРИВЕТСТВИЕ ОРГАНИЗАТОРАМ, УЧАСТНИКАМ И ГОСТЯМ ШЕСТНАДЦАТОГО МЕЖДУНАРОДНОГО ФОРУМА «ПАРТНЕРСТВО ГОСУДАРСТВА, БИЗНЕСА И ГРАЖДАНСКОГО ОБЩЕСТВА ПРИ ОБЕСПЕЧЕНИИ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»**

Уважаемые организаторы, участники и гости Международного форума «Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности»!

Национальная Ассоциация международной информационной безопасности в очередной раз собирает ведущих российских и зарубежных экспертов для обсуждения ключевых проблем безопасности в информационной сфере и поиска оптимальных решений в интересах формирования системы обеспечения международной информационной безопасности.

В центре внимания Шестнадцатого форума — актуальные вопросы построения многополярного мира в глобальной ИКТ-среде, обеспечения ее безопасности и стабильности.

Программа форума традиционно нацелена на поиск эффективных решений, направленных на предотвращение межгосударственных конфликтов в глобальном информационном пространстве. Дискуссионные площадки, по основным направлениям профильного сотрудничества предоставляют возможность его участникам обменяться опытом противодействия нарастающим вызовам и угрозам в информационной сфере и укрепить взаимодействие заинтересованных сторон.

Новыми обсуждаемыми направлениями форума 2022 года станут проблематика защиты суверенитета государств и национальных духовных ценностей, а также развития регионального сотрудничества в интересах формирования системы обеспечения международной информационной безопасности.

Практическая ориентированность тематических круглых столов и экспертных дискуссий по наиболее важным вопросам обеспечения безопасности глобального информационного пространства стали визитной карточкой форума, заслуженно сделав его одной из самых авторитетных международных площадок.

Полагаю, что выработанные участниками форума подходы к обеспечению международной информационной безопасности получат практическое применение при рассмотрении данной проблематики на профильных площадках Организации Объединенных Наций, БРИКС, ШОС, СНГ, ОДКБ, ОБСЕ, Регионального форума АСЕАН по безопасности, других международных организаций.

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

Желаю всем успешной и плодотворной работы!

*Сопредседатель Оргкомитета,  
заместитель Секретаря Совета Безопасности  
Российской Федерации*



О. ХРАМОВ

# СОДЕРЖАНИЕ

## ПЛЕНАРНОЕ ЗАСЕДАНИЕ

### **В.П. Шерстюк**

Сопредседатель оргкомитета Форума, советник Секретаря Совета Безопасности Российской Федерации, Президент Национальной Ассоциации международной информационной безопасности ..... 10

### **О.В. Сыромолотов**

Заместитель Министра иностранных дел России ..... 14

### **С.М. Бойко**

Начальник департамента проблем безопасности в информационной сфере аппарата Совета Безопасности Российской Федерации  
О ПЕРСПЕКТИВАХ ВЫРАБОТКИ ЮРИДИЧЕСКИ ОБЯЗАТЕЛЬНЫХ НОРМ РЕГУЛИРОВАНИЯ ДЕЯТЕЛЬНОСТИ ГОСУДАРСТВ В ИНФОРМАЦИОННОМ ПРОСТРАНСТВЕ ..... 16

### **В.А. Уваров**

Директор Департамента информационной безопасности, Центробанк России ..... 19

### **Чен Гопин**

Начальник Департамента, Китайское общество дружбы с зарубежными странами ..... 23

### **Г.С. Логвинов**

Заместитель Генерального секретаря ШОС ..... 24

### **С.К. Кузнецов**

Заместитель председателя правления ПАО Сбербанк ..... 27

### **Д.И. Григорьев**

Вице-президент по информационной безопасности ПАО «ГМК «Норильский никель»  
НОВЫЕ ВЫЗОВЫ В ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЛЯ ПРОМЫШЛЕННЫХ КОМПАНИЙ:  
ОПЫТ «НОРНИКЕЛЯ» ..... 30

### **В.О. Запивахин**

Министерство обороны, эксперт  
ОБ УЧАСТИИ МИНОБОРОНЫ РОССИИ В ФОРМИРОВАНИИ МЕЖДУНАРОДНО-ПРАВОВОГО РЕЖИМА ПРЕДОТВРАЩЕНИЯ КОНФЛИКТОВ В ГЛОБАЛЬНОМ ИНФОРМАЦИОННОМ ПРОСТРАНСТВЕ ..... 33

### **О.С. Макаров**

Директор Белорусского института стратегических исследований ..... 35

### **А.В. Крутских**

Специальный представитель Президента Российской Федерации по вопросам международного сотрудничества в области информационной безопасности, советник Министра иностранных дел ..... 37

### **Н.Н. Мурашов**

Заместитель директора Национального координационного центра по компьютерным инцидентам  
ПРОТИВОБОРСТВО КИБЕРУГРОЗАМ В СОВРЕМЕННЫХ УСЛОВИЯХ ..... 42

### **Маурисио Ленин Соза Рубело**

Национальная полиция (Никарагуа) ..... 45

### **А.Г. Оганесян**

Главный редактор журнала «Международная жизнь» МИД России, член президиума НАМИБ ..... 48

### **Санджай Гоэл**

Государственный университет штата Нью-Йорк (США)  
НЕОБХОДИМОСТЬ СОТРУДНИЧЕСТВА В КИБЕРПРОСТРАНСТВЕ, НЕСМОТРЯ НА СРЕМИТЕЛЬНО  
ОБОСТРЯЮЩИЕСЯ КОНФЛИКТЫ МЕЖДУ ГОСУДАРСТВАМИ ..... 51

### **В.Н. Бенгин**

Директор департамента кибербезопасности, Минцифры России ..... 53

### **С.В. Плохов**

Заместитель начальника Главного управления международно-правового сотрудничества — начальник организационно-правового управления, Генеральная прокуратура РФ  
О МЕЖДУНАРОДНОМ СОТРУДНИЧЕСТВЕ ГЕНЕРАЛЬНОЙ ПРОКУРАТУРЫ РОССИЙСКОЙ ФЕДЕРАЦИИ В СФЕРЕ ПРОТИВОДЕЙСТВИЯ ИНФОРМАЦИОННОЙ ПРЕСТУПНОСТИ ..... 55

### **Филипп Бомард**

Штатный профессор университета, директор лаборатории оборонной разведки безопасности (ESR3C)  
ЭКОНОМИЧЕСКАЯ ВОЙНА В СОЧЕТАНИИ С ВОЕННОЙ ЭКОНОМИКОЙ: БАЛАНС МЕЖДУ  
СТРАТЕГИЧЕСКОЙ БЕЗОПАСНОСТЬЮ И КИБЕРСТАБИЛЬНОСТЬЮ ..... 58

**О.Г. Карпович**

д.ю.н., д.полит.н., профессор, проректор по научной работе Дипломатической академии МИД России  
ВСЕМИРНАЯ ПАУТИНА: ПОПЫТКИ «ОТМЕНИТЬ» РОССИЮ. . . . . 60

**КРУГЛЫЙ СТОЛ № 1****ОБЕСПЕЧЕНИЕ СУВЕРЕНИТЕТА ГОСУДАРСТВ В ГЛОБАЛЬНОЙ ИКТ-СРЕДЕ****А.А. Стрельцов**

д.т.н., д.ю.н., профессор, член-корреспондент Академии криптографии РФ, вице-президент НАМИБ  
ВНЕШНЯЯ И ВНУТРЕННЯЯ ФОРМЫ ПРОЯВЛЕНИЯ СУВЕРЕНИТЕТА ГОСУДАРСТВА В ИКТ-СРЕДЕ. . . . . 66

**Т.А. Полякова**

д.ю.н., профессор, главный научный сотрудник, и.о. заведующего сектором информационного права и международной информационной безопасности Института государства и права РАН, Заслуженный юрист Российской Федерации

**А.А. Смирнов**

к.ю.н., доцент, старший научный сотрудник сектора информационного права и международной информационной безопасности Института государства и права РАН  
ПРОБЛЕМЫ ИМПЛЕМЕНТАЦИИ ДОБРОВОЛЬНЫХ И НЕОБЯЗАТЕЛЬНЫХ НОРМ ОТВЕТСТВЕННОГО ПОВЕДЕНИЯ ГОСУДАРСТВ В ИКТ-СРЕДЕ В НАЦИОНАЛЬНОЕ ЗАКОНОДАТЕЛЬСТВО . . . . . 69

**Е.С. Зиновьева**

д.п.н., профессор, заместитель директора Центра международной информационной безопасности и научно-технологической политики МГИМО МИД России  
АКТУАЛЬНЫЕ ТЕНДЕНЦИИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОГО СУВЕРЕНИТЕТА В МНОГОПОЛЯРНОМ МИРЕ . . . . . 73

**Г.Г. Шинкарецакая**

д.ю.н., главный научный сотрудник Института государства и права РАН  
СУВЕРЕНИТЕТ ГОСУДАРСТВА В КИБЕРПРОСТРАНСТВЕ . . . . . 76

**П.У. Кузнецов**

д.ю.н., профессор, заведующий кафедрой информационного права Уральского государственного юридического университета  
ОТДЕЛЬНЫЕ МЕТОДОЛОГИЧЕСКИЕ АСПЕКТЫ ПРАВОВОГО ОБЕСПЕЧЕНИЯ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В КОНТЕКСТЕ ЖИЗНЕОБЕСПЕЧЕНИЯ ЧЕЛОВЕКА . . . . . 80

**А.В. Морозов**

д.ю.н., профессор, академик РАЕН, профессор кафедры компьютерного права и информационной безопасности МГУ им. М.В. Ломоносова  
ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ ПОДГОТОВКИ КАДРОВ ВЫСШЕЙ КВАЛИФИКАЦИИ В ОБЛАСТИ ПРАВОВОГО ОБЕСПЕЧЕНИЯ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. . . . . 83

**А.С. Марков**

д.т.н., президент АО «НПО »Эшелон», профессор МГТУ им. Н.Э. Баумана, профессор Финансового университета при Правительстве РФ  
ПРОБЛЕМНЫЕ ВОПРОСЫ ПОВЫШЕНИЯ ДОСТОВЕРНОСТИ ИДЕНТИФИКАЦИИ РЕСУРСОВ КРИТИЧЕСКИ ВАЖНОЙ ИНФРАСТРУКТУРЫ. . . . . 86

**А.К. Жарова**

д.ю.н., старший научный сотрудник сектора уголовного права, уголовного процесса и криминологии Института государства и права РАН  
ПРАВОВОЕ ОБЕСПЕЧЕНИЕ АТРИБУЦИИ КИБЕРАТАК . . . . . 92

**Н.П. Ромашкина**

к.п.н., профессор, Центр международной безопасности Института мировой экономики и международных отношений имени Е. М. Примакова (ИМЭМО) РАН  
ФОРМИРОВАНИЕ МЕЖДУНАРОДНО-ПРАВОВОГО РЕЖИМА ПРЕДОТВРАЩЕНИЯ КОНФЛИКТОВ В ГЛОБАЛЬНОМ ИНФОРМАЦИОННОМ ПРОСТРАНСТВЕ: НОВЫЙ ФОРМАТ . . . . . 94

**А.А. Морозов**

к.ю.н., эксперт в области международной информационной безопасности  
ПРАВОВОЙ АСПЕКТ ОПРЕДЕЛЕНИЯ ГРАНИЦ ИНФОРМАЦИОННОГО ПРОСТРАНСТВА В СФЕРЕ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ . . . . . 99

**Е.М. Скворцова**

Эксперт Министерства обороны Российской Федерации  
К ВОПРОСУ ОБ УГРОЗАХ СУВЕРЕНИТЕТУ В ИКТ-СРЕДЕ: ОТРИЦАНИЕ КОНЦЕПЦИИ, ПОЛИТИЧЕСКАЯ АТРИБУЦИЯ И КИБЕРСАНКЦИИ . . . . . 102

**А.Н. Курбацкий**

Белорусский государственный университет  
СУВЕРЕНИТЕТ И МОЛОДЕЖЬ . . . . . 105



## КРУГЛЫЙ СТОЛ № 2

### ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

#### А.В. Чичилимов

Главный советник ДМИБ МИД России

РОССИЙСКИЕ ПОДХОДЫ К ВОПРОСАМ ЗАЩИТЫ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ  
ИНФРАСТРУКТУРЫ В КОНТЕКСТЕ РЕАЛИЗАЦИИ МЕР УКРЕПЛЕНИЯ ДОВЕРИЯ В ИНФОРМАЦИОННОМ  
ПРОСТРАНСТВЕ НА ПРИМЕРЕ ОБСЕ ..... 110

#### Тимур Аитов

к.ф.-м.н., зампред комиссии по цифровым финансовым технологиям Совета ТППРФ

Совета ТППРФ по финансово-промышленной и инвестиционной политике

ЦИФРОВАЯ ЭКОНОМИКА В УСЛОВИЯХ САНКЦИЙ. СТРАТЕГИИ ПРОРЫВА ..... 114

#### А.Ю. Ярных

Эксперт АО «Лаборатория Касперского»

КОНСТРУКТИВНАЯ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ..... 118

#### П.Л. Пилюгин

к.т.н., Центр проблем информационной безопасности ВМК МГУ им. М.В. Ломоносова

О МНОГОУРОВНЕВОЙ ПОЛИТИКЕ БЕЗОПАСНОСТИ ПРИМЕНительно К КРИТИЧЕСКОЙ  
ИНФРАСТРУКТУРЕ ..... 122

#### Джон К. Мэллори

Массачусетский технологический университет, США

ВОЕННАЯ КИБЕРСТАБИЛЬНОСТЬ И КРИТИЧЕСКАЯ ИНФОРМАЦИОННАЯ ИНФРАСТРУКТУРА ..... 125

## КРУГЛЫЙ СТОЛ № 3

### ПРОТИВОДЕЙСТВИЕ ИСПОЛЬЗОВАНИЮ ИКТ ДЛЯ РАСПРОСТРАНЕНИЯ ИДЕОЛОГИИ НЕОНАЦИЗМА

#### С.В. Коротков

к.в.н., генерал-майор, начальник аналитического отдела НАМИБ

О НЕОНАЦИЗМЕ КАК УГРОЗЕ НАЦИОНАЛЬНОЙ И МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ  
БЕЗОПАСНОСТИ. .... 128

## КРУГЛЫЙ СТОЛ № 4

### ФОРМИРОВАНИЕ МЕЖДУНАРОДНОГО ПРАВОВОГО РЕЖИМА ПРЕДОТВРАЩЕНИЯ КОНФЛИКТОВ И ПРОТИВОДЕЙСТВИЯ ПРЕСТУПНОСТИ В ИКТ-СРЕДЕ

#### Э.В. Чернухин

Начальник отдела ДМИБ МИД России

ФОРМИРОВАНИЕ МЕЖДУНАРОДНО-ПРАВОВОГО РЕЖИМА ПРОТИВОДЕЙСТВИЯ ПРЕСТУПНОСТИ  
В ИКТ-СРЕДЕ. .... 134

#### Ю.А. Ясносокирский

Начальник отдела ООН и глобальных форматов ДМИБ МИД России

АТРИБУЦИЯ КОМПЬЮТЕРНЫХ АТАК: ДУБИНА ИЛИ СРЕДСТВО МИРОВОЙ ПОЛИТИКИ ..... 136

#### Л.А. Осадчая

Представитель Национального центрального бюро Интерпола, МВД России

ОБ УЧАСТИИ НЦБ ИНТЕРПОЛА МВД РОССИИ В БОРЬБЕ С МЕЖДУНАРОДНОЙ КИБЕРПРЕСТУПНОСТЬЮ. .... 138

#### Т.А. Абрегов

Старший прокурор отдела Управления по надзору за исполнением законов о федеральной

безопасности, межнациональных отношениях, противодействии экстремизму и терроризму

Генеральной прокуратуры Российской Федерации

ПРОТИВОДЕЙСТВИЕ ПРОЯВЛЕНИЯМ ЭКСТРЕМИЗМА И ТЕРРОРИЗМА В СЕТИ «ИНТЕРНЕТ».

ЗАКОНОДАТЕЛЬНОЕ РЕГУЛИРОВАНИЕ ВОПРОСОВ ОГРАНИЧЕНИЯ ДОСТУПА К ИНФОРМАЦИИ. .... 140

#### Н.М. Гудков

Старший прокурор Главного управления по надзору за следствием, дознанием и оперативно-разыскной

деятельностью Генпрокуратуры России

СОВРЕМЕННЫЕ УГРОЗЫ ИСПОЛЬЗОВАНИЯ ВЫСОКИХ ТЕХНОЛОГИЙ В ПРЕСТУПНЫХ ЦЕЛЯХ

И ПРИНИМАЕМЫЕ МЕРЫ ПО ПРОТИВОДЕЙСТВИЮ ПОСЯГАТЕЛЬСТВАМ В УКАЗАННОЙ СФЕРЕ ..... 142

#### А.А. Вураско

Руководитель группы развития специальных сервисов ООО «Ростелеком-Солар»

НОВЫЕ РЕАЛИИ: ВЛИЯНИЕ ГЕОПОЛИТИЧЕСКОЙ ОБСТАНОВКИ НА ЛАНДШАФТ КИБЕРУГРОЗ

В РОССИИ В КРАТКОСРОЧНОЙ И ДОЛГОСРОЧНОЙ ПЕРСПЕКТИВАХ. .... 146

#### М.Л. Немсадзе

Заместитель начальника отдела международного сотрудничества в области безопасности Департамента

международного права и сотрудничества Минюста России

МЕЖДУНАРОДНО-ПРАВОВЫЕ МЕХАНИЗМЫ СОТРУДНИЧЕСТВА В ОБЛАСТИ БОРЬБЫ

С ИНФОРМАЦИОННОЙ ПРЕСТУПНОСТЬЮ И ПЕРСПЕКТИВЫ ИХ СОВЕРШЕНСТВОВАНИЯ ..... 150



## КРУГЛЫЙ СТОЛ № 5

### РАЗВИТИЕ РЕГИОНАЛЬНОГО СОТРУДНИЧЕСТВА В СИСТЕМЕ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

#### О.С. Лобанова

Атташе ДМИБ МИД России

О ПРОДВИЖЕНИИ РОССИЙСКИХ ПОДХОДОВ ПО МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ПРОФИЛЬНЫХ РЕГИОНАЛЬНЫХ ПЛОЩАДКАХ . . . . . 154

#### Д.Б. Фролов

Советник генерального директора ФГУП «Российская телевизионная и радиовещательная сеть» (РТПС), зав. базовой кафедрой РТПС «Цифровое телерадиовещание и информационная безопасность» ИПК МТУСИ ДИПФЕЙКИ И ВОПРОСЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В МЕЖДУНАРОДНОМ И РЕГИОНАЛЬНОМ АСПЕКТАХ . . . . . 157

#### В.А. Педанов

Генеральный директор ООО «Технологии безопасности транспорта», представитель Группы компаний «Инжиниринговые Технологии» в АСЕАН

АКТУАЛЬНЫЕ ПРОБЛЕМЫ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В АСЕАН . . . . . 160

#### А.Ж. Мартиросян

Научный сотрудник Института актуальных международных проблем, аспирант Дипломатической академии МИД России, руководитель Школы международной информационной безопасности Дипломатической академии

РЕГИОНАЛИЗАЦИЯ КАК ТЕНДЕНЦИЯ ФОРМИРУЮЩЕЙСЯ СИСТЕМЫ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. . . . . 169

#### И.В. Сурма

к.э.н., заведующий кафедрой государственного управления во внешнеполитической деятельности Дипломатической академии МИД России, член-корреспондент РАЕН, член экспертно-консультационного совета СФ РФ

«ЦИФРОВОЙ РЕАЛИЗМ» И ПОСТНЕОКОЛОНИАЛИЗМ: ПЕРСПЕКТИВЫ И ВЫЗОВЫ СУВЕРЕНИТЕТУ ГОСУДАРСТВА . . . . . 171

#### Бай Яцзе

Эксперт МГИМО МИД России (Китай)

КИБЕРВОЙНА ЗАПАДА НА УКРАИНЕ — НОВЫЕ ТЕХНОЛОГИИ ПО СТАРЫМ ЛЕКАЛАМ. . . . . 174

#### С.М. Аль-Сахель

Эксперт МГИМО МИД России (Иордания)

ВИРТУАЛЬНЫЙ УКРАИНСКИЙ ФРОНТ — ВЗГЛЯД ИЗ АРАБСКОГО МИРА . . . . . 176

#### В.И. Булва

Эксперт, помощник директора Центра международной информационной безопасности и научно-технологической политики МГИМО МИД России

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ МОЛОДЕЖИ В ИНФОРМАЦИОННОМ ПРОСТРАНСТВЕ В УСЛОВИЯХ ГЕОПОЛИТИЧЕСКОЙ ТРАНСФОРМАЦИИ . . . . . 179

# ПЛЕНАРНОЕ ЗАСЕДАНИЕ

**Ведущий:**

*Шерстюк В.П., президент НАМИБ*

## **В.П. Шерстюк**

*Сопредседатель оргкомитета  
Форума, советник Секретаря Совета  
Безопасности Российской Федерации,  
Президент Национальной Ассоциации  
международной информационной  
безопасности*

Уважаемые участники международного Форума!

Уважаемые гости!

Дамы и господа!

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

Хотелось бы начать со слов искренней признательности всем участникам и гостям Форума. Несмотря на сложную международную обстановку, беспрецедентные антироссийские санкции и продолжение пандемии коронавирусной инфекции COVID-19 вам удалось найти возможность принять участие в работе Форума. Третий год подряд мы встречаемся в г. Москве, в здании Дипломатической академии МИД России. В этой связи хотелось бы поблагодарить руководителей Академии и, прежде всего, ректора — Чрезвычайного и Полномочного посла Российской Федерации Александра Владимировича Яковенко, а также сотрудников Академии за огромную практическую помощь в подготовке Форума.

Наш Форум имеет свою историю. Ежегодно, в течение 16 лет мы собираемся для того, чтобы обсуждать проблемы международной информационной безопасности и пути их решения. Наша многолетняя совместная работа принесла свои плоды. Она, в определенной степени, способствовала тому, что международное экспертное сообщество, по существу, перешло от обсуждения актуальности противодействия угрозам злонамеренного и вредоносного использования информационно-компьютерных технологий (ИКТ) к обсуждению возможных направлений сотрудничества в противодействии этим угрозам.

ИКТ-среда — это особая среда. Ее исключительность обусловлена существенными отличиями от традиционных пространств международного сотрудничества — суши, моря, воздушного и космического пространства.



Во-первых, в ИКТ-пространстве отсутствуют общепризнанные границы, которые, в общем-то, не совпадают с географическими.

Во-вторых, отсутствует закреплённый в источниках права международный режим безопасности объектов ИКТ-среды: коммуникационных и вычислительных устройств, информационных систем ИКТ и информационной инфраструктуры.

В-третьих, отсутствуют правовые механизмы проведения расследований по инцидентам, связанным со злонамеренным использованием ИКТ.

Сегодня становится все более очевидным, что только международное право, учитывающее специфику информационно-коммуникационных технологий и регулирующее на нормативной основе деятельность государств в глобальном информационном пространстве может составить основу системы противодействия угрозам международной информационной безопасности.

В целях поиска путей увеличения потенциала международного права по регулированию международного сотрудничества в области безопасности ИКТ-среды (а именно эта тема вынесена на обсуждение на Круглом столе №1 форума) Еще в 2001 году Генеральной Ассамблеей ООН был дан старт работе Групп правительственных экспертов по достижениям в сфере информатизации и коммуникаций в контексте международной безопасности.

Усилиями этих рабочих органов удалось подготовить и принять консенсусом в 2015 и 2021 гг. предложения по нормам ответственного поведения государств в ИКТ-среде. По мнению международных экспертов, а мы разделяем это мнение, практическое применение разработанных норм может привести к снижению угрозы международному миру и стабильности. Как представляется, реализация этих ожиданий возможна лишь в случае, если в процессе применения норм все государства будут обладать равными возможностями для обеспечения национального суверенитета. С этой точки зрения представляется важным продолжение изучения рекомендаций по нормам ответственного поведения государств в ИКТ-среде, поддержанных резолюциями 70-й, 76-й сессий Генеральной Ассамблеи ООН. Возможность исследования этих рекомендаций включена в мандат Рабочей группы открытого состава ООН по вопросам безопасности в сфере использования информационно-коммуникационных технологий и самих ИКТ (2021–2025 гг.). Здесь мне приятно отметить, что в августе этого года Национальная ассоциация международной информационной безопасности официально аккредитована при Рабочей группе открытого состава ООН.

Ассоциацией к настоящему времени завершен первый этап фундаментальной научно-исследовательской работы по проблеме применения норм ответственного поведения государств в ИКТ-среде, основные результаты которой изложены в представленных раздаточных материалах Форума, опубликованы на сайте НАМИБ и предложены для обсуждения на третьей субстантивной сессии Рабочей группы открытого состава ООН.

К сожалению, отправить делегацию Ассоциации в Нью-Йорк (США) для представления полученных результатов на заседании третьей субстантивной сессии Рабочей группы открытого состава не удалось. Государственный департамент США без объяснения причин не выдал визы членам нашей делегации. На наш взгляд это является еще одним явным нарушением США международных обязательств как страны расположения центральных органов ООН, закрепленных Резолюцией Генеральной Ассамблеи ООН (1947 г). Полагаем такое поведение внешнеполитического ведомства США недопустимым.

Пользуясь трибуной Форума, обращаюсь к руководителю Рабочей группы открытого состава ООН господину Б. Гафуру с просьбой оказать содействие в создании нормальных и равных для всех условий работе в группе.

На обсуждение участников **Круглого стола № 2** (20 сентября) вынесена проблематика обеспечения безопасности объектов критической информационной инфраструктуры.

Эта тема традиционно является на наших Форумах одной из центральных. По мнению многих экспертов, за последние годы опасность злонамеренного и вредоносного использования информационных технологий для нанесения ущерба объектам критической информационной инфраструктуры, осуществления других социально опасных деяний возросла.

Существо обсуждаемой проблемы заключается в определении направлений адаптации норм и принципов международного права к регулированию отношений в области применения ИКТ и функционирования глобальной информационной инфраструктуры в рамках ИКТ-среды как нового пространства международного сотрудничества.

Адаптация норм и принципов международного права должна способствовать, с одной стороны, достижению устойчивого развития национальных обществ на основе использования потенциала ИКТ во всех сферах жизнедеятельности человека, а с другой — поддержанию международного мира и безопасности в условиях возникновения инцидентов в ИКТ-среде.

При этом, видимо, справедливо полагать, что международные инциденты в ИКТ-среде возникают, в основном, вследствие злонамеренной и вредоносной деятельности некоторых государств и иных субъектов против критически важной информационной инфраструктуры, направленной на достижение военных, террористических и преступных целей на национальном, региональном и глобальном уровнях.

В рамках адаптации норм и принципов международного права к применению в ИКТ-среде можно было бы внести ряд важных правовых новаций.

Во-первых, осуществить международное правовое закрепление границ зон ответственности государств в ИКТ-среде.

Во-вторых, уточнить международные обязательства государств в ИКТ-среде, вытекающие из норм и принципов международного права, а также обязательства, обусловленные применением норм ответственного поведения государств в ИКТ-среде.

В-третьих, определить содержание международного правового режима безопасности критически важной инфраструктуры.

Кроме того, представляется важным определить обязательства государств в области обмена информацией, оказания взаимопомощи, преследования лиц, виновных в террористическом и преступном использовании ИКТ, а также создания системы компетентных координаторов на политическом и техническом уровнях и определения порядка их взаимодействия в целях обеспечения безопасного использования и устойчивого функционирования ИКТ-среды.

На обсуждение участников **Круглого стола № 3** (20 сентября) вынесены вопросы противодействия использованию ИКТ для распространения идеологии неонацизма и экстремизма.

Как представляется, проблема заключается в осознании международным сообществом того, что пропаганда национальной исключительности в глобальном информационном обществе несовместима с обязательством государств развивать дружественные отношения между нациями (ст. 1 п. 2 Устава ООН) и может наносить ущерб международному миру и безопасности.

В настоящее время со стороны США и его союзников расширяется поддержка агрессивного национализма. Для этой цели создана и задействована сеть некоммерческих организаций, поддерживающих неонацизм, и гигантский сегмент интернет-ресурсов.

Для поддержания международной безопасности важно выработать приоритетные меры содействия реализации внешней политики в интересах формирования международной системы применения норм ответственного поведения государств в ИКТ-среде в целях противодействия распространению идеологии неонацизма и экстремизма.

На международном уровне следует обсудить целесообразность создания эффективного независимого процедурного механизма для справедливого судебного наказания за

киберпреступления, связанные с использованием информационно-коммуникационных технологий в интересах неонацистских организаций.

События на Украине сразу после начала СВО породили целый ряд глобальных вызовов в сфере ИКТ. Они носят как технологический, так и содержательный характер. Спровоцированная киевским режимом неонацистская риторика, отражающая экстремистскую идеологию, которая последние десятилетия усиленно культивировалось и поощрялась властями в украинском обществе, выплеснулась в мировую информационную сеть. Волна агрессивной русофобии была поддержана Западом на различных платформах и в социальных сетях. Эта поддержка выразилась как в форме жесткой цензуры любой альтернативной точки зрения, так и активными действиями по публикации и продвижению собственного контента агрессивного русофобского характера.

Следует отметить, что данная кампания, охватившая мировое медийное пространство, наносит ущерб не только душам людей, и чревата угрозой жизни и здоровья российским гражданам, и всем, кто выражает свою поддержку России или просто сочувственно относится к ней, вопреки соркестрованному Западом информационному «мейнстриму».

Участникам **Круглого стола № 4** (21 сентября) предлагается обсудить проблемы формирования международного правового режима предотвращения конфликтов и противодействия преступности в ИКТ-среде. Это обсуждение могло бы способствовать разработке всеобъемлющей международной конвенции о противодействии использованию ИКТ в преступных целях на базе уже предложенного российского проекта, а также содействовать успешной работе Специального межправительственного комитета экспертов открытого состава ООН.

Содействие со стороны экспертного сообщества деятельности Специального комитета, а также создание условий для последующего принятия государствами-членами ООН конвенции отнесены к одному из основных направлений реализации государственной политики Российской Федерации в области международной информационной безопасности.

На обсуждение участников **Круглого стола № 5** (21 сентября) выносится вопрос

развития регионального сотрудничества в системе международной информационной безопасности.

Как известно, в качестве приоритетного направления этой деятельности на заседании Совета безопасности Российской Федерации 26 марта 2021 года Президентом Российской Федерации В.В. Путиным обозначен диалог с нашими ближайшими партнерами по ОДКБ, СНГ, ШОС и БРИКС.

Как отметил глава государства, «Россия, как и прежде, открыта для диалога и конструктивного взаимодействия со всеми партнерами, причем как в двустороннем формате, так и на площадках международных структур и форумов, прежде всего, конечно, в Организации Объединенных Наций».

Развитию регионального сотрудничества будет способствовать проведение на регулярной основе двусторонних и многосторонних экспертных консультаций, согласование позиций и основных направлений сотрудничества в области обеспечения международной информационной безопасности с государствами-участниками СНГ, объединения БРИКС, государствами-членами ОДКБ, ШОС, АСЕАН, «Группы двадцати», другими государствами и международными организациями.

Укреплению региональной составляющей будет способствовать подписание межправительственных соглашений о сотрудничестве в области обеспечения международной информационной безопасности.

Развитию регионального сотрудничества активно способствуют двусторонние межведомственные консультации по вопросам совместного противодействия нарастающим вызовам и угрозам международной информационной безопасности, предотвращения межгосударственных конфликтов в глобальном информационном пространстве.

Уважаемые коллеги!

По данным Оргкомитета, желание участвовать в работе Форума высказали более 260 экспертов из 43 стран мира, из них порядка 150 примут участие в режиме видеоконференции, организованной на платформе Webinar.

Сегодня, здесь, в Актовом зале Дипломатической академии МИД России на пленарном заседании Форума присутствуют эксперты из 10 стран.

Мы приветствуем наших иностранных гостей, в их числе Заместителя Министра связи и информационных технологий Исламской республики Иран господина Амира Мохаммада Ладжеварди и посла Иорданского Хашимитского Королевства в России господина Халида Абдуллу Краиема Шавабха.

Позвольте заверить Вас, что организаторы Форума сделают все возможное для того, чтобы участники могли свободно и открыто обсуждать наиболее острые вопросы международного сотрудничества в области обеспечения безопасности использования глобальной ИКТ-среды как в интересах развития национальных государств, так и международного сообщества в целом.



## О.В. Сыромолотов

*Заместитель Министра иностранных дел  
России*

Уважаемые дамы и господа!

Рад приветствовать организаторов и участников XVI Международного форума «Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности».

Мероприятие имеет репутацию авторитетной площадки для обсуждения вопросов, связанных с обеспечением безопасности в сфере использования информационно-коммуникационных технологий. Форум становится все масштабнее, расширяется его тематический портфель, растет интерес к нему со стороны иностранных партнеров. Сегодня здесь присутствуют представители более 50 государств мира. Вижу в этом закономерный результат плодотворной работы организаторов — Национальной Ассоциации международной информационной безопасности и оказавших им содействие госструктур, в том числе МИД России.

Заявленная Оргкомитетом тема мероприятия — «Многополярный мир в глобальной ИКТ-среде» на фоне происходящей сейчас масштабной перестройки всей системы международных отношений является особенно актуальной. Как неоднократно отмечал Президент России В.В.Путин, «либерально-глобалистский американский эгоцентризм» уходит в прошлое, уступая место полицентричности, основанной на подлинном суверенитете народов и цивилизаций.

Эти процессы затрагивают и цифровую сферу.

Сегодня против России ведется настоящая война в информационном пространстве. Развязав ее, наши противники намеревались нанести непоправимый урон безопасности российского государства, экономике, системе госуправления и общественной стабильности. Недруги России просчитались. Отечественная информационная инфраструктура продемонстрировала высокую степень устойчивости.

Россия продолжает оставаться интеллектуальным лидером в продвижении тематики международной информационной безопасности на международной арене. По нашей



инициативе в 2021 г. в рамках ООН была запущена профильная Рабочая группа открытого состава. В качестве ключевых задач, стоящих перед этой структурой, отмечаем укрепление межправительственного сотрудничества по линии компетентных ведомств, выработку юридически обязывающих договоренностей в сфере ИКТ, наращивание технологического потенциала развивающихся стран.

В рамках Группы последовательно противостояим навязываемым Западом попыткам размывания межгосударственного характера переговорного процесса. Добились приемлемых для России и ее единомышленников параметров участия неправительственных субъектов в работе РГОС в сугубо консультативном статусе. Обеспечили возможность подключения к ней отечественных НПО — Национальной Ассоциации международной информационной безопасности, Школы МИБ при Дипломатической академии МИД России и Высшей школы экономики. Успехом стало принятие Группой первого ежегодного промежуточного доклада в июле текущего года.

Другая важная площадка, созданная по инициативе нашей страны под эгидой ООН — Спецкомитет по разработке всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях. За состоявшиеся с начала года три субстантивные сессии сторонам уже удалось



согласовать структуру будущего документа, план и порядок его разработки, провести первое обсуждение всех его глав. Рассчитываем, что мандат Спецкомитета будет выполнен в срок и столь важная для мирового сообщества конвенция будет принята уже в 2024 году.

Последовательно придерживаемся курса на интернационализацию управления Интернетом и равноправное участие всех стран в этом процессе, сохранение суверенного права государств регулировать национальный сегмент глобальной сети. В данном контексте считаем принципиальным обеспечить выполнение Тунисской программы 2005 г. Всемирной встречи на высшем уровне по информационному обществу. Отмечаем недопустимость попыток фрагментации Всемирной сети через создание келейных форматов управления ею с ограниченным составом участников.

Энергично продвигаем наши подходы в Международном союзе электросвязи, Всемирном почтовом союзе. Взаимодействуем с союзниками как в рамках региональных объединений — СНГ, ШОС, БРИКС, АСЕАН, ЛАГ, Африканский союз — так и на двусторонней

основе. За неполные три года заключено семь соответствующих межправительственных соглашений — с Азербайджаном, Арменией, Индонезией, Ираном, Киргизией, Никарагуа и Узбекистаном.

Свой весомый экспертный вклад в эту комплексную работу, без сомнения, вносит Национальная Ассоциация международной информационной безопасности и ежегодно проводимый ею Форум.

Убежден, что предстоящая трехдневная дискуссия станет плодотворной. Продолжит сложившиеся в предыдущие годы традиции предметного обсуждения наиболее актуальных вопросов обеспечения международной информационной безопасности. Позволит участникам обменяться опытом противодействия нарастающим вызовам и угрозам в информационной сфере, а также будет способствовать укреплению взаимодействия в целях предотвращения конфликтов в глобальном информационном пространстве.

Желаю организаторам и участникам Форума продуктивной и успешной работы, содержательной дискуссии и всего самого доброго.

## С.М. Бойко

*Начальник департамента проблем безопасности в информационной сфере аппарата Совета Безопасности Российской Федерации*

### **О ПЕРСПЕКТИВАХ ВЫРАБОТКИ ЮРИДИЧЕСКИ ОБЯЗАТЕЛЬНЫХ НОРМ РЕГУЛИРОВАНИЯ ДЕЯТЕЛЬНОСТИ ГОСУДАРСТВ В ИНФОРМАЦИОННОМ ПРОСТРАНСТВЕ**

В контексте основной цели Форума — обсуждение направлений развития сотрудничества в области обеспечения безопасности использования глобальной ИКТ-среды и формирования системы международной информационной безопасности — отмечу, что одним из ключевых направлений сотрудничества, нацеленного на построение безопасного и стабильного многополярного мира в ИКТ-среде, является формирование международно-правового режима предотвращения конфликтов в глобальном информационном пространстве.

Такое сотрудничество осуществляется на всех уровнях создаваемой системы обеспечения международной информационной безопасности. Глобальном, региональном, многостороннем и двустороннем.

Глобальный уровень представлен площадкой Организации Объединенных Наций и ее единственным в настоящее время профильным механизмом, созданным по инициативе России — Рабочей группой ООН открытого состава по вопросам безопасности в сфере использования ИКТ и самих ИКТ 2021–2025 (РГОС).

Одна из ключевых задач РГОС, предусмотренных ее мандатом согласно резолюции A/RES/75/240 — это дальнейшая выработка норм, правил и принципов ответственного поведения государств и путей их имплементации, при необходимости, внесения в них изменений или формулирования дополнительных правил поведения.

Причем эта задача ставится на площадке ООН, начиная еще с 2011 года, когда резолюцией A/RES/66/24 было определено создание в 2012 году очередной Группы правительственных экспертов с подобным мандатом. Такая же задача стояла и перед следующи-



ми группами правительственных экспертов в 2014–2015, 2016–2017, 2019–2021 годах.

Аналогичный мандат был у первой Рабочей группы ООН открытого состава по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности, равно как и ныне действующей новой РГОС, возглавляемой сингапурским дипломатом Бурханом Гафуром, которая будет продолжать свою деятельность до 2025 года.

Безусловно, на начальном этапе разработка этих норм и правил была революционным шагом, поскольку предполагала, по сути, определение рамок ответственного поведения государств в информационном пространстве.

К первоначальному своду таких правил, закрепленному 5 декабря 2018 года в резолюции A/RES/73/27, принятой по инициативе России, добавился еще ряд норм и правил, изложенных в итоговом докладе первой РГОС и промежуточном докладе новой Группы.

Поэтому сегодня мы имеем уже достаточно четко сформулированные правила, которые определяют некий формат достижения международного мира и безопасности в информационной сфере. Но у данного формата есть один, но существенный недостаток — эти правила носят необязательный и добровольный характер.

Буду откровенен, такое положение дел, безусловно, устраивает те государства, которые обладают технологическим превосход-

ством, позволяющим диктовать свои условия другим странам, манипулировать ими.

В реальной жизни мы сталкиваемся с тем, что США и ряд других стран Запада сами определяют, какие необязательные правила и для кого являются обязательными, а для кого они носят только рекомендательный, то есть ни к чему не обязывающий, характер.

Такой избирательный подход способен разбалансировать систему обеспечения международной информационной безопасности, фундамент которой закладывался в ООН благодаря усилиям России и сторонникам ее подходов уже более 20 лет назад.

Необязательные правила и нормы зачастую становятся инструментом для достижения западными странами собственных целей, ни в коей мере не связанных с обеспечением безопасности и стабильности в информационной сфере.

К примеру, сегодня стала обычной практика выдвижения обвинений, прежде всего, в адрес России и Китая, в совершении кибератак на информационную инфраструктуру других государств. Причем обвинений, не имеющих реальных доказательств таких деяний.

Принцип *highly likely* с подачи не только средств массовой информации, но даже официальных лиц правительств стран Запада стал доминирующим.

При этом виновные назначаются по собственному усмотрению.

А ведь еще в докладе Группы правительственных экспертов ООН 2015 года в рекомендациях всему мировому сообществу было сказано: «указание на то, что та или иная деятельность в сфере ИКТ была начата или иным образом происходит с территории или объектов ИКТ-инфраструктуры государства, может быть недостаточным для присвоения этой деятельности указанному государству... Обвинения в организации и совершении противоправных деяний, выдвигаемые против государств, должны быть обоснованными».

В последующем нашими оппонентами было сделано всё возможное, чтобы эта норма больше не упоминалась.

А в ее отсутствии странами Запада начинают формироваться механизмы политической атрибуции кибератак, не только не учитывающие рекомендации профильных групп ООН, но и игнорирующие легитимные меха-

низмы всемирной организации, прежде всего, Совета Безопасности.

Такое положение дел в полной мере устраивает эти страны. Но оно не устраивает большинство членов мирового сообщества. И несогласие с этим все чаще звучит с трибуны Рабочей группы открытого состава.

Сегодня есть запрос на принятие юридически обязательных норм, регулирующих деятельность государств в ИКТ-среде. Это доказывает и сам ход дискуссий на площадке РГОС, и положения докладов Группы, как итогового 2021 года, так и промежуточного, июльского, доклада 2022 года.

Напомню, что в пункте 80 принятого консенсусом итогового доклада РГОС 2019 – 2021 отмечается, что «были высказаны ... важные предложения, включая возможность принятия дополнительных юридически обязательных обязательств».

А в приложении к этому докладу – в резюме председателя — указывается, что «ввиду быстро меняющегося характера угроз и серьезности риска необходимы согласованные на международном уровне и имеющие обязательную юридическую силу нормативные рамки использования ИКТ».

Россия не скрывает цели своей государственной политики в области международной информационной безопасности. Она отражена в ключевом профильном документе стратегического планирования — Основы государственной политики Российской Федерации в области международной информационной безопасности, утвержденных Указом Президента Российской Федерации от 12 апреля 2021 года № 213.

Цель — содействие установлению международно-правового режима, при котором создаются условия для предотвращения межгосударственных конфликтов в глобальном информационном пространстве.

Число сторонников такого подхода, впервые озвученного Россией на площадке ООН, продолжает неуклонно расти. Правовая неурегулированность деятельности государств в ИКТ-среде создает предпосылки к хаосу, диктату сильных, их безответственности и безнаказанности за свои противоправные деяния.

В поддержку необходимости конвенционального закрепления норм международного права в этой области приведу слова Прези-

дента России В.В. Путина, сказанные им в октябре 2021 года на заседании Валдайского клуба: «...международное право — это совокупность международных норм. Это, кстати, не какие-то правила, которые кто-то себе под одеялом нарисовал и думает, что все это будут исполнять. Это согласованные решения, если мы говорим о нормах публичного международного права, то есть это те нормы, которые регулируют отношения между государствами, это результат договоренностей: подписали, взяли на себя обязательства, — исполняйте».

Надеюсь, что благодаря усилиям России и сторонников ее подходов упомянутым выше нормам и правилам, выработанным на площадке ООН, не будет уготована негативная участь. Эти нормы и правила могут стать основой Конвенции об обеспечении междуна-

родной информационной безопасности. Концепция такого документа была разработана Россией еще в 2011 году.

РГОС, будучи уникальной площадкой, собравшей всех членов мирового сообщества, должна не топтаться на месте, а идти вперед. Расширение и дополнение перечня норм и правил ответственного поведения государств не должно быть самоцелью. Сегодня важно переходить к субстантивной дискуссии о юридически обязательных нормах регулирования деятельности государств.

Повторю, основа для этого уже есть – это правила, нормы и принципы, выработанные за последнее десятилетие профильными группами ООН.

Осталось за малым — от слов перейти к делу.

## В.А. Уваров

Директор Департамента информационной безопасности, Центробанк России

Все чаще мы становимся свидетелями кибератак на финансовую сферу. Наша цель — предотвратить и максимально защитить от них как финансовые организации, так и потребителей финансовых услуг. А для этого необходимо скоординировать усилия регуляторов, правоохранительных органов, организаций кредитно-финансовой сферы. И сейчас я готов поделиться с вами опытом Банка России по организации такого взаимодействия.

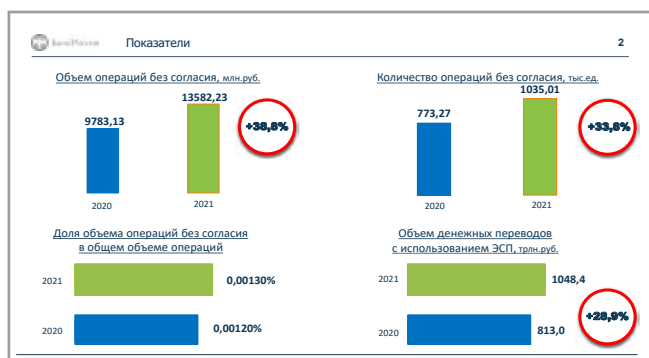
Для начала давайте посмотрим на основные показатели по операциям без согласия клиентов предыдущих лет. Эти сведения Банк России ежеквартально и ежегодно публикует на сайте в своих отчетах. Это параметры хищений по итогам 2020 и 2021 гг. В 2021 году мы наблюдали рост хищений, как в денежном выражении практически на 39%, так и в количественном на 34%. Основным инструментом злоумышленников для хищения средств было использование приемов и методов социальной инженерии, когда человек под психологическим воздействием добровольно переводит денежные средства или раскрывает банковские сведения, позволяющие злоумышленникам совершить хищение. Несмотря на снижение доли таких операций, они наносят наибольший ущерб гражданам за счет значительной суммы похищенного. В инструментарии злоумышленников лидером по-прежнему остается телефонное мошенничество, это порядка 80% из общего пула атак на граждан. Следующим по популярности каналом атаки являются интернет ресурсы, на которые наши граждане заходят самостоятельно (это фишинго-



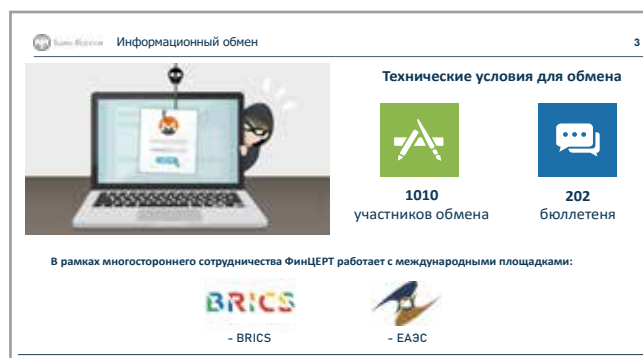
вые сайты, различные рекламные баннеры, социальные сети) и соответственно, оставляют там свои личные и финансовые данные (10%).

Сейчас я расскажу подробнее о ресурсах Банка России позволяющих выявлять и реагировать на мошеннические операции. В Банке России создано специальное подразделение — ФинЦерт. Финцерт Банка России — Центр взаимодействия и реагирования на компьютерные атаки в кредитно-финансовой сфере это структурное подразделение Департамента информационной безопасности Банка России. ФинЦЕРТ взаимодействует с поднадзорными Банку России организациями, разработчиками антивирусного ПО, операторами связи, и конечно, с иностранными участниками финансового рынка.

В рамках его деятельности выявляются фальшивые сайты, номера телефонов,



Слайд 2. Показатели



Слайд 3. Информационный обмен



которые используются в мошеннических целях. Основными задачами Финцента являются:

1. Мониторинг и аналитика, что включает в себя сбор и анализ информации о кибератаках, признаках и характере операций, совершенных без согласия клиентов,
2. Взаимодействие. В эту задачу входит информационный обмен с всеми участниками, разработка и распространение оперативных и аналитических материалов.

На этих 2 этапах очень важно оказать помощь коллегам из финансовых организаций в оперативном выявлении, и что еще не менее важно — путем своевременного информирования — предотвратить новые попытки хищения.

И 3 задача — реагирование. В нее входят мероприятия по запуску процедуры блокировки доменов сети Интернет и инициация мер реагирования на мошеннические телефонные номера.

Финцерт работает 24 часа в сутки 7 дней в неделю. За 2022 год в сторону партнеров Банк России направил более 202 бюллетеней. На сегодняшний день зарегистрировано 1010 участника информационного обмена.

В рамках сотрудничества ФинЦерт работает с международными площадками по двум направлениям — интеграционному и двустороннему. Об этом сотрудничестве я расскажу подробнее позже в своем выступлении.

Сейчас я хочу остановиться подробнее остановиться на задаче и ФинЦерта по осуществлению реагирования и результатах по этой задаче.

Одним из важных направлений по противодействию кибермошенничеству является

борьба с мошенничеством, осуществляемым с использованием Интернет сайтов и социальных сетей. Эту работу мы ведем совместно с Генеральной прокуратурой Российской Федерации, а также в рамках соглашений о взаимодействии, заключенными между Центральным банком Российской Федерации и администраторами доменных имен первого и второго уровней.

На основании данных соглашений Банк России обращается к регистраторам о прекращении делегирования различных фишинговых сайтов, а также сайтов, на которых осуществляются мошеннические действия с использованием платежных карт. Среднее время делегирования доменов регистратором занимает от трех часов до трех дней.

Также в целях противодействия увеличению масштабов использования сайтов сети «Интернет» для совершения мошеннических действий на финансовом рынке, Банк России инициировал изменения, указанные в Федеральном законе, на основании которых Банк России получил право обращаться в Генеральную прокуратуру Российской Федерации для внесудебной «блокировки сайтов» и в суд для осуществления «блокировки сайтов». Полномочия Банка России вступили в силу с 01.12.2021. За 2021 год мы инициировали блокировку 3100 мошеннических интернет-ресурсов.

В 2021 году Банк России инициировал блокировку 6213 сайтов в различных доменных зонах.

Я думаю не нужно объяснять, как важно и нужно развивать наше взаимодействие и сотрудничество в данном направлении. Именно при такой реализации действий мы сможем оперативно и эффективно пресекать мошеннические действия и прочие виды противоа-

Блокировка мошеннических сайтов

4

- Снято с делегирования 6213 интернет-ресурсов, используемых для хищения денежных средств
- 3100 доменов направлено на блокировку в Генеральную прокуратуру
- Нет реакции со стороны регистраторов за пределами РФ



Слайд 4. Блокировка мошеннических сайтов

Международное сотрудничество

5

ЕАЭС

Обмен информацией о киберугрозах

- Обмен информацией, гармонизация подходов по обеспечению информационной безопасности
- Оказание практической, консультационной и методической помощи
- Рабочая группа по вопросам обеспечения ИБ и противодействия компьютерным атакам в кредитно-финансовой сфере
- Практико-ориентированное обучения по информационной безопасности «Киберкурс»



Слайд 5. Международное сотрудничество ЕАЭС



конной деятельности. И мы очень рассчитываем на вашу поддержку.

В эпоху глобализации невозможно справиться с проблемами кибермошенничества в одиночку. Как я уже говорил ранее, мы развиваем международный информационный обмен по двум направлениям — интеграционному и двустороннему.

По первому направлению работа ведется в рамках сотрудничества с центральными (национальными) банками стран — участниц ЕАЭС и БРИКС. И сближение с национальными банками стран участниц ЕАЭС уже приносит свои плоды.

В рамках ЕАЭС разработаны и утверждены:

- Единый глоссарий по вопросам информационной и кибербезопасности,
- Перечень процессов обеспечения информационной безопасности,
- Документ по составу и содержанию требований к организациям, осуществляющим анализ защищенности и внешний аудит в рамках ЕАЭС.

В 2021 году и в 2022 году для коллег мы провели Практико-ориентированное обучение по информационной безопасности «КиберКурс. Международный блок», а также круглый стол по проблемам социальной инженерии. Такой подход высоко оценили на международном уровне, и наша программа получила приз конкурса Всемирной встречи на высшем уровне по вопросам информационного общества (WSIS 2021) под эгидой ООН.

Кроме того, утверждены обновленные Дорожные карты Рабочих Групп по координации развития национальных платежных систем, а 27.06.2022 Национальным банком Республики Казахстан проведена презентация АСОИ «QAINAR».



Слайд 6. БРИКС

Аналогичное сотрудничество развивается и в рамках БРИКС.

Проводится работа по заключению соглашений/меморандумов со странами BRICS в области информационной безопасности», заключено соглашение с Индией.

В рамках БРИКС разработаны, утверждены и опубликованы:

Электронный буклет регуляторных актов стран БРИКС в сфере ИБ

Сборник лучших практик стран по ИБ

Доклад по цифровой финансовой доступности.

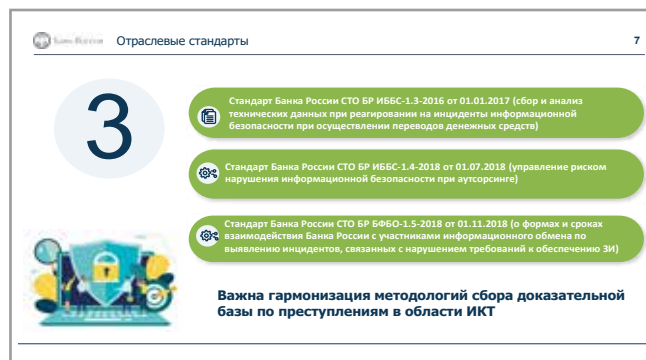
Одобрена подготовленная МИД Концепция участия России в БРИКС.

Принято участие в BRICS Seminar — Information Security and Consumer Protection. Следует отметить, что в июне 2021 года Банк России в рамках обучения по информационной безопасности «КиберКурс» для коллег из центральных (национальных) банков стран — БРИКС провел обучающее мероприятие. В рамках курса обсуждались актуальные вопросы, ведущие эксперты активно делились опытом и реальными кейсами.

Банк России участвует в процессах стандартизации в области информационной безопасности на всех уровнях: международном, национальном, отраслевом.

Эксперты Департамента информационной безопасности Банка России принимают участие в работе профильных групп Международной организации по стандартизации (ИСО), Международной электротехнической комиссии (МЭК), Международного союза электросвязи, национального Технического комитета по стандартизации (ТК122) «Стандарты финансовых операций».

Наши эксперты вносят свой вклад в работу перечисленных организаций по стандар-



Слайд 7. Отраслевые стандарты

тизации. Также основываясь на уникальном опыте коллег, мы принимаем за основу лучшие наработки в области регулирования вопросов информационной безопасности при разработке своих нормативных актов, стандартов (отраслевых, национальных).

В рамках ВТО Банк России принял участие в подготовке Совместной инициативы ВТО по вопросам регулирования электронной торговли (в форме соглашения).

На текущий момент в России в основе организации информационного обмена по вопросам информационной безопасности лежит комплекс отраслевых стандартов, разработанных Банком России. Мы разработали 3 основных стандарта:

1. Стандарт о реагировании на инциденты информационной безопасности.
2. Стандарт о формах и сроках взаимодействия.
3. И порядок управления риском.

Сейчас мы завершаем работу над стандартом СТО БР БФБО-1.5-2022 «Управление инцидентами, связанными с реализацией информационных угроз, и инцидентами операционной надежности.

Уважаемые коллеги! Уже ни для кого не секрет, что мы живем в эпоху тотальной глобализации, где весь мир — как единый организм, здоровье которого напрямую зависит от слаженной работы его составных частей. Глобальный характер носят и проблемы, которые мы сегодня обсуждаем. И именно поэтому сегодня так важно всем вместе искать пути решения этих проблем. Развитие системы трансграничных платежей дало возможность преступникам ускорить процесс получения

денег. Злоумышленник может находиться в любой точке мира и атаковать граждан абсолютно любой страны. Причем массово. Глобальная сеть Интернета позволяет это сделать.

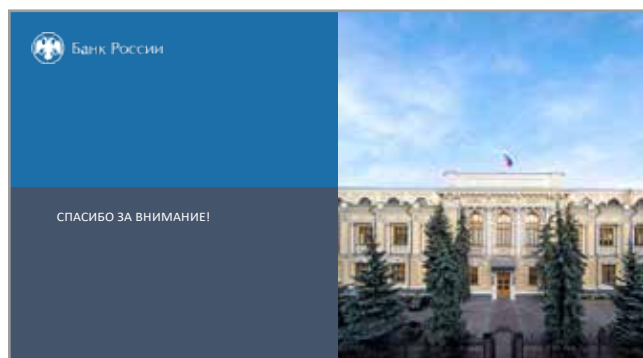
Опыт нашего общения с коллегами из ЕАЭС свидетельствует, что работает как правило такая схема: сначала техника вывода средств и атаки отрабатывается в РФ, затем, по мере выстраивания защиты российских банков и их клиентов, вектор атак перемещается на русскоязычное пространство, не входящее в нашу юрисдикцию и потому не так хорошо защищенное теми механизмами, которые мы реализовали для российского финансового сектора.

Мы не сможем противостоять действиям злоумышленников, если каждый из нас будет работать в одиночку, крайне необходимо и важно разработать единые принципы взаимодействия финансовых регуляторов и гармонизации антифрод процедур. Я призываю всех участников встречи поддержать меня это сделать. С своей стороны мы предлагаем взять за основу комплекс разработанных нами стандартов, уже показавших себя в действии, о них я говорил ранее. Полагаю, что наше сотрудничество уберет границы между странами в вопросах борьбы с кибермошенничеством.

В завершении своего выступления хотел бы поблагодарить Вас за возможность выступить и отметить что Банк России всегда открыт к конструктивному диалогу и готов к международному сотрудничеству и обмену опытом. Уверен, что координация совместных усилий между странами в вопросах борьбы с кибермошенничеством несомненно даст свои плоды!



**Слайд 8. Противодействие преступности при трансграничных платежах**



**Слайд 9.**

## Чен Гопин

*Начальник Департамента, Китайское общество дружбы с зарубежными странами*

Дорогие российские друзья!

Китайское общество дружбы с зарубежными странами приветствует Вас и поздравляет с началом работы XVI международного форума «Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности».

Как Вы хорошо знаете, наше общество более 30 лет имеет дружеские связи с российскими партнерами и в течение половины этого периода члены нашего общества работают совместно с российскими друзьями по теме «информационная безопасность». Мы безмерно благодарны Президенту Национальной ассоциации международной информационной безопасности генералу Владиславу Петровичу Шерстюку за приглашение работать вместе. Многие результаты, полученные в ходе совместной работы, докладывались руководству страны и послужили обеспечению информационной безопасности нашей Родины.

В основе нашей совместной работы лежат крепкие дружеские, равноправные партнерские отношения, сложившиеся между Председателем Китайской народной республики Си Цзиньпином и Президентом России Владимиром Путиным. Как заявил глава китайского внешнеполитического ведомства Ван И «руководствуясь важным консенсусом, достигнутым между главами двух стран, Китай готов



сотрудничать с Россией, чтобы в новую эпоху вывести двухсторонние отношения на более высокий уровень». Это высказывание подтверждается и результатами состоявшейся встречи наших руководителей в Самарканде. Со всей ответственностью мы будем следовать этим решениям.

Мы уверены, что прерванные пандемией COVID-19 прямые отношения с российскими друзьями будут в скором времени возобновлены и мы сможем встретиться за дружеским столом, чтобы продолжить нашу совместную работу.

Еще раз примите наши дружеские поздравления.

До скорой встречи.

## Г.С. Логвинов

*Заместитель Генерального секретаря  
ШОС*

Уважаемый Владислав Петрович,  
Уважаемый Олег Владимирович,  
Уважаемый Сергей Михайлович,  
Коллеги и друзья!

Прежде всего, позвольте от имени Секретариата ШОС поблагодарить Национальную Ассоциацию Международной информационной безопасности за организацию сегодняшнего Форума и приглашение выступить на его открытии.

Тематика МИБ свыше 16 лет назад появилась в повестке дня ШОС и за прошедшие годы выдвинулась на высшие строки на шкале приоритетов в деятельности Организации, став одним из наиболее заметных и даже знаковых направлений в функционировании ШОС. Согласно статистике Internet World Stats<sup>1</sup> на пространстве ШОС в 2022 году зарегистрировано 2 млрд. из 5 млрд. общего числа интернет-юзеров, что уже само по себе обуславливает важность этого направления в работе Организации.

Едва ли будет преувеличением сказать, что в области МИБ ШОС идет в авангарде, а порой возглавляет международные усилия по выработке универсальных, юридически обязывающих норм ответственного поведения государств в информационном пространстве, недопущения использования информационно-коммуникационных технологий в противоправных целях. В том числе, в ШОС принято более широкое понимание МИБ, чем в ООН. В Соглашении между правительствами государств-членов ШОС о сотрудничестве в области МИБ 2009 года «информационная безопасность» определяется как «состояние защищенности личности, общества и государства и их интересов от угроз, деструктивных и иных негативных воздействий в информационном пространстве». В рамках такого понимания проблемы отрабатывается практическое взаимодействие государств-членов в данной сфере. Отмечу, в частности, совместные антитеррористические учения компетентных органов государств-членов ШОС



по выявлению и пресечению использования сети Интернет в террористических и сепаратистских целях.

На принятом в 2020 году в Москве Заявлении Совета глав государств-членов ШОС о противодействии распространению террористической, сепаратистской и экстремистской идеологии, в том числе в сети Интернет, была подтверждена важность коллективных подходов к борьбе с терроризмом и питающим его экстремизмом. В развитие этого Заявления на юбилейном заседании СГГ ШОС в Душанбе в прошлом году был принят План взаимодействия государств-членов ШОС по вопросам обеспечения международной информационной безопасности на 2022–2023 годы, который в настоящее время реализуется. Хочу также обратить внимание на то, что недавно в составе Исполнительного комитета Региональной антитеррористической структуры ШОС был создан Департамент МИБ, который возглавил заместитель Директора Исполкома, гражданин Индии Ракеш Кумар. В перспективе предполагается формирование специального профильного учреждения, либо полностью самостоятельного, либо как автономной структуры Универсального центра ШОС по борьбе с угрозами, в который предполагается преобразовать PACT. Оба варианта внимательно изучаются сторонами.

<sup>1</sup> <https://www.internetworldstats.com/stats3.htm>



Взаимодействие в сфере информационно-коммуникационных технологий в рамках ШОС далеко не ограничивается одним измерением МИБ. ИКТ в целом все глубже проникают в практическую ткань взаимодействия в рамках ШОС, пронизывают один за другим механизмы Организации. Дополнительный импульс этому процессу придала пандемия коронавируса, вследствие которой в течение двух лет заседания Совета глав государств-членов — высшего органа ШОС — проводились в он-лайн режиме. В этом плане только что завершившийся саммит в Самарканде стал первым после перерыва, прошедшим полностью в очном формате. Предстоящее же позднее в этом году заседание Совета глав правительств состоится по-прежнему в режиме видеоконференции. Посмею предположить, что даже в будущем, когда, не сомневаюсь, человечество справится с коронавирусом, и, если только не появится какая-нибудь другая, еще более зловредная инфекция, многие экспертные совещания и обсуждения будут по-прежнему проводиться в он-лайн режиме. В этой связи встает вопрос о совершенствовании каналов интернет-связи между государствами-членами, поскольку на сегодня, как показывает практика, различных помех остается достаточно много, что неизбежно негативно сказывается на качестве и эффективности таких совещаний.

Три года назад, на заседании СГГ ШОС в Бишкеке была утверждена Концепция сотрудничества государств-членов Шанхайской организации сотрудничества в сфере цифровизации и информационно-коммуникационных технологий. В ней четко сформулированы основные цели и задачи взаимодействия на данном направлении, в том числе: повышение глобальной конкурентоспособности и цифровое преобразование в национальных экономиках государств-членов ШОС путем внедрения инноваций и современных ИКТ; повышение инвестиционного потенциала, преодоление цифрового разрыва, повышение информационной безопасности для обеспечения равного и безопасного доступа к современным ИКТ и др.

Обусловленные пандемией глобальные сбои в функционировании транснациональных производственных, техноло-

гических, транспортных и логистических цепочек, нанешие болезненный удар по экономикам государств-членов, выдвинули на передний план задачу форсированной цифровизации экономики, в связи с чем на упомянутом заседании в Москве Совет глав государств-членов принял Заявление о сотрудничестве в области цифровой экономики. В нем констатирована важность развития сотрудничества в сфере цифровизации, информационно-коммуникационных технологий в промышленности, транспорта, сельского хозяйства, здравоохранения, образования, туризма, энергетики, торговли, финансов и таможни; изучения вопросов взаимодействия в сфере программ и научных разработок в области «сквозных» цифровых технологий, искусственного интеллекта, робототехники, Интернета вещей и др.

Новое развитие взаимодействия в сфере ИКТ получило на нынешнем саммите, прошедшем на днях в Самарканде. На нем были приняты Программа сотрудничества между уполномоченными органами государств-членов по развитию цифровой грамотности и Программа сотрудничества между уполномоченными органами государств-членов по развитию искусственного интеллекта.

Уважаемые коллеги,

Нынешние тектонические потрясения в мире, обвальная деградация международных отношений и стремительное погружение международного сообщества в конфронтационную пучину убедительно подтвердили тот факт, что информационные технологии получили прямое военное применение, а цифровое пространство превратилось в плацдармы и поля сражений. Подобные обстоятельства мы неизбежно должны учитывать при планировании совместных действий по поддержанию благоприятного медийного фона вокруг нашей Организации и проводимых под ее эгидой мероприятий. Стоит предусматривать возможные попытки дискредитации усилий ШОС, провокационные вбросы и дезинформационные кампании. На это было обращено особое внимание на ежегодных консультациях руководителей информационных служб министерств иностранных дел государств-членов в мае с.г.

Все более актуальный характер приобретает задача выработки в рамках ШОС

согласованных правил, норм и принципов поведения на интернет-площадке. Стоит активизировать поддержку независимых информационных порталов в противовес таким социальным сетям, как Facebook, Instagram, YouTube, на которых западными странами публикуется под видом достоверных сообщений заведомо ложная информация, а правдивый контент, который противоречит пропагандистскому нарративу, постоянно блокируется.

Наконец, стоит иметь в виду перспективу создания системы оперативной закрытой связи между главами государств-членов ШОС, а также отдельными министерствами и ведомствами — иностранных дел, по чрезвычайным ситуациям и др.

Желаю всем участникам Форума плодотворной работы!

Спасибо за внимание!



## С.К. Кузнецов

Заместитель председателя правления  
ПАО Сбербанк

- В кибервойне принимает более участие **300 тыс.** человек — «ИТ-армия Украины», хакерские группировки при поддержке спецслужб западных стран.
- Количество кибератак против российских компаний увеличилось **в 15 раз.**
  - о С февраля жертвами кибератак стали около **700** организаций РФ. Первые удары пришлись на госорганы, медиаиндустрию, телекомы, финансовый сектор. Киберпреступники стремятся вывести из строя критическую инфраструктуру страны.
  - о Злоумышленники используют все доступные им средства, включая мощные DDoS-атаки, взломы сайтов, кражи данных, фишинг, информационные атаки.
- В рамках ведущейся кибервойны мишенями для киберпреступников являются не только российские организации, но и граждане всей страны. **Сейчас наступил новый этап кибервойны именно против граждан.**
- За лето злоумышленники выложили в открытый доступ **140** баз данных российских компаний, содержащих различную информацию об их клиентах, в том числе персональные данные. Всего — свыше **300 миллионов записей.** Только в августе выложено **100 баз** — это антирекорд.
- Важно, что злоумышленники сейчас не продают утекшие данные другим преступникам, а выкладывают их бесплатно. Таким образом, их цель — нанести максимальный ущерб.

### DDoS-атаки

- С начала года Сбер отразил более **450** DDoS-атак, что сравнимо с общим количеством атак на банк за последние **5 лет.**
- В пиковые периоды Сбер отражал более **40** одновременных атак.
- Кейс: 6 мая Сбер отразил самую мощную DDoS-атаку в своей истории. Она была направлена на сайт банка, а



**вредоносный трафик, сгенерированный ботнетом, исходил из более чем 27 тысяч устройств из Тайваня, США, Японии и Великобритании.**

### Фишинг

- Количество фишинговых доменов с использованием бренда Сбербанка выросло до **250–300** доменов в неделю, что в 1,3 раза больше, чем до начала СВО.
- Тенденция — целевой фишинг на крупные компании.

### ВПО

- Сбер выявил порядка **30** образцов вирусного программного обеспечения, нацеленного на российские организации.
- Кейс: вирусная атака (шифровальщик — Wiper) с адресов ФНС России. 13 и 14 июня 2022 года зафиксирована попытка рассылки писем от ФНС России, содержащих ссылку на вредоносный ресурс, с которого осуществлялась загрузка ВПО для шифрования и уничтожения данных.

### Сетевые атаки

- В сравнении с прошлым годом Сбер фиксирует рост сетевых атак **в 2,5 раза.**
- Для получения первоначального доступа к инфраструктуре банка злоумышленники осуществляли сканирование

веб-сервисов на периметре банка на наличие уязвимостей и предпринимали попытки проведения различных веб-атак.

### Информационные атаки

- В первые дни после начала СВО Сбербанк столкнулся с потоком фейковых сообщений, касающихся деятельности банка. Только за март Сбербанк опроверг 19 фейков.
- Пример фейкового сообщения: «У пользователей приложения Сбер-Банк Онлайн включилась функция автоматического снятия денег, уже подтверждены факты несанкционированных списаний».
- С ноября 2021 по февраль 2022 года число мошеннических звонков россиянам достигало **100 тыс.**, а за февраль-март 2022 года их фактически не было. В настоящее время количество мошеннических звонков плавно растет.
- Сегодня против российских граждан действует около 100 колл-центров.
- Место размещения основных колл-центров — Украина (Львов, Днепр, Запорожье, Одесса, Тернополь, Черновцы и другие города в западной части).
- Колл-центр в Бердянске располагал данными более **35 млн** граждан РФ. С этой базой персональных данных «работали» более **300** сотрудников колл-центра, которые совершали более **15 тыс.** звонков ежедневно.
- Восстановлено **более 50** мошеннических сценариев общения с потенциальными жертвами.
- Преступные доходы, обеспечиваемые деятельностью колл-центра, превышали **200 млн** рублей в месяц.
- Мошенники разработали собственные системы для создания клонов банковских сайтов **40** крупнейших банков. За несколько кликов система позволяет создать набор документов для обмана граждан (платежки, справки, удостоверения).
- С помощью технологий искусственного интеллекта, графовой аналитики и суперкомпьютера «Кристофари» **наши специалисты смогли идентифици-**

**ровать всех работников колл-центра** и их связи. Нами достоверно установлено, что мошенники обманули несколько **тысяч** граждан, уже возбуждено более тысячи уголовных дел.

- В мошенническом колл-центре соблюдался высокий уровень безопасности и анонимности: использовались VPN, криптоконтейнеры.
- Вывод средств осуществлялся через профессиональные дроп-сервисы на специализированных площадках в Darknet с ежедневными расчетами через биткоин.
- Важным элементом кибервойны против России является уход западных технологических вендоров с российского рынка. Отечественные компании столкнулись со сложностями в покупке средств защиты информации, прекратилась техподдержка, остановился обмен информацией об уязвимостях.
- На государственном уровне эти вызовы понимают и правильно стимулируют бизнес: совершенствуется регулирование, приняты важные указы: Указ Президента РФ №166 от 30 марта 2022 г., Указ Президента РФ №250 от 01 мая 2022 г.
- С 1 января 2025 года вступит в действие запрет на использование иностранного ПО для значимых объектов КИИ, а также запрет на использование средств защиты недружественных иностранных государств.
- Сбер активно развивает тему импортозамещения: банк внедряет у себя отечественные программные решения (это продукты компаний BI.ZONE, Ростелеком Solar, «Лаборатории Касперского»), а также разрабатывает собственные.
- Весь критичный функционал **SOC** — полностью российская разработка, и на **90% разработка команды Сбера**. Разработка защищена 7 патентами и получила 8 международных наград.
- Собственной разработкой является **антифрод-система** Сбера: основной инструмент, который Сбербанк использует для защиты клиентов от мошенничества.

- о Система выявляет **99%** всех попыток мошенничества. Этот показатель уникален для всей мировой финансовой системы.
- о Для защиты клиентов Сбербанк собирает в антифрод-системе всю информацию об их операциях и анализирует её с помощью искусственного интеллекта. Сегодня это более **450 млн** операций в сутки.
- о Только за 2021 год с помощью системы от мошенников спасено **112 млрд** рублей средств клиентов. А за истекший период 2022 года — уже более **108 млрд** рублей.

Антифрод-система Сбера постоянно развивается. Так, в августе мы добавили в приложение СберБанк Онлайн новую опцию для дополнительной защиты клиентов от телефонных мошенников.

## Д.И. Григорьев

Вице-президент по информационной безопасности ПАО «ГМК «Норильский никель»

### НОВЫЕ ВЫЗОВЫ В ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЛЯ ПРОМЫШЛЕННЫХ КОМПАНИЙ: ОПЫТ «НОРНИКЕЛЯ»

События на мировой арене обострили существующие проблемы в сфере информационной безопасности. В текущем геополитическом контексте и под гнетом масштабных санкций, введенных странами западного блока, российская промышленность столкнулась с новыми вызовами и угрозами в цифровом пространстве.

«Исход» крупнейших западных технологических компаний из России, привел к серьезным затруднениям в использовании их продуктов и решений для информационных систем компаний индустриального сектора. Зарубежное программное обеспечение и техника превратились в «мину замедленного действия»: с каждым днем их эффективность снижается и существует угроза полного отказа в работе в любой момент. Это не могло не привести к повышению уязвимости информационных систем, в том числе, отвечающих за функционирование критической информационной инфраструктуры.

Снижение устойчивости перед информационными угрозами извне на фоне беспрецедентного роста количества кибератак не только создает риски на уровне непосредственно информационной инфраструктуры, но, как следствие, повышает вероятность техногенных катастроф.

Аналогичные проблемы возникли и в сфере защиты информации и данных. В последнее время мы наблюдали устойчивую тенденцию со стороны

IT-вендоров по переводу IT-сервисов в «облака». Сейчас, после ухода из России крупнейших глобальных провайдеров облачных сервисов, чьи комплексные платформы включают продукты и услуги с технологиями обработки данных, искусственного интеллекта, «интернета вещей» и блокчейна, встала задача по переходу на российские облачные решения или по отказу от «облаков». Для крупных государственно-значимых промыш-



ленных холдингов принципиальное значение имеет защищенность информационных ресурсов в соответствии с суверенными требованиями их государств, что затруднительно обеспечить в облачных решениях. К тому же, зарубежные «облака» продемонстрировали свою крайнюю ненадежность.

В условиях беспрецедентных санкций в технологической сфере неизбежно произойдет снижение темпов цифровизации промышленности, это может потенциально повлиять на уменьшение объемов производства, изменение качества продукции, нарушение логистических цепочек, реализацию экологических программ — все эти последствия проистекают из сферы обеспечения безопасности и непрерывности работы информационно-коммуникационных технологий, и распространяются далеко за ее пределы, оказывая влияние и на глобальные процессы развития промышленной отрасли.

Наконец, в текущей ситуации возникли сложности с сертификацией промышленных компаний на соответствие международным стандартам информационной безопасности. Появились риски приостановки работы сертификационных органов на территории России. Компаниям, чьи сертификаты соответствия выпущены данными органами, приходится переопределять свои дальнейшие пути демонстрации соответствия в зависимости от требований рынка, на который они работают.

Мы неоднократно подчеркивали, что видим серьезный вызов в том, что ИТ-инфраструктура крупных промышленных холдингов построена в основном на решениях/продуктах/услугах ограниченного числа вендоров, зарегистрированных в юрисдикции США и еще нескольких стран Западного блока.

Столкнувшись с геополитическим противостоянием на международной арене и ставшими реальностью политическими мотивированными санкциями в сфере информационных технологий, мы наблюдаем возникновение реальной угрозы для промышленного бизнеса, и в первую очередь, для объектов информационной инфраструктуры, которыми этот бизнес владеет или управляет.

В условиях тотального нарушения ранее принятых договоренностей и с учетом возможных и вполне реальных последствий реализации угроз безопасности информационных систем промышленных компаний, считаем важным поставить вопрос о необходимости введения особого международно-правового режима для продукции и услуг вендоров, составляющих основу информационных систем значимой доли промышленного сектора, и о выведении данных компаний и продуктов из-под юрисдикции отдельных государств с целью повышения надежности и устойчивости глобальной ИТ-инфраструктуры.

Принципиальные, юридически значимые для промышленности положения информационной безопасности должны быть закреплены в международных документах: в рамках Рабочей группы ООН открытого состава по вопросам безопасности в сфере использования информационно-коммуникационных технологий и самих информационно-коммуникационных технологий или на других площадках. Мы также приветствовали бы принятие отдельного специализированного документа, закрепляющего принципы защиты информационной инфраструктуры на международном уровне. Проект такого документа — Хартии информационной безопасности критических объектов промышленности — был представлен «Норникелем» на международном уровне в 2017 году.

Норникель — это инновационная компания и одновременно один из флагманов российской экономики. Наш ключевой при-

оритет — непрерывность и эффективность производственного цикла, выполнение обязательств перед партнерами, работниками и регионами присутствия компании. Поэтому мы уделяем большое внимание тем продуктам и решениям, которые используем. Ранее, где это было возможным, мы делали выбор в пользу национального производителя, особенно в вопросе обеспечения безопасности критической информационной инфраструктуры. Сейчас же мы готовы в инициативном порядке участвовать в процессе импортозамещения в сфере ИКТ и стимулировать скорейший переход на отечественную продукцию и технологические решения. Уже занимаемся подбором и тестированием российских технологических решений в тесном контакте с коллегами из отрасли.

Выполняя указ Президента РФ № 250 от 1 мая 2022, мы в рамках организации подняли значимость вопросов ИБ до уровня вице-президента компании. Мне поручено курировать все вопросы по этой тематике. Также для этих целей мы создали дочернюю компанию ООО «Норникель Сфера», которая будет отвечать за безопасность всех информационных систем Норникеля.

Однако, как отметил Президент Норникеля Владимир Потанин в одном из недавних интервью: «Даже успешная реализация импортозамещения не избавляет нас от проблемы того, что нельзя быть отрезанным от международных цепочек создания различного рода технологических продуктов.... Тут очень важно не допустить полной изоляции и не сделать ошибку, импортозамещение — это тактика выживания, а не стратегия развития. Поиск партнеров должен быть и будет продолжен».

Мы нацелены наращивать потенциал компании в сфере информационной безопасности и делиться своей экспертизой с партнерами по отрасли. В частности, в начале сентября мы организовали «киберсессию» в рамках заседания КБ МПА, где «Норникель» является сопредседателем. Коллеги из ЮАР, Европы и Америки, представители крупных промышленных добывающих и перерабатывающих компаний узнали о подходах Норникеля к вопросу организации распределенной системы ИБ и поделились своими наработками в этой области.



Несмотря ни на что, Норникель стремится продолжать сертифицировать свои системы ИБ на соответствие международным стандартам; намерены в дальнейшем поддерживать процессы ИБ на уровне международных требований вне зависимости от доступности сертификационных аудитов.

И наконец, мы интенсифицировали диалог в рамках Клуба «Безопасность инфор-

мации в промышленности» (БИП-Клуб, основан Норникелем в 2017 году), предоставили участникам Клуба площадку для обмена информацией и взаимодействия с представителями госорганов для обеспечения максимально эффективного сотрудничества между государственным и частным сектором.

## В.О. Запивахин

Министерство обороны, эксперт

### ОБ УЧАСТИИ МИНОБОРОНЫ РОССИИ В ФОРМИРОВАНИИ МЕЖДУНАРОДНО- ПРАВОВОГО РЕЖИМА ПРЕДОТВРАЩЕНИЯ КОНФЛИКТОВ В ГЛОБАЛЬНОМ ИНФОРМАЦИОННОМ ПРОСТРАНСТВЕ»<sup>1</sup>

В последнее время «коллективный» Запад развязал против Российской Федерации массированную информационную кампанию. Масштабы ее колоссальные.

СМИ, ИТ-компании и частные интернет-ресурсы, зарегистрированные в юрисдикциях западных стран, непрерывно распространяют антироссийскую информацию откровенно русофобского характера. Наиболее яркий пример — решение корпорации МЕТА о размещении призывов к уничтожению российских военнослужащих в ходе специальной военной операции на Украине. Хотя именно эта корпорация в 2019 году, а также ряд других западных медиахолдингов (Amazon, Dailymotion, Google, Microsoft, Qwant, Twitter и YouTube) нарушают взятое на себя в рамках Крайстчерчского призыва 2019 года обязательство ликвидировать весь насильственный экстремистский контент в Интернете.

Стоит отметить и молчаливую реакцию Запада на героизацию нацизма, получившую особенно широкий размах на Украине, в Прибалтике и пустившую уже глубокие корни практически по всей Европе.

Запад продолжает кампании, по пересмотру итогов Второй Мировой войны, пытаясь возложить ответственность за все те нацистские деяния на страны Советского Союза и в частности на Российскую Федерацию.

Кроме того, западные страны во главе с США принудительно ограничивают свободы пророссийских средств массовой информации. Отмечаем, что необоснованные ограничения деятельности СМИ и распространение ненавистнической риторики являются грубыми нарушениями международного права.

При этом нами отмечается и возросшее количество компьютерных атак различного характера и высокой интенсивности на ин-



формационные системы России, в том числе Минобороны России, что является грубым вмешательством во внутренние дела государства и нарушением его суверенитета.

В тоже время сами США проводят политику установления в информационном пространстве мирового «порядка, основанного на правилах», отвечающих интересам только Соединенных Штатов и их союзников. Основным характерным признаком такого порядка является проведение разделительных линий между так называемыми «государствами-единомышленниками» США и всеми остальными. Первые надзирают за соблюдением «правил поведения в киберпространстве» теми, кто находится якобы вне рамок «демократического мира», выявляют нарушения, предъявляют публичные обвинения в духе «мегафонной дипломатии» и вводят против «злонамеренных государств» различного рода рестрикции (высылка дипломатов, экономические санкции, уголовные преследования виновных и др.). Более того, в случае «серьезных последствий» инцидентов в информационном пространстве, в качестве «крайней меры реагирования» ими планируется применение военной силы. При этом, фактов доказывающих виновность того или иного государства не предоставляется.

Считаем такой подход откровенно агрессивным, направленным на навязывание своей

<sup>1</sup> Выступление подготовлено коллективом экспертов Минобороны России в области международной информационной безопасности в следующем составе: Дылевский И.Н., Базылев С.И., Запивахин В.О., Юниченко С.П., Шевченко А.Л., Комов С.А.

воли другим странам под угрозой «наказания» или неких «последствий». Он не обеспечивает равноправных отношений в информационном пространстве между всеми государствами — членами ООН, и представляет угрозу международному миру и безопасности.

В свою очередь взгляды Минобороны России на формирование системы обеспечения международной информационной безопасности, в том числе на военную политику в данной сфере, кардинально отличаются от западного подхода и основываются на равноправном партнерстве, уважении национального информационного суверенитета, акцентируя внимание на предотвращение (урегулирование) межгосударственных конфликтов в глобальном информационном пространстве, а не «реагирование» на них.

Минобороны России активно развивает международное сотрудничество в области формирования международно-правового режима предотвращения конфликтов в глобальном информационном пространстве. Данная работа проводится как в межведомственном формате, так и по линии военных ведомств.

Так, в 2021 году министрами обороны Российской Федерации и Республики Беларусь были утверждены Основы военной политики Союзного государства в области

МИБ, что позволяет формировать и проводить согласованную в рамках Союзного государства военную политику в данной сфере с учетом имеющихся и вновь возникающих угроз. Предлагаем нашим партнерам ознакомиться с данным документом, который размещен на сайте Минобороны России в сети Интернет.

Кроме того, сегодня Минобороны России прорабатывает с рядом своих коллег вопрос о заключении Соглашения о военном сотрудничестве по предотвращению инцидентов с использованием ИКТ, направленного на недопущение эскалации напряженности и урегулирование инцидентов, которые могут возникнуть вследствие опасной военной деятельности в информационном пространстве, мирными средствами.

Таким образом, хочется отметить, что Минобороны России в рамках формирования международно-правового режима предотвращения конфликтов в глобальном информационном пространстве стремиться не нагнетать, обострять и политизировать ситуацию в информационном пространстве по принципу США и их союзников, а предотвращать, урегулировать, минимизировать и исключать возможность перерастания инцидентов в информационном пространстве в военный конфликт.

## О.С. Макаров

Директор Белорусского института  
стратегических исследований

На сегодняшний день в сфере международной информационной безопасности наблюдается ряд стратегически важных трендов. Прежде всего несмотря на то, что **цифровизация по-прежнему остаётся основной потребностью общества**, очевидно изменение ее стратегий и форм. К примеру, если до недавнего времени на международном уровне активно обсуждались вопросы «цифрового разрыва» (digital divide), и страны с высоким уровнем информатизации общественных отношений старались помочь другим странам нарастить потенциал, то на сегодняшний день наблюдается обратная тенденция, связанная с целенаправленным ограничением потоков данных и доступа к ряду цифровых сервисов. По аналогии с «цифровым разрывом» появляется так называемый «разрыв в данных» (data divide). Ответом на этот вызов может быть или новый этап глобальной цифровизации, или островизация глобальной информационной сферы, т.е. создание региональных закрытых систем. Очевидно, что островизация с большей вероятностью будет сдерживать развитие планетарного информационного общества, однако у национальных и региональных систем появится шанс повысить уровень информационной безопасности и создать платформы, которые в большей степени будут соответствовать культурному коду и запросам конкретного социума.

В контексте уже наметившейся регионализации информационных отношений обращает на себя внимание проблематика **обеспечения безопасности критически важной инфраструктуры**. Очевидно, что для целого ряда КВОИ нужны общие для всех стран стандарты. К примеру, угроза нормальному функционированию ядерных энергетических объектов является угрозой планетарного уровня. Помимо этого, по мере поступательного внедрения собственного программного обеспечения и аппаратных средств особую остроту приобретает вопрос обеспечения безопасности национальной критической информационной инфраструктуры.

Все более актуальной становится **проблема обеспечения технологического и ин-**



**формационного суверенитета.** В Концепции информационной безопасности Республики Беларусь понятие «информационный суверенитет» разрабатывалось на основе правовой доктрины, т.е. верховенство права в информационной сфере на основе подходов к обеспечению государственного суверенитета. Однако на сегодняшний день информационный суверенитет становится чётко увязанным с технологическим суверенитетом. Это новое прочтение информационного суверенитета несет в себе определенные риски для небольших государств, которые вряд ли смогут обеспечить абсолютный информационный и технологический суверенитет самостоятельно. В этом смысле вопрос островизации информационной сферы приобретает особую значимость, так как именно в рамках региональных союзов небольшие государства с большей вероятностью смогут гарантировать свою безопасность.

Важнейшим вызовом в сфере международной информационной безопасности является **конкуренция между государствами и транснациональными корпорациями**. Попытки государств диктовать свои права и определять правила на данный момент не приводят к принципиальному изменению политики корпораций, которые готовы идти на некоторые компромиссы связанные, к примеру, с налогообложением, однако продолжают доминировать в информационном пространстве.

При построении национальных и региональных систем информационной безопасности все более актуальным становится поиск **баланса интересов государства и общества**. Слишком быстро меняется законодательство и переносятся красные линии в сфере информационной безопасности. То, что вчера было совершенно законным сегодня может являться объектом преступления или определять состав преступления. Очевидно, что обществу необходимо время для адаптации.

Необходимо подчеркнуть, что **в новых условиях активно изменяются правоотношения**. Во-первых, право не успевает адаптироваться. Во-вторых, в условиях активной милитаризации информационного пространства снижается активность общественных и государственных структур, которые занимаются международной правоохранительной деятельностью, призывают к правовой справедливо-

сти и выступают за равноправное международное взаимодействие в рамках правового обеспечения информационной безопасности. Границы противоправного поведения размываются, преследование преступников становится практически невозможным. На смену правовым механизмам регулирования общественных отношений приходят не находящиеся в правовом поле скоординированные действия, управляющие поведением людей в информационном пространстве.

В условиях, когда **быстрое создание глобальной правовой платформы в информационной сфере вряд ли возможно**, соответственно повышается роль региональных союзов и региональных правовых экосистем. Представляется, что практики, апробированные первоначально на региональном уровне, к примеру, в рамках Союзного государства, ШОС и БРИКС, впоследствии целесообразно предлагать и на глобальный.



## А.В. Крутских

*Специальный представитель Президента Российской Федерации по вопросам международного сотрудничества в области информационной безопасности, советник Министра иностранных дел*

Хотел бы, прежде всего выразить признательность организаторам мероприятия за актуальную повестку дня и создание условий для конструктивного обмена мнениями.

- **Человечество сегодня как никогда зависит от цифровых технологий**, на развитии которых **основан** современный этап **научно-технической революции**.
- Эту **зависимость** еще больше **усугубила пандемия** коронавирусной инфекции **COVID-19**, поскольку **вызвала лавинообразное увеличение пользователей цифровых инструментов**.
- **Следствием** этого стал **колоссальный рост киберуязвимостей разного рода, преступности** в информационном пространстве, **активизация кибермошенников**, а также увеличение количества кибератак на **объекты критической информационной инфраструктуры, социальной сферы, предприятия, банки**. Это существенно **приумножило экономический ущерб от подобных противоправных действий и вред благополучию миллионов людей**.
- Бизнес уже **давно и прочно встал на цифровые рельсы**: управление бизнесом, финансовыми потоками, логистика, промышленное производство, все виды транспорта осуществляется при широком использовании ИКТ. Во многие сферы бизнеса начинается широкое внедрение технологий искусственного интеллекта.
- **Бизнес вкладывает колоссальные средства в техническое обеспечение собственной безопасности, но при этом продолжает терять огромные финансовые ресурсы**.
- Широкое применение ИКТ **по-новому ставит вопрос о понимании и трактовке** понятия национального или государственного суверенитета.



- Преступность в информационном пространстве все чаще **используется в качестве маскировки для подрыва общественно-политической и социально-экономической обстановки внутри государств, несет угрозу их суверенитету**.
- **Глобальное информационное пространство**, которое способно нивелировать значимость территории государства как материальной субстанции суверенитета выступает фактором, также **создающим угрозу размывания суверенных прав**.
- ИКТ иначе трактуют понятие **«границы суверенных государств»**. Цифровое пространство трансграничное по своей сути. Однако **расплывчатость виртуальных границ киберпространства и неопределенность в применяемой юрисдикции не должны приводить к ошибочному выводу о невозможности правового регулирования** отношений в цифровом пространстве.
- Международное сообщество сегодня **не имеет специального раздела международного права, который, по аналогии с воздушным, морским, космическим правом, регулировал бы отношения в цифровом пространстве**. При этом **действующие нормы международного права не всегда**

могут быть применимы к цифровому пространству.

- **Цифровизация экономики** рассматривается многими странами как один из **основных драйверов собственного развития, обеспечения безопасности и защиты суверенитета.**
- Безусловно, **без настойчивого и эффективного внедрения и освоения передовых цифровых инструментов и технологий** о равноправной и честной конкуренции на мировых рынках вряд ли можно говорить.
- **Не является ли вызовом государственному суверенитету создание облачных транснациональных хранилищ данных?** С технологической точки зрения — это новая реальность представляется весьма перспективной и эффективной. Но **возникает вопрос об обеспечении неуязвимости данных в этих трансграничных хранилищах.** Как должен реализовываться суверенитет государств с учетом этой реальности? Кто будет управлять этими трансграничными хранилищами и обеспечивать их безопасность: узкая группа владельцев, операторы, роботы или искусственный интеллект, который все активнее стал использоваться? В какой степени к этим данным будут иметь доступ государства и их уполномоченные органы? Все эти вопросы требуют скорейшего ответа и выработки четких правовых норм.
- В этой ситуации как **обеспечить национальный и личный суверенитет над данными, которые могут находиться на территории других государств, формально под чужой юрисдикцией.**
- **Введение в оборот цифровых денег и криптовалют разве не подрывает суверенитет?** Денежные суррогаты, создаваемые без участия центробанков, на анонимной и глобальной основе, вступают в конфликт с денежно-кредитной политикой государств и провоцируют риски в области государственного управления кредитно-финансовыми отношениями.

- Безусловно, сами по себе ИКТ не ограничивают суверенитет государства. Но их **целенаправленное использование в целях воздействия на сознание, убеждения, поведение отдельных индивидов и масс населения** может производить значимый эффект для отдельных государств или мира в целом, навязывать определенную модель поведения.
- Но проблема не в самих технологиях, а в том, что **некоторые страны стали использовать их для достижения собственных геополитических целей, попыток навязывания своей гегемонии, распространения дезинформации и фейков, установления цензуры отдельных СМИ, манипулирования информацией, использования информационного пространства для подогревания напряженности и разжигания конфликтов.**
- Крупнейшие цифровые бизнес-гиганты, **принадлежащие США и действующие в рамках американского законодательства, подменяют собой национальные государства и ограничивают их суверенитет.** Достаточно вспомнить отключение от социальной сети действующего президента США. Еще совсем недавно такое было невозможно представить.
- По мнению ряда экспертов, сегодня именно **цифровые гиганты представляют главный источник информационной угрозы для цифрового суверенитета большинства государств мира.**
- Отключение от международной платежной системы SWIFT российских банков в рамках нового пакета антироссийских санкций, **как и сами санкции в принципе, разве это не покушение на суверенитет государства?**
- Интернет, как глобальная сфера, **продолжает единолично контролироваться США** через корпорацию по управлению доменными именами и IP-адресами ICANN, которая остается под американской юрисдикцией и полностью подчиняется правительству США. Такая ситуация **бросает вызов**

- информационному суверенитету всех стран. Хотя еще в 2005 г. народы мира сделали свой демократический выбор в пользу интернационализации управления Интернетом при равноправном участии государств в этом процессе. Это **важнейшее решение было закреплено в Тунисской программе Всемирной встречи на высшем уровне по информационному обществу**. Но по факту его исполнение попросту игнорируется.
- Вместо этого **американцы продолжают навязывать свой «подход с участием всех заинтересованных сторон» (multistakeholder model) к управлению Интернетом**, который лишь **создает иллюзию участия других государств в соответствующем процессе при сохранении и даже укреплении тотального контроля правительства США над Интернетом**.
  - Для этих целей **Вашингтон анонсирует попытки создания альянсов по принципу ad hoc в области Интернет-регулирования, принимает политизированные документы, по типу «Декларации о будущем Интернета» от 28 апреля 2022 г. При этом фактически проводятся искусственные разделительные барьеры между государствами, искусственное разделение государств на «демократические» и «авторитарные». Проведение подобных «разделительных линий» применительно к Интернету — разве это не попытка фрагментации Интернета?**
  - Российская Федерация исходит из понимания, что **Интернет должен быть открытым глобальным ресурсом, способным обеспечить всеобщие равные возможности доступа для всех стран**.
  - Россия поддерживает **необходимость интернационализации управления сетью Интернет, обеспечения равных прав государств на участие в этом процессе, их суверенного права на управление сетью Интернет в своем национальном сегменте на основе норм международного права**.
  - Фактически **реализуется суверенитет избранных государств и суверенитет сильных стран**, обладающих современными технологиями.
  - А как в этом случае быть странам, которые нуждаются в повышении своего технологического потенциала?
  - Западная модель суверенитета формально выглядят космополитичной. Формальная логика **Запада сводится к формуле: если технологии по своей сути трансграничные, то суверенитета быть не может**.
  - Российский подход заключается в том, что **государственный суверенитет должен учитывать современные реалии цифровой среды и природу информационно-коммуникационных технологий**.
  - Страны **смогут отстоять свой суверенитет, если будут выработаны юридически обязывающие нормы, регулирующие отношения в цифровом пространстве**.
  - Одним из способов защиты государственного суверенитета в настоящее время **можно считать предпринимаемые по инициативе российской дипломатии усилия международного сообщества добиться установления международно-правовых стандартов ответственного поведения государств в глобальном информационном пространстве**.
  - Взяв на себя инициативную роль в организации переговорного процесса по международной информационной безопасности (МИБ) под эгидой ООН, Россия начиная с 1998 г. (внесения первого проекта российской резолюции «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» на заседании Генеральной Ассамблеи ООН) все это время **обеспечивает ему максимальную непрерывность и эффективность**.
  - **Безусловно, поддержка наших партнеров и единомышленников важна и значима**.
  - Знаковым можно считать консенсусное принятие итогового доклада ГПЭ ООН

четвертого созыва 26 июня 2015 г., в котором **зафиксированы 11 правил ответственного поведения государств в информационном пространстве** и фиксировались положения о том, что:

- **ИКТ должны использоваться исключительно в мирных целях, а международное сотрудничество необходимо нацелить на предотвращение конфликтов** в информационном пространстве;
- **государства обладают юрисдикцией над информационно-коммуникационной инфраструктурой, расположенной на их территориях;**
- **обязанность государств соблюдать в процессе использования ИКТ** (наряду с другими принципами международного права) такие принципы, как **государственный суверенитет, суверенное равенство, разрешение споров мирными средствами и невмешательство во внутренние дела других государств;**
- **государства не должны использовать посредников для совершения международно-противоправных деяний с применением ИКТ и должны обеспечивать, чтобы их территория не служила для совершения подобных деяний;**
- **любые обвинения в организации и совершении противоправных деяний в сфере ИКТ, выдвигаемые против государств, должны быть обоснованными и доказанными;**
- **необходимо дальнейшее изучение вопроса применимости международного права к сфере использования ИКТ.**
- В настоящее время при **поддержке подавляющего большинства государств** действуют **два магистральных переговорных процесса**, запущенных в ООН по **российской инициативе** в последние годы и **закрепивших интеллектуальное лидерство нашей страны в продвижении тематики МИБ на международной арене.**
- Первый из них — **созданная нами Рабочая группа открытого состава**

**по вопросам безопасности в сфере использования ИКТ и самих ИКТ на 2021–2025 гг.** Отстаиваем в ней формирование международно-правовых основ регулирования деятельности государств и негосударственных субъектов в информационном пространстве через выработку универсальных юридически обязывающих инструментов. Таковые должны закреплять принципы предотвращения конфликтов, невмешательства во внутренние дела и равноправное участие государств в управлении ИКТ и сетями связи, а также суверенитет государств в их информационном пространстве.

- Второй — **запущенный в 2021 г. Специальный комитет по разработке всеобъемлющей универсальной конвенции по противодействию использованию ИКТ в преступных целях.** В качестве национального вклада Россия внесла собственный проект универсальной всеобъемлющей конвенции по противодействию информпреступности, соавторами которого стал Китай и еще ряд государств.
- Важно **сбалансировать систему многостороннего сотрудничества, сделать ее универсальной и более эффективной, укрепив возможности всех без исключения государств в борьбе с преступностью в сфере применения информационно-коммуникационных технологий.** Но главное, чтобы **борьба с киберпреступностью не использовалась как предлог для нарушения суверенитета государств и не служила предлогом для вмешательства в их внутренние дела.**
- Важной международной площадкой является **Международный союз электросвязи (МСЭ) — специализированное агентство ООН.** Считаем актуальной задачей сохранить за МСЭ работу в рамках действующего мандата и не допустить любого противостояния «на полях» Союза, не допустить политизации диалога на площадке МСЭ.
- Россия прилагает **значительные усилия для снижения степени политизации этой специализированной орга-**

низации и стремится сохранить роль МСЭ как единственной влиятельной в системе ООН площадки для решения задач в области развития ИКТ с целью обеспечения глобальной безопасности. Особое внимание придаем задачам **оказания технического и консультативного содействия странам, которые нуждаются в поддержке со стороны МСЭ в целях развития**

**современных технологий электросвязи и преодоления цифрового разрыва.**

- В целях решения всех этих задач Россия выдвигает своего кандидата на пост Генсекретаря МСЭ для избрания в ходе предстоящей уже через несколько дней решающей для судьбы этого органа ООН Полномочной конференции.



## Н.Н. Мурашов

*Заместитель директора Национального координационного центра по компьютерным инцидентам*

### ПРОТИВОБОРСТВО КИБЕРУГРОЗАМ В СОВРЕМЕННЫХ УСЛОВИЯХ

Обстановка в глобальном информационном пространстве продолжает характеризоваться ростом количества и сложности компьютерных атак. В связи с этим международное сообщество сталкивается с необходимостью создания прозрачных механизмов практического взаимодействия для урегулирования возникающих межгосударственных споров.

В соответствии с Федеральным законом от 26 июля 2017 года № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» был создан Национальный координационный центр по компьютерным инцидентам (сокращенно — НКЦКИ).

Основной задачей НКЦКИ является координация деятельности субъектов критической информационной инфраструктуры по вопросам обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты.

В Российской Федерации НКЦКИ является уполномоченным органом по организации и осуществлению обмена информацией о компьютерных инцидентах между субъектами критической информационной инфраструктуры, уполномоченными органами иностранных государств, международными, международными неправительственными и иностранными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты.

Иными словами, НКЦКИ выполняет функции единой точки контактов Российской Федерации по вопросам реагирования на компьютерные атаки.

По нашему мнению, определение в каждой стране именно уполномоченного государством органа — единой точки контактов существенно облегчит взаимодействие и снизит рост напряженности в результате компьютерного инцидента. Только такой механизм взаимодействия по вопросам прекращения



деятельности вредоносных ресурсов мы считаем эффективным.

В 2022 году нашим центром осуществлялся обмен сведениями о компьютерных инцидентах с компетентными иностранными организациями из 120 стран.

От зарубежных партнеров было получено 273 уведомления о компьютерных инцидентах, источниками которых являлись информационные ресурсы, расположенные на территории Российской Федерации. На основании полученных данных российским провайдерам и операторам связи НКЦКИ направил уведомления, по результатам обработки которых деятельность вредоносных ресурсов была полностью прекращена.

Инопартнерам наш центр отправил 1358 уведомлений о компьютерных атаках на информационные ресурсы Российской Федерации, источники которых находятся в соответствующих национальных сегментах сети Интернет.

Применительно к озвученным мною статистическим данным следует отметить, что зарубежные компетентные иностранные организации ответили только лишь на 50 % уведомлений НКЦКИ, тогда как наш Центр обрабатывает абсолютно все поступившие сообщения независимо от национальной принадлежности инопартнера.

Одной из основных мер укрепления доверия в информационном пространстве яв-

ляется наращивание взаимодействия между национальными уполномоченными органами в области реагирования на компьютерные инциденты.

Данный вопрос неоднократно обсуждался на площадке Рабочей группы ООН открытого состава по вопросам безопасности в сфере использования ИКТ и самих ИКТ, сокращенное наименование — РГОС.

На одной из ее сессий большинство государств-членов выступило за создание глобального реестра контактных пунктов под эгидой ООН.

Перечислю основные, на наш взгляд, принципы его функционирования.

Реестр должен способствовать снижению напряженности и угрозы конфликта из-за неправильного понимания и восприятия инцидентов в области безопасности ИКТ, что могло бы привести к просчетам и возможной эскалации, а также упрощению связи и ведению диалога по вопросам безопасности при использовании ИКТ и самих ИКТ.

Контактный пункт на национальном уровне должен быть уполномочен осуществлять и координировать взаимодействие в области обнаружения, предупреждения и ликвидации последствий компьютерных атак, а также реагировать на компьютерные инциденты.

Независимо от международной обстановки, контактный пункт будет стремиться сохранять политическую нейтральность, продолжая осуществлять взаимодействие с другими контактными пунктами в области реагирования на угрозы безопасности при использовании ИКТ и самих ИКТ.

Контактные пункты не должны подвергаться международным санкциям.

Контактные пункты будут отдавать предпочтение прагматичному взаимодействию в области реагирования на угрозы безопасности при использовании ИКТ и самих ИКТ в целях недопущения рисков ошибочного восприятия, эскалации и конфликтов, которые могут возникнуть в результате использования ИКТ.

В рамках осуществления своей деятельности контактные пункты должны учитывать рекомендации, выработанные РГОС, а также следовать правилам, нормам и принципам ответственного поведения государств в информационном пространстве.

Кроме того, указанный механизм может рассматриваться в качестве альтернативы продвигаемой западной концепции политической атрибуции компьютерных атак и практике «назови и пристыди».

Таким образом, создание глобального реестра контактных пунктов на площадке ООН позволит укрепить статус межгосударственного взаимодействия в области реагирования на угрозы безопасности при использовании ИКТ и самих ИКТ и будет содействовать снижению напряженности и угрозы конфликта из-за неправильного понимания и восприятия инцидентов. Эффективная коммуникация в режиме реального времени уполномоченных органов государств-членов ООН позволит повысить транспарентность, предсказуемость, стабильность и сократить риски ошибочного восприятия, эскалации и конфликтов, которые могут возникнуть в результате использования ИКТ.

Реестры контактных пунктов уже сформированы на региональном уровне, в частности, в Организации по безопасности и сотрудничеству в Европе (сокращенно — ОБСЕ) и на площадке Регионального форума Ассоциации государств Юго-Восточной Азии по безопасности (сокращенно — АРФ).

В ОБСЕ сформирована система контактных пунктов для связи на политическом и техническом уровне и диалога по вопросам безопасности при использовании ИКТ и самих ИКТ. В Российской Федерации обеспечение функционирования контактного пункта для связи на техническом уровне возложено на ИКЦКИ.

В организации взаимодействия с использованием реестра контактных пунктов ОБСЕ существуют некоторые недостатки.

Упомянутый реестр задействуется в основном для проведения регулярных проверок связи, а также для бездоказательных обвинений государств-участников ОБСЕ в организации компьютерных атак. При этом возможность эффективного взаимодействия по разрешению компьютерных инцидентов, которая была заложена в основу при создании комплекса мер укрепления доверия ОБСЕ, фактически отсутствует. Так далеко не всеми государствами указаны технические контактные пункты, а некоторые технические контактные пункты, содержащиеся в реестре, не уполномочены

на национальном уровне осуществлять деятельность по обнаружению, предупреждению и ликвидации последствий компьютерных атак, в том числе реагированию на компьютерные инциденты.

Таким образом, организацию взаимодействия с использованием реестра контактных пунктов ОБСЕ в настоящее время сложно назвать эффективной. И на этом фоне с подачи некоторых государств в ОБСЕ насаждается использование Сети связи ОБСЕ, являющейся дорогостоящим, ненадежным с точки зрения обеспечения безопасности данных и избыточным способом организации взаимодействия.

Далее перейдем к организации взаимодействия в АРФ.

В 2019 году государствами-участниками АРФ была разработана мера укрепления доверия «Реестр контактных пунктов АРФ по безопасности использования ИКТ и самих ИКТ», направленная на повышение эффективности международного сотрудничества в сфере реагирования на компьютерные инциденты. Эта мера доверия предусматривает, также, как и в ОБСЕ, взаимодействие на политическом и техническом уровнях.

Функционирование контактного пункта Российской Федерации для связи на техническом уровне обеспечивает НКЦКИ, взаимодействуя с 23 из 26 участников АРФ.

Концептуальный документ, определяющий упомянутую мною меру доверия, содержит процедуры запроса информации, касающейся компьютерного инцидента, а также реагирования на него.

НКЦКИ при осуществлении взаимодействия с иностранными партнерами придерживается этих процедур. Полагаем, что соответствующие принципы должны быть рас-

смотрены и получить развитие на глобальном уровне, в частности на профильной площадке в ООН.

Кроме того, для проведения двусторонних и многосторонних межведомственных консультаций в целях проработки вопросов эффективного сотрудничества по линии работы ИКЦКИ задействуется площадка Межсессионной встречи АРФ по международной информационной безопасности.

Упомянутый мною «Реестр контактных пунктов АРФ по безопасности использования ИКТ и самих ИКТ» сформирован относительно недавно. Такой подход в организации взаимодействия групп реагирования на компьютерные инциденты на региональном уровне обладает большим потенциалом, к раскрытию которого целесообразно приложить усилия всех государств-участников АРФ.

Полагаем целесообразным при создании глобального реестра контактных пунктов на площадке ООН учесть весь накопленный на региональном уровне опыт, как положительный, так и отрицательный.

Считаем, что для запуска глобального реестра контактных пунктов на первом этапе необходимо установить конкретные цели и принципы его функционирования, определить соответствующие уполномоченные контактные пункты с указанием адресов электронной почты и номеров телефонов, порядок их взаимодействия, а также согласовать базовый набор сведений, необходимый для изучения компьютерной атаки и инцидента.

При этом инициативу о создании сети контактных пунктов на первоначальном этапе считаем дорогостоящим проектом, который в настоящее время не отвечает интересам государств-членов ООН.

## Маурисио Ленин Соза Рубело

Национальная полиция (Никарагуа)

Доброе утро всем делегациям, участвующим в Программе XVI Международного форума «Ассоциация государства, бизнеса и гражданского общества по обеспечению безопасности международной информации».

В составе никарагуанской делегации присутствует Римма Гуссман, которая любезно выступает в качестве переводчика с испанского на русский.

Делегация Никарагуа высоко оценивает возможность принять участие в этом мероприятии; с этой целью мы сделаем краткую презентацию о законодательных достижениях с 2020 года в области киберпреступности и кибербезопасности.

Этим законодательным достижениям способствовала решительная поддержка нашего Правительства примирения и национального единства под председательством командующего Даниэля Ортеги Сааведры и вице-президента Росарио Мурильо Замбраны.

- 3 марта 2020 года наша Дistinguished Национальная Ассамблея ратифицировала «Иbero-американское соглашение о сотрудничестве в области расследования, обеспечения и получения доказательств в области киберпреступности».

Ратификация настоящего Соглашения благоприятствует расследованию, заверению и получению доказательств между властями иbero-американских государств в качестве средства укрепления и ускорения сотрудничества в области киберпреступности.

- 29 декабря 2020 года вступил в силу «Специальный закон 1042 о киберпреступности».
- 29 сентября 2022 года вступила в силу наша «Национальная стратегия кибербезопасности 2020–2025».

Наша стратегия заключается в том, чтобы определить позицию Никарагуа в отношении новой концепции кибербезопасности в преддверии ее усилий по содействию развитию безопасного и надежного киберпространства на территории Никарагуа в рамках политики национальной безопасности.

- В этом же году был утвержден «План действий стратегии кибербезопасности на 2020–2025 годы».



Настоящий План действий разрабатывает пять стратегических осей в соответствии с Национальной стратегией кибербезопасности на 2020–2025 годы, на которые я указываю:

- Первая ось: речь идет об институциональном укреплении
- Вторая ось: направлена на совершенствование правовой базы
- Третья ось: развивает навыки посредством образования и обучения
- Четвертая ось: нацелена на технологическое развитие
- Пятая ось: Обеспечивает безопасность и устойчивость критически важных услуг и инфраструктур на национальном уровне.

Как мы уже упоминали, 29 декабря 2020 года вступил в силу «Специальный закон 1042 о киберпреступности, имеющий следующую цель: предупреждение, расследование, судебное преследование и наказание преступлений, совершенных с помощью информационно-коммуникационных технологий; и применяется к тем, кто совершает преступления на национальной территории и за ее пределами.

Вышеупомянутый Закон состоит из 8 глав и 48 статей, в которых подчеркивается:

- Общие положения
- Преступления, связанные с целостностью компьютерных систем
- Компьютерные преступления



- Компьютерные преступления, связанные с хранением данных
- Киберпреступления, связанные с сексуальной свободой
- Процедуры, меры предосторожности и процедурные меры.
- Международное сотрудничество
- Заключительные положения

Устанавливаются сроки заключения от одного года до 10 лет лишения свободы.

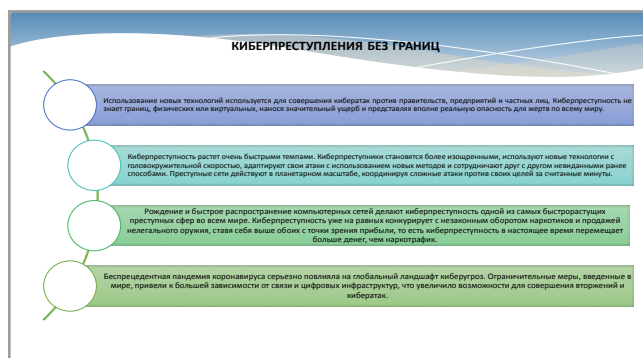
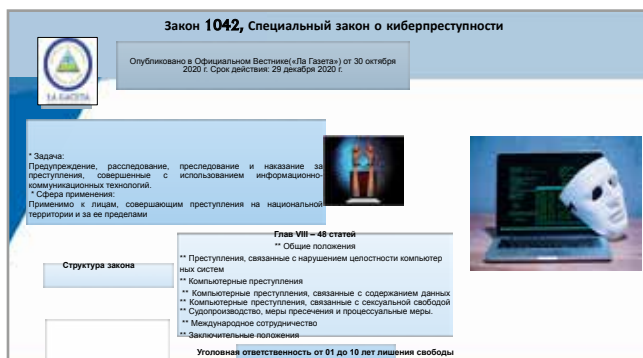
Данное правовое регулирование не позволило нам укрепиться в области кибербезопасности, развивая следующие сильные стороны:

- Правовые рамки для защиты суверенной безопасности Никарагуа.
- Она создает необходимые правовые инструменты для предупреждения, расследования, судебного преследования и наказания за преступления, совершенные на национальной территории или за ее пределами, с использованием информационно-коммуникационных технологий.
- Она укрепляет политику защиты отдельных лиц, семей и общин, которая способствует нашему благому управлению, особенно женщинам, детям, пожилым людям и людям с различными способностями.
- Она обеспечивает защиту нашей критической инфраструктуры, которая пре-

доставляет основные услуги, эксплуатация которых незаменима и позволяет нам альтернативные решения.

Киберпреступления не имеют границ и трагируют всех нас:

- Использование новых технологий используется для совершения кибератак против правительств, предприятий и частных лиц. Киберпреступность не знает границ, ни физических, ни виртуальных, нанося значительный ущерб и представляя вполне реальную опасность для жертв во всем мире.
- Киберпреступность растет очень быстрыми темпами. Киберпреступники становятся все более гибкими, эксплуатируя новые технологии с головокружительной скоростью, адаптируя свои атаки с использованием новых методов и сотрудничая друг с другом способами, невиданными ранее. Преступные сети действуют в планетарном масштабе, координируя комплексные атаки на свои цели за считанные минуты
- Рождение и быстрое распространение компьютерных сетей делают киберпреступность одной из самых быстрорастущих криминальных областей во всем мире. Киберпреступность уже конкурирует на равных с наркотрафиком и продажей нелегального оружия,





позиционируя себя с точки зрения прибыли выше обоих, то есть киберпреступность в настоящее время перемещает больше денег, чем незаконный оборот наркотиков.

- Беспрецедентная пандемия коронавируса глубоко повлияла на глобальный ландшафт киберугроз. Меры блокировки, введенные в отношении мира, привели к большей зависимости от подключения и цифровых инфраструктур, увеличению возможностей для вторжений и кибератак.

Никарагуа укрепляет свои возможности в области предотвращения, разведки и расследования киберпреступлений.

Эти проблемы приводят нас к следующим вопросам:

Что мы делаем? И как мы собираемся это сделать?

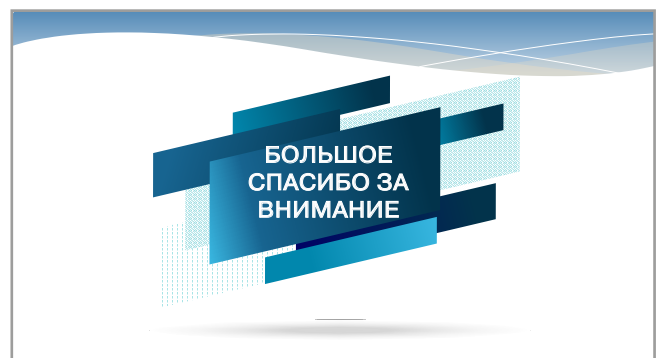
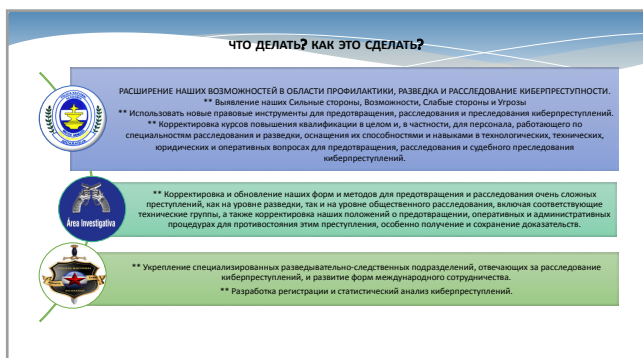
- Мы определяем наши сильные стороны, возможности, слабые стороны и угрозы (SWOT)
- Нам известно о новых правовых документах по предотвращению, расследованию и судебному преследованию киберпреступлений.
- Скорректированы учебные курсы в целом, и в частности для персонала, который работает по специальностям ис-

следований и разведки, предоставляя им навыки и умения в технологических, технических, правовых и оперативных вопросах для предотвращения, расследования и судебного преследования киберпреступлений.

- Корректировка и новаторство наших способов и методов предотвращения и расследования преступлений большой сложности, как на уровне разведки, так и общественного расследования, включает в себя соответствующее техническое оснащение и корректировку наших правил предотвращения, оперативных и административных процедур для противостояния этим преступлениям, особенно сбора и сохранения доказательств.
- Укрепление специализированных разведывательных и следственных подразделений, отвечающих за расследование киберпреступлений, и развитие форм международного сотрудничества,
- И, наконец, разработка семантического и статистического анализа киберпреступлений.

Делегация Никарагуа признательна за Ваше внимание.

Большое спасибо.



## А.Г. Оганесян

Главный редактор журнала  
«Международная жизнь» МИД России,  
член президиума НАМИБ

Конечно, это уже расхожая фраза, что мы с вами находимся в самой бурной фазе информационной войны. В отличие от других войн информационная война — вещь перманентная в истории, особенно когда речь идет о противодействии великих держав, цивилизаций, то победителей в ней быть не может. Могут быть отдельные выигранные баталии. На самом деле, опасность заключается в другом. Культура ненависти или, правильнее сказать, «антикультура ненависти», которая вырабатывалась украинским режимом, в которой нет никаких аллюзий, но прямые параллели с идеологией нацизма, она, выплеснувшись в мировую информационную среду, приобрела глобальный характер, а самое главное, была подхвачена. И неожиданность заключалась в том, с какой беспардонностью, беспринципностью эта гремучая смесь неонацизма, неоязычества, оккультизма, чего хотите, была подхвачена на Западе и ей был придан небывалый импульс.

В свое время ваш покорный слуга участвовал в заседании группы экспертов Совета Европы, которая на министерский уровень готовила документы. Связаны они были с ситуацией в Сербии, когда волна сербофобии привела к расправам над людьми в Косово. И тогда был выработан кодекс, где прямо определялось, что такое hate language, то есть что такое «язык ненависти». Где сейчас эти документы? И кто придерживается этих норм в Европе? Кстати, вот мы говорим о русофобии, но ведь, как вы понимаете, это имеет отношение не только к России. Начнем с того, что подвергается преследованиям через соцсети с указанием кого конкретно надо там подвергать всякого рода преследованиям, упоминаются люди, которые просто сочувствуют России, которые выражают альтернативную точку зрения. Ну и, наконец, любая на расовой почве, на цивилизационной почве ненависть, она выплескивается всегда и на других. Мы с вами помним сербскую кампанию, когда сербы в одночасье превратились в парии, Иран, Ирак и т.д. И вот что примечательно: мы сейчас наблюдаем трансформацию «антикуль-



туры ненависти». Мы привыкли и понимаем, что такое манипуляция сознанием и как она калечит души, но сейчас речь идет уже о том, что социальные сети представляют реальную угрозу здоровью людей и их жизни. Это нечто новое, всегда где-то подспудно присутствующее, но сейчас оно становится очень ярко выраженным и опасным. Приведу почти анекдотический случай, который сам по себе весьма показателен. Бывший военный из Украины видно эмигрировал, попал во Францию и напал на украинских девушек, которые слушали украинские песни, но он подумал, что это русские. А украинские девушки, которых он избил, думали, что это на них напал русский. Вот в этой маленькой картинке отражается вся эта бесовщина ненависти, готовая обрушиться на человека уже не только словом, но и кулаком. Существует и другая угроза, связанная с первой. О ней, кстати, говорилось и не так давно в Государственной Думе. Вот госпожа О. Занко, зампреда комитета Государственной Думы по развитию гражданского общества, отметила: «Мы видим, как участились хакерские атаки на государственные сайты, сайты социально ориентированных некоммерческих организаций. Вот, например, если мы берем специально ориентированные НКО, там вшиты персональные данные миллионов людей, это дети, волонтеры, общественники, добровольцы. Мы считаем важным защитить ресурсы социально ориентированных НКО».

Речь идет о волонтерах, общественниках, которые, например, собирают одежду или медикаменты и как-то помогают участникам СВО. Так вот эти данные надо, конечно, защищать. Для этого сейчас разрабатывается соответствующий законопроект.

А теперь посмотрим на интересные факты, которые следуют из опроса, который провели исследователи Университета Аделаиды в Австралии, проанализировав более 5 млн. англоязычных публикаций по украинской тематике в соцсети Twitter. Выяснилось, в частности, что наиболее влиятельными стали, якобы, «пророссийские» аккаунты, которые ведут живые люди, в эту категорию записали всех тех, кто критически оценивал заполнившую сеть западную пропаганду о событиях на Украине. Их публикации распространялись в том числе в нейтральных и проукраинских сегментах Twitter и получили в среднем гораздо больший охват, чем комментарии, сгенерированные ЦИПСО киевского режима и украинскими ботами. По этому поводу был интересный комментарий со стороны официального представителя МИД Марии Захаровой: «Надо помнить и про то, что авторы исследования умалчивают, что речь здесь идет не о равной конкуренции идей, смыслов и фактов в социальных сетях. Созданные коллективным Западом режим наибольшего благоприятствования для ботов и троллей киевского режима, и их группы поддержки с одной стороны, с другой — жесткая цензура, использование непрозрачных алгоритмов, блокировка и удаление «неправильных» мнений, включая опубликованные на официальных ресурсах, отмену честных критически мыслящих блогеров и журналистов, пытающихся непредвзято разобраться в происходящем. И несмотря на все это наиболее влиятельными все равно оказываются пророссийские аккаунты».

Хотел бы вернуться к языку ненависти. Рыба, как известно, тухнет с головы. Вот несколько наиболее одиозных примеров. Премьер-министр Польши Якуб Моравецкий назвал Россию на весь мир раковой опухолью, это было опубликовано в английском Daily Telegraph, и широко разошлось в соцсетях: «Русский мир — это рак, пожирающий не только большую часть российского общества, но и представляющий смертельную угрозу для всей Европы. Поэтому он должен быть иско-

ренен. Совершенно справедливо, конечно, забанил Россвязьнадзор появившееся в сети выступление депутата сейма Латвии Александра Кирштейнса в Twitter. Вы помните эту историю, когда были арестованы, разогнаны люди, которые протестовали против того, чтобы сносили памятник освободителям Риги: «Надо было, — он пишет, — впустить их всех, а выход закрыть. После чего установить охранные вышки, туалеты, привезти кашу и выпускать только тех, кому посольство России купило билет в один конец — в Москву». К вопросу о «забанивании», некоторые говорят, это нарушение свободы слова, ну нет, перед нами образчик языка ненависти, мы здесь поступаем совершенно в рамках того, что было принято в Совете Европы, пусть кто-то не придерживается, а мы придерживаемся, и это конечно язык ненависти и унижения.

Правда тут возникает не простой вопрос, когда мы противодействуем уже целым платформам, как например Instagram, всегда ли это оправдано? Ведь речь идет не только о том, что мы получаем информацию через некоторые платформы, но и для нас это шанс, как мы видим из результатов исследования в Австралии, выхода на глобальную аудиторию. То есть здесь надо, как бы, сбалансировано подходить к тому, что запрещать, а что оставлять как нужное окно общения с людьми, которые хотят знать правду, хотят объективно разобраться, хотят знать альтернативную антироссийскую точку зрения.

К сожалению, несмотря на заявление верховного комиссара по правам человека в ООН, который осудил дискриминацию и назвал русофобию видом дискриминации, комитет по противодействию всем формам дискриминации ООН никак не отреагировал и не реагирует на запросы в адрес этого комитета с просьбой обратить внимание на то, что налицо отмена русской культуры, отчисление российских студентов, закрытие русских школ, преследование детей россиян, которые учатся в европейских школах и там подвергаются нападкам, избиениям и психологическому давлению и травле, как это было, например, в Бельгии.

А завершить выступление хочу высказыванием швейцарского историка Ги Метанна. Он написал книгу под названием «Запад — Россия. Тысячелетняя война», в которой он

пишет: «Теперь в начале XIX века в разгаре войны информационной русофобия — это сугубо западное явление в том смысле, что всегда было и остается негласным инструментом западноевропейской реальной политики и выражается в активной заведомо враждебной позиции, целью которой являет-

ся если и не нанесение прямого ущерба, то по крайней мере стремление ущемить другого в правах. С этой точки зрения русофобия — сродни расизму: во что бы то ни стало принизить другого, чтобы сподручней было над ним властвовать».

## Санджай Гоэл

Государственный университет штата  
Нью-Йорк (США)

### НЕОБХОДИМОСТЬ СОТРУДНИЧЕСТВА В КИБЕРПРОСТРАНСТВЕ, НЕСМОТРИ НА СРЕМТЕЛЬНО ОБОСТРЯЮЩИЕСЯ КОНФЛИКТЫ МЕЖДУ ГОСУДАРСТВАМИ

Последнее десятилетие ознаменовалось политическими потрясениями и глобальными конфликтами, включая Ближний Восток, Индию, Украину и Африку. Интернет превратился в ключевую составляющую конфликта не только для проведения кибератак, но и для дезинформации и искажения информации. Ни одна страна или блок не могут быть исключены из числа тех, кто занимается пропагандой — она становится универсальной составляющей военной игры. Страх перед иностранным вмешательством и влиянием на внутреннюю политику через Интернет постепенно превращает свободный и открытый Интернет в контролируемый и цензурируемый. В то время как конфликты в Интернете нарастают, развитие новых технологий, основанных на Интернете, продолжается ударными темпами. Самоуправляемые автомобили, смарт-сети, носимые медицинские устройства — все это окажет огромное влияние на наш образ жизни, энергопотребление, здоровье и благополучие. Наша постоянно растущая зависимость от Интернета создала гораздо более обширную область уязвимостей с гораздо более высокими ставками. Сегодня атаки с использованием программ-вымогателей угрожают заблокировать вашу информацию, а завтра атаки с использованием программ-вымогателей будут угрожать заблокировать подачу кислорода пациентам в больницах, ставя под угрозу жизнь и здоровье пациентов.

Использование искусственного интеллекта сделало хакеров гораздо более эффективными в выявлении уязвимостей и проведении атак, и в то же время боты, управляемые искусственным интеллектом, вывели дезинформацию на новый уровень. Возможности кибероружия продолжают расти, и в то же время потенциал катастрофического ущерба продолжает увеличиваться. Гонка кибервооружений, если она будет продолжаться бесконтрольно, приведет к балканизации Интер-



нета — процесс балканизации уже начался с появлением жестких национальных брендауэров не только в Китае, но и во многих других странах, включая Турцию, ОАЭ, Египет, Иран и Вьетнам.

Продолжающиеся глобальные конфликты подрывают взаимное доверие и сделали сотрудничество по разработке и использованию кибероружия неразрешимой задачей, тем более что кибератаки являются неотъемлемой частью военных действий. К счастью, сегодня страны лучше оснащены для противодействия кибератакам и лучше подготовлены к противодействию дезинформации. Это очевидно из отсутствия влияния кибератак на конфликт в Украине и слабого влияния дезинформации на президентские выборы в США.

Идеально было бы избежать конфликтов между странами, однако конфликты неизбежны, и, учитывая транснациональную природу Интернета, нам необходимо продолжать сотрудничать по вопросам, связанным с Интернетом, даже во время конфликтов. Для начала нам необходимо определить области, в которых мы можем сотрудничать — например, у нас есть сотрудничество в области гражданской авиации и морского транспорта. Нам необходимо начать налаживать сотрудничество в области наземного транспорта по мере того, как самодвижущиеся автономные транспортные средства будут повсеместно интегрироваться в общество.



Сейчас идет борьба за контроль над международными организациями: разные страны пытаются ослабить гегемонию США в Интернете. Россия и Китай являются активными сторонниками интернационализации управления Интернетом и обеспечения равных прав стран на регулирование всемирной сети. Китайская модель интернет-суверенитета ставит во главу угла государственный контроль над деятельностью в сети, включающий цензуру и слежку, в то время как США (и их союзники) выступают за открытый интернет с анонимностью, конфиденциальностью и свободой выражения мнений.

И Россия, и Китай активно работают над достижением этих целей, причем Китай - через Международный союз электросвязи, специализированное агентство ООН по информационным и телекоммуникационным технологиям, а Россия - через ГПЭ ООН и форум открытого состава на ГА ООН.

Китайское правительство использует свое лидерство в Международном союзе электросвязи для принятия телекоммуникационных стандартов, которые соответствуют китайскому режиму цензуры и наблюдения, и отстаивает китайское видение архитектуры Интернета. Он выступает за систему слабо связанных между собой сетей, каждая из которых имеет определенные правила, обеспечиваемые через VPN. Это позволит создать контрольные пункты, способные расшифровывать сообщения, обеспечивать соблюдение или отключать трафик. Предстоящие в сентябре выборы нового генерального секретаря и группы высокопоставленных чиновников МСЭ могут заложить основу для того, насколько Китай сможет диктовать правила, стандарты и лучшие практики в отношении новых технологий, таких как сети 5G, в зависимости от того, кто будет избран.

Хотя все страны поддержали бы международную конвенцию по противодействию

использованию информационных технологий в преступных целях, отсутствие взаимного доверия затрудняет эту задачу. Кроме того, сотрудничество в области развития технологий становится все более затруднительным, поскольку страны пытаются создать свой собственный суверенный Интернет. Создание операционных систем, коммуникационных протоколов и аппаратных средств, предназначенных для интернетов стран, со временем приведет к несовместимости, что сделает невозможной реинтеграцию Интернета. Например, Китай и Россия разрабатывают различные варианты операционной системы Linux для внутреннего потребления. Взаимные подозрения уже привели к технологическим войнам между США и Китаем. Ссылаясь на угрозы национальной безопасности, правительство США начало отдавать распоряжения об изъятии оборудования китайского производства из телекоммуникационных сетей и сетей безопасности, при этом основное внимание уделялось ZTE и Huawei. Эпоха сотрудничества в киберпространстве уступила место конкуренции в киберпространстве с конкурирующими протоколами и конкурирующими финансовыми интересами. В условиях взаимозависимости между глобальными компаниями в области программного обеспечения, чипов и аппаратного обеспечения узкоспециальные интересы начинают подавлять инновации.

Дальнейший путь представляется сложным — с конкурирующими глобальными интересами, взаимным недоверием и активными международными конфликтами, которые сводят на нет любые усилия по международному сотрудничеству и ужесточают идеологические позиции. Нам необходимо содействовать здоровым дебатам о реальной золотой середине, где мы сможем продолжать развивать единый Интернет без балканизации и ограничения инноваций в Интернете.

## **В.Н. Бенгин**

*Директор департамента  
кибербезопасности, Минцифры России*

Поскольку Минцифры является ФОИВом, ответственным за выработку государственной политики и нормативно правового регулирования в сфере ИТ, связи, обработки персональных данных, СМИ, включая Интернет, электронной подписи и т.д., вопросы обеспечения международной информационной безопасности для нас имеют принципиально важное значение.

Мы являемся одним из государственных органов, осуществляющих в пределах своей компетенции реализацию государственной политики Российской Федерации в области МИБ и выступаем в качестве Администрации связи Российской Федерации при осуществлении международной деятельности в области связи.

Минцифры уделяет значительное внимание вопросу выстраивания подобного сотрудничества с иностранными государствами как в двустороннем, так и в многостороннем формате и участвует в формировании и отстаивании позиции государства практически на всех специализированных международных площадках.

И нельзя не признать, что многие аспекты развития ИКТ, а также информационной безопасности в настоящее время недостаточно урегулированы, либо урегулированы лишь на региональных уровнях. Примеров таких аспектов множество.

Так, мы видим множество потенциальных угроз, обусловленных недостаточным регулированием в части обеспечения безопасности персональных данных. На сегодняшний день, когда трансграничные потоки персональных данных на территории иностранных государств осуществляются повсеместно, существенные различия в правовых системах государств зачастую не позволяют национальным компетентным органам обеспечить защиту прав своих граждан, являющихся субъектами переданных данных.

В этой связи на различных международных площадках, включая РГОС ООН, мы выступаем за согласование единых для всех государств-членов ООН принципов обработки персональных данных и полагаем, что их



определение позволит значительно повысить уровень защиты персональных данных при соответствующем трансграничном обмене, будет способствовать развитию законодательства в области защиты персональных данных в странах, где такое законодательство недостаточно развито или отсутствует вовсе, а также может помочь выстроить эффективные механизмы взаимодействия уполномоченных национальных органов.

В качестве еще одного примера можно выделить отсутствие глобального механизма обеспечения безопасного функционирования и развития сети Интернет. В настоящее время основные игроки в сфере управления Интернетом не обладают статусом международных организаций и иммунитетом к решениям национальных администраций, в юрисдикции которых находятся. А функции, ими выполняемые, по сути являются транснациональными по характеру.

С последствиями подобного пробела в международно-правовом регулировании мы столкнулись сравнительно недавно, когда рядом иностранных удостоверяющих центров под давлением национальных администраций были отозваны интернет-сертификаты безопасности (TLS-сертификаты), применяемые для организации информационного взаимодействия в сети «Интернет», в том числе федеральными органами государственной власти и крупнейшими организациями, в первую очередь банками.

Указанная задача была решена посредством создания отечественного аналога инфраструктуры выдачи TLS-сертификатов на базе национального удостоверяющего центра в целях обеспечения устойчивого функционирования устройств в российском сегменте сети «Интернет».

Во многом поэтому, а также и по ряду иных причин, мы выступаем за институционализацию вопросов регулирования безопасного функционирования и развития сети Интернет на основе равноправного участия мирового сообщества в управлении глобальной сетью.

Также, разумеется, одним из наиболее чувствительных вопросов является борьба с киберпреступностью. Мы видим необходимость совершенствования международной нормативной базы, создающей механизм взаимодействия компетентных органов для оперативного противодействия такого рода действиям.

В этой связи мы поддерживаем и активно участвуем в процессе по выработке всеобъемлющей конвенции ООН по противодействию преступному использованию ИКТ. В ходе данной работы нами выдвинут ряд предложений, в том числе по криминализации на глобальном уровне деяний, связанных с незаконной обработкой персональных данных; созданием и обеспечением функционирования вредоносных информационных ресурсов; нарушение функционирования информационных систем и информационно-коммуникационных сетей и т.д.

Важным при осуществлении данной работы представляется криминализация не только лишь деяний, напрямую связанных с «вмешательством в работу компьютерных систем», на чем настаивают многие наши западные «пар-

тнеры», но и иных преступлений, масштаб которых несоизмеримо увеличивается с использованием ИКТ. Такой узкий, «западный» подход не позволит нам использовать данный механизм для борьбы с рядом противоправных деяний, включая, к примеру, телефонное мошенничество.

Мы убеждены в том, что обеспечение эффективного международного взаимодействия по вопросам развития, внедрения и использования ИКТ возможно лишь при наличии универсальных нормативных правовых актов обязательного характера, посвященных различным аспектам обеспечения информационной безопасности и закрепляющих, в том числе, принципы взаимодействия всех участников процесса цифровой трансформации.

Не забываем мы и о двустороннем взаимодействии. К примеру, летом этого года проведено два значимых заседания с аналогичными министерствами Ирана и Китая, по итогам которых достигнуты принципиальные договоренности как по сотрудничеству по линии министерств, так и по содействию сотрудничеству национальных коммерческих ИБ компаний. В проработке также находится вопрос заключения двусторонних меморандумов о сотрудничестве с государственными органами ряда иностранных государств по вопросам, отнесенным к компетенции Минцифры.

Учитывая значимость рассматриваемых вопросов, такие дискуссионные площадки, как данный форум, предоставляющие возможность для обмена мнениями специалистам из самых разных учреждений и организаций, могут сыграть очень важную роль в выстраивании общих подходов при осуществлении мероприятий, направленных на обеспечение ИБ в глобальном пространстве.

## С.В. Плохов

*Заместитель начальника Главного управления международно-правового сотрудничества — начальник организационно-правового управления, Генеральная прокуратура РФ*

### **О МЕЖДУНАРОДНОМ СОТРУДНИЧЕСТВЕ ГЕНЕРАЛЬНОЙ ПРОКУРАТУРЫ РОССИЙСКОЙ ФЕДЕРАЦИИ В СФЕРЕ ПРОТИВОДЕЙСТВИЯ ИНФОРМАЦИОННОЙ ПРЕСТУПНОСТИ**

Вынесенная сегодня на обсуждение тема остается крайне актуальной и с каждым годом продолжает требовать к себе всё большего внимания со стороны как государства, так и всего мирового сообщества.

Масштабы информационной преступности обусловлены пандемией COVID-19, широким процессом цифровизации, распространением виртуальных активов и их анонимным трансграничным перемещением.

Взрывной рост киберпреступлений во всем мире не обошел стороной и Россию. Сейчас каждое четвертое регистрируемое в России преступление совершается с использованием информационно-коммуникационных технологий (ИКТ).

Складывающаяся криминогенная обстановка в сфере IT-преступности способствует появлению новой терминологии и классификации способов совершения рассматриваемых преступлений, большинство из которых являются различными формами социальной инженерии. При их использовании потенциальный потерпевший, будучи введенным в заблуждение, добровольно предоставляет мошенникам конфиденциальную информацию, тем самым становясь жертвой преступления.

Практика доказывает эффективность борьбы с подобными явлениями путем проведения широкой разъяснительной работы среди населения. Соответствующая задача в России реализуется в виде размещения социальной рекламы в интернет-пространстве, средствах массовой информации, общественном транспорте. Однако эту работу необходимо своевременно видоизменять, исходя из актуальных на конкретный период угроз, поскольку только в этом случае она может достичь необходимого профилактического эффекта.



При этом в силу способности рассматриваемой категории преступности к трансформации ее структура и динамика продолжают видоизменяться значительно быстрее, чем системы правового регулирования и безопасности, а это, в свою очередь, требует и от законодателей, и от правоприменителей оперативного принятия скоординированных мер, направленных на формирование системы обеспечения информационной безопасности.

В этих целях Генеральным прокурором Российской Федерации Красновым И.В. два года назад создана межведомственная рабочая группа по противодействию информационной преступности, объединяющая представителей ряда российских уполномоченных органов.

Работа группы — не что иное, как реализация функции координации деятельности правоохранительных органов по противодействию преступности данного вида, являющейся одним из ключевых направлений работы органов прокуратуры России в контексте утвержденных указами Президента Российской Федерации в прошлом году Стратегии национальной безопасности и Основ государственной политики Российской Федерации в области международной информационной безопасности.

В рамках ее деятельности, например, разработан и утвержден перечень преступлений, относимых к числу совершенных в сфере



ИКТ. Разработанные критерии позволяют повысить информативность статистических показателей на данном направлении для более оперативного реагирования на развивающиеся в цифровой среде угрозы.

Причем плоды нашей координационной деятельности с каждым годом все очевиднее. Например, по итогам первого полугодия текущего года этого мы уже наблюдаем отрицательную динамику информационной преступности (-8%).

Киберпреступность трансгранична по определению, поэтому деятельность МРГ сосредоточена не только на совершенствовании российского законодательства и практики его применения, но и на вопросах международного сотрудничества в сфере противодействия киберпреступности, включая формирование соответствующих международных механизмов.

Значимым результатом работы группы стала подготовка входящими в ее состав экспертами российского проекта конвенции ООН о противодействии использованию ИКТ в преступных целях, который в июле прошлого года официально внесен в специальный межправительственный комитет ООН. В спецкомитете развернута активная деятельность. Его третья субстантивная сессия завершилась две недели назад, однако нам ещё предстоит большая работа.

В отличие от избранного западными странами узкого подхода к разработке международного документа, направленного на противодействие исключительно компьютерным преступлениям (а это лишь полтора процента в структуре нашей информационной преступности), нами будущая конвенция видится как универсальный механизм борьбы с широким кругом деяний, совершенных с использованием ИКТ.

В российском проекте нашли отражение 23 состава преступлений, включая несанкционированный доступ к персональным данным, незаконное распространение фальсифицированных лекарственных средств и медицинских изделий, терроризм, экстремизм, реабилитация нацизма, незаконный оборот наркотиков, оружия, вовлечение несовершеннолетних в противоправную деятельность и многое другое.

Противоречия со странами Запада имеются и по другим принципиальным моментам, подробно останавливаться на которых мне не

позволяет регламент. Тем не менее, даже не смотря на текущую внешнеполитическую обстановку, мы продолжаем отстаивать свою линию, убеждать в этом другие государства, и заручаться поддержкой всё большего числа делегаций.

Однако даже при таком раскладе мы прекрасно понимаем, что на согласование конвенции и ее принятие уйдут годы, а проблемы надо решать уже сегодня.

Поэтому Генеральная прокуратура Российской Федерации одновременно идёт по пути заключения с компетентными органами иностранных государств соглашений и программ сотрудничества, предусматривающих межпрокурорское взаимодействие в сфере противодействия информационным преступлениям. За последние полтора года Генеральный прокурор России подписал более двух десятков таких документов. Это положительно сказывается и на рассмотрении запросов о правовой помощи — а это на сегодняшний день основной наш инструмент международного сотрудничества по уголовным делам.

Так, например, за 8 месяцев 2022 г. в Генеральной прокуратуре Российской Федерации организовано исполнение более 3 тыс. запросов компетентных органов иностранных государств о правовой помощи по уголовным делам данной категории. По более 2 тыс. исполненным запросам в компетентные органы иностранных государств направлены соответствующие материалы. Наиболее активное взаимодействие в сфере ИКТ ведется с Белоруссией, Арменией, Республикой Корея, Польшей, Турцией и Францией.

Как видно, в целом, несмотря на общую сложную политическую ситуацию, сложившуюся вокруг нашей страны, сотрудничество в правоохранительной сфере в вопросах противодействия преступлениям, совершаемым с использованием ИКТ, продолжается.

Вместе с тем сейчас отдельные юрисдикции отказываются от сотрудничества и обмена данными в правоохранительных целях. От подобной позиции выигрывают только преступники, в связи с чем она неприемлема.

Примечательно, что с марта по август текущего года мы получили более 70 отказов в выдаче лиц, значительная часть из которых принята названными странами по политическим мотивам.



При этом после каждого такого отказа мы предлагаем иностранному государству осуществлять уголовное преследование задержанного, но не выданного нам лица на территории такого государства. Вместе с тем ни в одном случае мы не получили заинтересованность в направлении материалов уголовного дела. Как в иностранных государствах дальше поступают с задержанными по нашим запросам убийцами, насильниками и ворами — для нас остается загадкой.

Очевидно, что такой неконструктивный подход сопряжен с нарушением международ-

ных договоров. В угоду политической конъюнктуре лица, совершившие преступления, остаются безнаказанными.

В то же время мы со своей стороны продолжаем исполнять взятые на себя международные обязательства и открыты к честному взаимовыгодному диалогу с коллегами во всем мире для совместной борьбы с наиболее опасными криминальными вызовами и угрозами современности, к числу которых, несомненно, относится информационная преступность.

## Филипп Бомард

Штатный профессор университета,  
директор лаборатории оборонной  
разведки безопасности (ESR3C)

## ЭКОНОМИЧЕСКАЯ ВОЙНА В СОЧЕТАНИИ С ВОЕННОЙ ЭКОНОМИКОЙ: БАЛАНС МЕЖДУ СТРАТЕГИЧЕСКОЙ БЕЗОПАСНОСТЬЮ И КИБЕРСТАБИЛЬНОСТЬЮ



**Экономическая война в сочетании с военной экономикой :  
Баланс между стратегической безопасностью и  
киберстабильностью**

Филипп Бомард  
Штатный профессор университета  
Директор, Лаборатория оборонной разведки безопасности  
(ESR3C)

XVI Международный форум "Партнерство государства, бизнеса и  
гражданского общества в обеспечении международной  
информационной безопасности"





**Экономическая война или "санкции с применением оружия"**

- ❑ **Блокады и осады всегда были инструментами войны**
  - ❑ Во время Французских войн (1792-1815 гг.) британцы сломили "континентальную систему" Наполеона, призванную ослабить британскую экономику.
  - ❑ История Средиземного моря - это непрерывная череда экономических противостояний, санкций, принуждений и, в конечном итоге, войн.
- ❑ **Первые немецкие теоретические разработки - до 1914 года**
  - ❑ Уже в 1894 году Германия вводит баланс между национальной затарией (зерно, мясо, сырье) и разработкой военных планов для достижения сухопутной победы над Францией и Россией.
  - ❑ Оконная война 1914 года ускорила первые немецкие теоретические разработки экономической войны, породив концепцию "жизненно важных земель". Союзникам потребовалось 2 года, чтобы договориться и обеспечить эффективную блокаду. За 2 года ежедневное городское потребление мяса в Германии снизилось с 2,3 фунтов до 0,3 фунтов. Смертность немецких гражданских лиц, вызванная блокадой, к 1918 году достигла 293 000 человек.

2 Оружейные санкции во время дефицита



**Оружейные санкции как путь 3<sup>го</sup> во время холодной войны**

- ❑ **Чем дальше в холодную войну, тем дальше становилась прямая конфронтация.**
  - ❑ МАД и прямые конфронтации были отброшены как вариант задолго до падения Берлинской стены.
  - ❑ Мятельная экономика (Baumgard, 2012) стала повторяющимся тактическим режимом, который, в свою очередь, привел к сложным проблемам с порядком внутри страны, быстрому росту глобальной криминальной экономики.
- ❑ **Почему экономическая война почти всегда терпит неудачу?**
  - ❑ Исторически экономическая война велась как средство, с помощью которого одна страна могла добиться от другой коммерческой или политической уступки (Braudel, 1949).
  - ❑ После Второй мировой войны "экономическая война" стала средством замены военного принуждения или принуждения к "мировому порядку".
  - ❑ Конечно, с крутой кривой обучения, большинство стран научились строить свою взаимозависимость таким образом, чтобы избежать санкций.

3 Оружейные санкции во время дефицита



**Маоистские теоретизирования и криминализация**

- ❑ **После 1968 года риторики заново изобретают "экономическую войну"**
  - ❑ Санкции и эмбарго быстро осуждаются как "оружие богатых" против "людей слабых"
  - ❑ Харбулат (1989) в своей работе "Машина экономической войны" предлагает концепцию, вдохновленную Мао, где экономическая война становится асимметричным оружием слабых против сильных. Экономические диверсии, саботаж, информационная война представляются как "законный арсенал" экономической войны (поддерживая корневые теории марксистских противостояний).
- ❑ **Но было ли это действительно новым?**
  - ❑ Санкции никогда не обеспечивали соблюдение морали. Крестовые походы уже создали свои вторичные рынки рэкета, грабежа, вымогательства, контрабанды, процветание черных рынков.
  - ❑ Экономическая война была неотъемлемой частью государственного строительства Елизаветы I. Солдаты удачи, охотники за призами и головами были актуальными векторами грабежа и экономической войны.

4 Оружейные санкции во время дефицита



**Каково влияние необратимости истощения ресурсов**

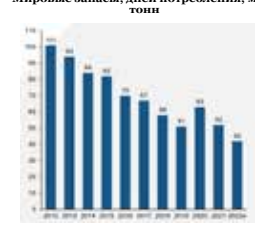
- ❑ **Сложная взаимозависимость возникает, когда применение силы является незначительным фактором (Keohane и Nye, 1977)**
  - ❑ Но параллелизм и соответствие **сильно зависят** от ожидания предстоящей отдачи
  - ❑ Ака в отсутствие взаимной предсказуемости и при уверенности в необратимости истощения ресурсов отказ от соблюдения ("не-режим") может быть лучшим вариантом, когда санкции с применением оружия не стоят ставки?
- ❑ **Истощение может создать необратимые режимы нестабильности**
  - ❑ Стоимость "отказа" от уязвимой взаимозависимости может быть ниже, чем стоимость поддержания взаимно болезненного режима взаимных санкций, когда жизненно важные ресурсы истощаются
  - ❑ Другими словами, если мы уже знаем, что альтернатива будет более неприятной, чем несоблюдение, зачем вообще реагировать на экономические санкции? (учитывая, что другие субъекты согласны с таким восприятием и согласны помочь обойти санкции)

5 Оружейные санкции во время дефицита



**Запасы (почти полностью) израсходованы**

Мировые запасы, дней потребления, млн. тонн



- ❑ 2022 - 2030 гг. рынок в большом дефиците
- ❑ Положительный рост мирового спроса (+3-4% в год)
- ❑ Ограничения предложения из-за энергетических проблем, экологической политики (рост предложения +0-1% в год)
- ❑ Китай (50% рыночного предложения) в структурном дефиците
- ❑ Товарно-материальные запасы на рекордно низком уровне
- ❑ Отраслевые затраты значительно возросли

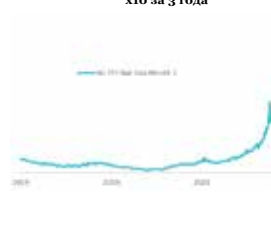
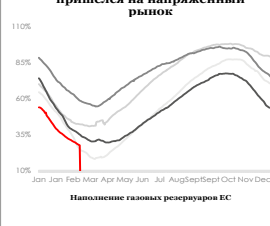
6 Оружейные санкции во время дефицита



**Европейский энергетический рынок: в центре внимания - газ**

Кризис Россия/Украина пришел на напряженный рынок

Цена на газ в ЕС сжалась: рост на 10 за 3 года



7 Оружейные санкции во время дефицита



### Чему мы научились за 8 веков экономической войны?

le cnam  
sécurité défense

**Урок №1: Инфраструктура экономической войны всегда переживает саму войну**

- Эмбарго и санкции создают криминализованные вторичные системы, которые часто становятся доминирующей логикой в конце войны (англо-американская война; наполеоновские войны; французская алжирская война; война в Индокитае и т.д.).

**Урок №2: Неразглашенные санкции укрепляют и диверсифицируют санкционированную страну**

- Британские контрмеры наполеоновской континентальной системы, поскольку они не были должным образом запечатаны, способствовали многочисленным инновациям в бизнесе (и континентальной коррупции).

**Урок №3: Экономическая война всегда перестраивает долгосрочные альянсы**

- Нарушение мирной эксплуатации всегда приводит к вопросу о том, не были ли предыдущие соглашения слишком само собой разумеющимися (ценными и стабилизирующими). Нарушение эксплуатации порождает разведку.

10 Оружейные санкции во время дефицита

### Экономическая война или "санкции с применением оружия"

le cnam  
sécurité défense

**Ссылки:**

- Baumard, P. (1992), "Экономическая война и разведывательное сообщество", *Revue Politique et Parlementaire*, pp. 51-57.
- Baumard P. (1996), "From Information Warfare to Knowledge Warfare: Подготовка к смене парадигмы", в книге: Col. Alan D. Campen, USAF, Douglas H. Dearth and R. Thomas Goodden (Eds.), *Cyberwar: Безопасность, стратегия и конфликт в информационную эпоху*, Фэрфакс, Вирджиния: Ассоциация связи и электроники вооруженных сил, Международная пресса, стр. 147-160.
- Baumard P. (2002), "Les limites d'une économie de la guerre cognitive", in: C. Harbulot, D. Lucas (Eds.), *La guerre cognitive*, Paris : Editions Lavoiselle, p. 35-55, 2002.
- Herzog, S, *Le plan de guerre commerciale de l'Allemagne*, Editions Payot, Paris, 1919.
- Кеокейн Роберт О. Кеокан и Джозеф С. Най (1977), *Власть и взаимозависимость: Мировая политика в переходный период*, Бостон, Литтл, Браун и компания, 1977 г.
- Хейлор, Р.Т., *Экономическая война: санкции, разрушение эмбарго и их человеческая цена*, Бостон: Издательство Северо-восточного университета, 2001.
- Soutou Georges-Henri, *L'or et le sang, les buts de guerre économiques de la Première guerre mondiale*, Paris, Fayard, 1989.

11 Оружейные санкции во время дефицита

## О.Г. Карпович

*д.ю.н., д.п.н., профессор, проректор  
по научной работе Дипломатической  
академии МИД России*

### **ВСЕМИРНАЯ ПАУТИНА: ПОПЫТКИ «ОТМЕНИТЬ» РОССИЮ**

Как и прогнозировали многие эксперты, одной из арен гибридной войны коллективного Запада против России стали безграничные просторы Всемирной сети. Превращение Интернета из средства коммуникации в инструмент решения геополитических задач и сдерживания отдельных государств прослеживалось давно. Собственно, и сам по себе он появился на свет как секретная разработка Пентагона в разгар холодной войны. Конечно, идеологи глобальной либерализации годами уверяли мировое сообщество, что американоцентричность базовых интернет-технологий давно ушла в прошлое, а сама Сеть стала достоянием всего человечества. Под подобными популистскими лозунгами доминирование в виртуальном пространстве обретали интернет-гиганты, получавшие колоссальную власть над умами и кошельками даже не миллионов — а уже миллиардов пользователей. Стремительный рост их влияния на словах должен был положить конец зависимости Сети от контроля со стороны правительства Соединенных Штатов.

Однако, результат оказался совершенно иным. За исключением разве что Китая, еще в 1990-е годы озаботившегося защитой своего веб-суверенитета, большинство государств мира оказались заложниками решений, совместно принимаемых американским правительством и крупнейшими корпорациями. Де-факто и де-юре, контроль над Сетью и ее инфраструктурой по-прежнему находится в руках созданной и базирующейся в США корпорации ICANN — несмотря на многолетние требования большинства стран мира, включая Россию, обеспечить реальную демократизацию и интернационализацию управления интернетом. Стремление Вашингтона всеми силами сохранять главенствующее положение не удивляет. На наших глазах мировой интернет семимильными шагами превращается в пространство тотальной цензуры и площадку для пропаганды единственной, исходящей



из Вашингтона, точки зрения на происходящие события. Украинский кризис лишь ускорил соответствующие процессы.

Разумеется, получили они и солидное дипломатическое прикрытие. Несколько месяцев назад администрация Байдена претворила в жизнь давно вынашивавшуюся идею о подписании, совместно с 60 союзниками, Декларации о будущем Интернета — весьма показательного по стилю и содержанию документа. Формально, его авторы заявляют о необходимости отстаивания идеи «глобального Интернета», открытого, инклюзивного, соответствующего западным представлениям о правах человека. Но в реальности, через Декларацию, по сути, предлагается оформить разделение Сети на два основных сегмента — «демократический» (т.е. проамериканский) и «авторитарный». С учетом закрепленного в США на доктринальном уровне понимания текущей мировой ситуации как «соревнования великих держав», такое разделение открывает «ящик Пандоры». Отнесенные к не-системному (по вашингтонской терминологии, «авторитарному») блоку страны в этой системе координат превращаются в своего рода «законную цель», в отношении которой все средства хороши.

Собственно, Россия в ходе специальной военной операции ощутила на себе насколько велик совместный деструктивный потенциал западных государств и интернет-гигантов

по организации тотальной дискриминации бросившей им вызов страны в сетевом пространстве. А ведь США способны и на куда более масштабные и разрушительные действия, будь то организация беспрецедентных кибератак или отключение от Интернета целых государств. Предпринимаемые Россией шаги по пресечению этих угроз, в том числе, через воплощение в жизнь закона «о суверенном Интернете» крайне важны. Но необходимо смотреть на ситуацию масштабнее и действовать, в том числе, через мобилизацию союзников. Как показывает список подписантов Декларации, США сегодня в меньшинстве — кроме их сателлитов этот документ практически никого не заинтересовал. На фоне скандалов последних десятилетий, включая откровения Сноудена, вашингтонская демагогия на тему верховенства крайне превратно понимаемого права и размытых либеральных ценностей, все чаще дает обратный эффект. Большинство стран-членов ООН не могут и не хотят смириться с реальностью, в которой под лозунгами о равенстве и открытости предпринимаются попытки закрепить глобальный диктат американского гегемона.

Интернетизация практически всех сфер жизни, достигшая пика с началом пандемии коронавируса, не оставляет нам шанса отгородиться от глобальной Сети. Но мы не должны забывать и о том, что Интернет — источник не только ярких возможностей и полезной информации, но и деструктивного контента, а также непосредственных угроз национальной безопасности, генерируемым инициаторами новой холодной войны в тех же США. Многочисленные попытки России наладить двусторонний диалог с Вашингтоном по вопросу о кибербезопасности не дали результата. Вроде бы обещавшие конструктив многосторонние переговоры по линии ООН, приблизившиеся к прорыву полгода назад, с подачи американской стороны зашли в тупик. Текст той же Декларации о будущем Интернета прямо обозначает стремление сформулировать видение будущего Сети, существующее в воображении американцев. России в этом будущем создатели и подписанты Декларации места явно не находят. Соответственно, наша цель должна состоять в планомерном выстраивании инфраструктуры, альтернативной той, что изначально заточена на зависимость от

США. Заручившись поддержкой других центров силы, в особенности — стран БРИКС, мы, безусловно, решим эту задачу. Решим, ответив на скандальную Декларацию конкретными действиями, направленными на освобождение глобальной сетевой экосистемы от воздействия одной сверхдержавы, которая всё никак не может смириться с тем, что времена однополярного доминирования остались далеко позади.

Как писал Гегель, история повторяется дважды — как трагедия, и как фарс. Трагедию мы уже наблюдали. Ровно сто лет назад, когда из пламени Гражданской войны возникло новое государство — Советский Союз — Запад в лице колониальных держав и примкнувших к ним Соединенных Штатов попытался с ходу изолировать СССР, выражаясь современным сленгом — «отменить» его. Что из этого вышло, мы все помним — в порыве антисоветской истерии страны Антанты допустили возникновение «Оси Берлин-Рим-Токио»; в итоге, отсутствие единства и солидарности между антифашистскими силами сделало неизбежным начало Второй мировой. За это время, столкнувшись с западным бойкотом Москва, с одной стороны, активно работала с несистемными силами в Европе и Америке, с другой — деятельно развивала дипломатию на других направлениях. Через несколько десятилетий после своего возникновения, СССР располагал огромной и постоянно, по мере развития процессов деколонизации, расширяющейся сетью альянсов со странами так называемого «третьего мира», установил фактический контроль над Восточной Европой, обзавелся политическими союзниками и бизнес-партнерами в «западном блоке». В начале 1950-х годов Вашингтон и европейские столицы захлестнула истерия насчет набирающей мощь и подступающей «красной угрозы». Кампания по изоляции Союза с треском провалилась. Лишь по счастливому стечению обстоятельств, последовавшая холодная война не переросла в ядерную.

Сегодня мы видим, что страны «победившей демократии» так и не научились делать выводы из своих ошибок. Как и в ситуации с молодым СССР, США и их сателлиты надменно уверены в своих силах. В ежедневном режиме повторяются мантры о том, что Россия в результате объявленной ей санкционной



войны беспрецедентно изолирована — но, похоже, на Западе занимаются банальным самовнушением. Дебаты в Генассамблее ООН, которые с маниакальной настойчивостью иницирует Вашингтон, дабы найти подтверждение собственной пропаганде, дают совсем иную картину. К примеру, страны Азии и Африки, в большинстве своем, демонстративно отказались поддерживать инициативу по исключению России из Совета по правам человека — не голосуя, выступив «против» или воздержавшись. Да и из тех, кто, что называется, взял под козырек, много ли искренних сторонников «отмены России»? Или их представители нажимают нужную кнопку, столкнувшись, как подробно объяснил президент А. Вучич, с беспрецедентным и агрессивным давлением? Если приглядеться, якобы сколоченная Байденом антироссийская коалиция — типичный колосс на глиняных ногах. Она базируется на принуждении, вассальной зависимости, лжи и пропаганде.

Раздражение американской стратегией будет неизбежно и стремительно нарастать по нескольким причинам. Во-первых, на дворе давно не 90-е годы, когда в мире существовал один полноценный центр силы. Для многих стран бывшего «третьего мира» ориентиром уже много лет является не Вашингтон, а региональные державы — страны БРИКС и их партнеры, которые, к нескрываемому раздражению США, вовсе не стремятся маршировать в общем строю под командованием «просвещенного» Запада. В тот момент, когда будут созданы механизмы по обходу вторичных санкций и минимизации издержек от невыполнения американских ультиматумов — а соответствующая работа идет полным ходом — региональные экономические системы по сигналу из Пекина, Нью-Дели, Претории, Бразилиа и стран ОПЕК, смогут оперативно перестроиться на еще более интенсивное сотрудничество с Москвой. А тогда и нужда в лишнем политесе и выслушивании лекций евро-атлантистов быстро пропадет.

Во-вторых, уже сегодня украинский конфликт для большинства развивающихся государств является малоинтересным отдаленным эпизодом, тогда как масштабный продовольственный кризис, вызванный перебоями в поставках зерна, рост цен на энергоносители, коллапс логистических цепочек — проблемы

куда более реальные и осязаемые. По мере усиления внутреннего напряжения, вызванного обнищанием и голоданием населения, открыто продвигаемая Евросоюзом идея победы над Россией на поле боя в войне до последнего украинца, будет выглядеть в глазах африканских, азиатских и, потенциально, латиноамериканских правительств все более циничной и оторванной от реальности, в которой живут и страдают их граждане.

В-третьих, и это, пожалуй, самый важный момент, тот самый вчерашний «третий мир» прекрасно знает цену американским заявлениям о борьбе за демократию и хорошо понимает, что имеет в виду Президент России В.В. Путин, говоря про «империю лжи». Не США ли вместе с Европой годами поддерживали диктатуры по всей планете, жестоко подавлявшие национально-освободительные движения? Разве не они провоцировали перевороты, кровопролитные восстания и гражданские войны для достижения своих весьма прагматичных идеологических и экономических целей? Да и интервенции с катастрофическими последствиями, причем, под сфальсифицированными предлогами, за пределами страдающего коллективным Альцгеймером Запада памятливы практически всем. Соответственно, и доверия к американской позиции по украинскому вопросу у видевших реальное лицо Вашингтона государств немного.

Не говоря уже о том, что сам киевский режим, одновременно героизировавший поборников нацизма и насильно внедрявший так называемые либеральные европейские ценности в культуру, основанную на традиционализме, точно не был образцом для других развивающихся стран. В Африке и Азии прекрасно понимают, что из себя представляет протянутая Западом рука дружбы. Там найдется немного правительств, которые так или иначе не ощутили беспардонное давление, в том числе, санкционное, как по незначительным вопросам (например, о правах трансгендеров и гей-браках), так и в критически важных областях. В частности, в том, что касается борьбы с терроризмом, где призывы США к инклюзивности, соблюдению прав человека, показной гуманности, выдавали полное непонимание местной специфики и подрывали эффективность противостояния этому злу. Им куда легче почувствовать солидарность с «от-

меняемой» Россией, чем с полулегитимным, марионеточным украинским режимом.

Запустив процессы по изоляции нашей страны, Запад, как и век назад, попал в плен собственных иллюзий. Мир намного ярче и многообразнее, плюралистичнее, чем его представляют в вашингтонских и брюссельских кабинетах. Де-факто, американо-европейский альянс, навязывая развивающимся странам эгоистичную и игнорирующую их ча-

яния игру, скорее, самоизолируется. «Отмена России» превращается в фарс — но фарс с далеко идущими последствиями. Поставив на кон все свое влияние в борьбе за выживание украинского проекта «анти-Россия», США и их союзники идут прямым курсом к окончательной утрате гегемонии даже в тех частях планеты, где она по недоразумению до сих пор сохранялась. И очередь из желающих заполнить возникшие лакуны уже выстраивается.



# **КРУГЛЫЙ СТОЛ № 1**

## **ОБЕСПЕЧЕНИЕ СУВЕРЕНИТЕТА ГОСУДАРСТВ В ГЛОБАЛЬНОЙ ИКТ-СРЕДЕ**

### **Модератор:**

*Капустин А.Я.*, научный руководитель Института законодательства и сравнительного правоведения при Правительстве Российской Федерации, президент РАМП, д.ю.н., профессор, заслуженный деятель науки Российской Федерации

## А.А. Стрельцов

д.т.н., д.ю.н., профессор,  
член-корреспондент Академии  
криптографии РФ, вице-президент НАМИБ

### ВНЕШНЯЯ И ВНУТРЕННЯЯ ФОРМЫ ПРОЯВЛЕНИЯ СУВЕРЕНИТЕТА ГОСУДАРСТВА В ИКТ-СРЕДЕ

Как отметил в докладе Президент Национальной ассоциации международной информационной безопасности В.П. Шерстюк, международное сообщество постепенно переходит от обсуждения актуальности обеспечения МИБ к поиску способов решения проблем формирования системы международной информационной безопасности.

К числу таких проблем относятся противодействие международной киберпреступности и практическое применение норм ответственного поведения государств в ИКТ-среде. Российский проект конвенции ООН о противодействии использованию информационных и коммуникационных технологий в преступных целях в 2022 году уже стал предметом обсуждения в Специальном комитете ООН открытого состава. Проблема применения норм ответственного поведения государств в ИКТ-среде находится в центре внимания экспертов международного сообщества.

Основными источниками норм являются рекомендации ГПЭ ООН (2015 г., 2021 г.), а также резолюции Генеральной Ассамблеи ООН, одобренные большинством участников обсуждения<sup>1</sup>.

С формальной точки зрения нормы ответственного поведения государств в ИКТ-среде не являются ни правовыми нормами, ни нормами «мягкого права». Данные нормы могут рассматриваться как средство привлечения дополнительного внимания международного сообщества к вопросам международного нормативного регулирования применения ИКТ. Опыт практического применения норм может помочь конкретизировать проблемы адаптации норм и принципов международного права и мер укрепления взаимного доверия в ИКТ-среде.

Обсуждение проблем формирования системы международной информационной без-



опасности на заседаниях сессий Генеральной Ассамблеи ООН, в ГПЭ ООН и Рабочей группе открытого состава<sup>2</sup> показывает единодушную поддержку международным сообществом применения норм ответственного поведения государств в ИКТ-среде.

Экспертами Ассоциации накоплен определенный опыт исследования этой проблемы.

В 2018–2020 гг. группой экспертов под эгидой Международного исследовательского консорциума информационной безопасности и Национальной ассоциации международной информационной безопасности, было выполнено исследование некоторых методологических вопросов применения норм ответственного поведения государств в ИКТ-среде. Группа объединила экспертов Московского государственного университета имени М.В. Ломоносова (РФ), Института Восток-Запад (США), Института киберполитики (Эстония) и Фонда «ИКТ за мир» (Швейцария). Отчет о результатах этой работы размещен в 2020 г. на сайте нашей Ассоциации.

При оценке результатов проведенного исследования необходимо учитывать два обстоятельства.

С одной стороны, это действительно бесценный опыт работы в составе международной группы экспертов высокого уровня, кото-

1 A/70/174, A/RES/73/27, A/RES/75/240

2 Final Substantive report. Open-ended working group on developments in the field of information and telecommunications in the context of international security. A/AC.290/2021/CR.P.2



рые уже длительное время изучают проблемы противодействия угрозам нарушения международного мира и безопасности посредством использования ИКТ.

С другой стороны, осталось разочарование тем, что совместная работа не привела к консолидации мнения коллектива относительно перспектив практического использования полученных результатов. Эксперты западных стран уже после подготовки материалов проекта выразили желание включить в него отдельный комментарий. В этом комментарии было отмечено, что «существуют не только политические, но также и фундаментальные методологические различия в том, как западные и российские ученые подходят к нормам поведения и международному праву. Существующие различия делают почти невозможным для западных коллег признание и оценку предложений, вносимых российскими коллегами».

Как представляется, политические расхождения в подходах к формированию механизмов применения норм ответственного поведения государств в ИКТ-среде в ходе проведения Российской Федерацией специальной военной операции на Украине вполне проявились. Видимо наши западные коллеги исходят из того, что при сохранении однополярного мироустройства во главе с США разрешение проблем применения норм будет осуществляться на основе распространения суверенитета этого государства на всю ИКТ-среду.

Более сложный характер имеет вопрос о фундаментальных методологических расхождениях в подходах к изучению проблемы применения норм ответственного поведения государств в ИКТ-среде.

Полагая предпочтительным многополярный мир, в котором данная проблема будет решаться с участием всех заинтересованных государств на основе равноправного и уважительного диалога, представляется важным четко сформулировать методологическую основу решения проблемы, которая может стать основой для международного сотрудничества в проведении соответствующих исследований.

Методологическая основа может включать четыре следующих базовых положения.

1. Система международной информационной безопасности – это система от-

ношений между суверенными государствами в области обеспечения безопасности в ИКТ-среде, включающая:

- международное сотрудничество в области устойчивого развития общества на основе использования потенциала глобальной ИКТ-среды;
- защиту национальных интересов в глобальном информационном пространстве;
- противодействие попыткам ущемления суверенитета государств в решении проблем защиты национальных интересов в ИКТ-среде.

2. Суверенитет государства в ИКТ-среде есть его верховенство в регулировании использования ИКТ и национальной информационной инфраструктуры гражданами, организациями и органами государственной власти, находящимися на государственной территории.

3. Суверенитет государства в ИКТ-среде обеспечивается деятельностью органов государственной власти и правомерной деятельностью граждан по следующим направлениям:

- поддержание устойчивого функционирования национального сегмента ИКТ-среды;
- поддержание правомерного использования ИКТ и информационной инфраструктуры;
- сотрудничество по вопросам соблюдения международных обязательств в области безопасности использования ИКТ и глобальной информационной инфраструктуры.

4. Соблюдение международных обязательств, вытекающих из норм и принципов международного права и касающихся поведения государств в ИКТ-среде, может быть обеспечено сотрудничеством по следующим вопросам:

- имплементация норм ответственного поведения государств в ИКТ-среде в национальное законодательство;
- международно-правовое закрепление границ национальных сегментов в ИКТ-среде;
- закрепление международного правового режима безопасности объектов национальных сегментов ИКТ-среды;

- закрепление требований к объектам национальных сегментов ИКТ-среды, обеспечивающих возможность получения юридических фактов по динамике правоотношений, связанных с нарушением международного правового режима безопасности объектов национальных сегментов ИКТ-среды.

Как представляется, на основе сформулированных положений может быть подготовлен проект универсального международного договора о применении норм ответственного поведения государств в ИКТ-среде, в полной мере соответствующий духу и букве Устава ООН, принципам и нормам международного права.

## **Т.А. Полякова**

*д.ю.н., профессор, главный научный сотрудник, и.о. заведующего сектором информационного права и международной информационной безопасности Института государства и права РАН, Заслуженный юрист Российской Федерации*

## **А.А. Смирнов**

*к.ю.н., доцент, старший научный сотрудник сектора информационного права и международной информационной безопасности Института государства и права РАН*

### **ПРОБЛЕМЫ ИМПЛЕМЕНТАЦИИ ДОБРОВОЛЬНЫХ И НЕОБЯЗАТЕЛЬНЫХ НОРМ ОТВЕТСТВЕННОГО ПОВЕДЕНИЯ ГОСУДАРСТВ В ИКТ-СРЕДЕ В НАЦИОНАЛЬНОЕ ЗАКОНОДАТЕЛЬСТВО**

Процессы цифровой трансформации обуславливают необходимость «модернизации правовых подходов к урегулированию новых общественных отношений»<sup>1</sup>. А.В. Минбалева обосновано указывает на то, что в современную цифровую эпоху методы правового регулирования должны быть достаточно гибкими и обеспечивать оперативную выработку системы способов и средств реагирования на новые угрозы и вызовы<sup>2</sup>. Исследования показывают, что эти выводы особенно значимы для международно-правового регулирования сферы международной информационной безопасности (далее — МИБ), где традиционные правовые источники регулирования в виде международных договоров пока недостаточно развиты. В этой ситуации важное значение имеет принятие и реализация иных международных актов в данной сфере, включая политико-декларативные документы и акты «мягкого права».

Одним из таких документов выступают *добровольные и необязательные нормы ответственного поведения государств в ИКТ-среде*. Данные нормы были закреплены в докладах Группы правительственных экспертов по до-



стижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности A/70/174 (далее — Доклад ГПЭ 2015) и A/76/135 (далее — Доклад ГПЭ 2021). Генеральная Ассамблея ООН на 75-ой сессии рекомендовала данные нормы для рассмотрения государствами. По мнению международного сообщества «применение норм ответ-

<sup>1</sup> Полякова Т.А. Цифровизация и синергия правового обеспечения информационной безопасности // Информационное право. 2019. № 2. С. 4.

<sup>2</sup> Цифровая трансформация: вызовы праву и векторы научных исследований: монография / Под общ. ред. А.Н. Савенкова; отв. ред. Т.А. Полякова, А.В. Минбалева. М.: РГ-Пресс, 2021. С. 62.

ственного поведения государств в ИКТ-среде параллельно с применением принципов и норм международного права может способствовать укреплению международного мира и безопасности»<sup>3</sup>.

Следует обратить внимание, что ранее, в 2011 г. Россия, КНР, Таджикистан и Узбекистан представили Генеральной Ассамблее ООН «Правила поведения в области обеспечения международной информационной безопасности»<sup>4</sup>. В 2015 г. был направлен второй обновленный вариант этого документа<sup>5</sup>. Полагаем, что указанный документ сыграл значимую роль в работе Группы правительственных экспертов ООН третьего и четвертого созыва, и был учтен при подготовке их итоговых докладов.

В Докладе ГПЭ 2015 группа предложила государствам рассмотреть «рекомендации в отношении добровольных и необязательных норм, правил или принципов ответственного поведения государств, призванных способствовать обеспечению открытой, безопасной, стабильной, доступной и мирной ИКТ-среды» (п. 13).

### **Правовая природа добровольных и необязательных норм ответственного поведения государств в ИКТ-среде**

Правовая природа добровольных и необязательных норм ответственного поведения государств в ИКТ-среде раскрыта в докладах ГПЭ 2015 и 2021. Согласно указанным докладам, добровольные и необязательные нормы ответственного поведения государств в ИКТ-среде не предусматривают ограничения или запрета действий, согласующихся с нормами международного права, т.е. по сути, эти нормы не устанавливают новых правовых ограничений для государств. При этом следует отметить, что в Докладе ГПЭ 2021 закреплено, что «нормы и существующее международное право существуют параллельно». Однако данное утверждение представляется дискуссионным, поскольку добровольные и необязательные нормы ответственного по-

ведения государств в ИКТ-среде, направлены на детализацию основополагающих принципов и норм международного права относительно ИКТ-среды.

Вместе с тем в докладах ГПЭ обозначается возможность разработки в перспективе дополнительных норм и, отдельно, отмечается возможность, что при необходимости возможна разработка в будущем «дополнительных твердых обязательств», т.е. юридически обязывающих международно-правовых норм. Российская Федерация много лет выступает с инициативой о принятии универсального международного договора в сфере международной информационной безопасности.

Также в докладах ГПЭ отмечается, что нормы ответственного поведения государств в ИКТ-среде отражают ожидания международного сообщества, определяют стандарты ответственного поведения и позволяют международному сообществу давать оценку действиям и намерениям государств. Таким образом, несмотря на отсутствие обязательной юридической силы, данные нормы могут рассматриваться в качестве определенных стандартов, позволяющих давать политико-правовую оценку действий государств в ИКТ-среде.

### **Проблемы имплементации добровольных и необязательных норм ответственного поведения государств в ИКТ-среде в национальное законодательство**

Основная сложность имплементации добровольных и необязательных норм ответственного поведения государств в ИКТ-среде в национальное законодательство состоит в том, что в отличие от международных договоров, для необязательных норм в национальном законодательстве, равно как и в международном праве, не установлен порядок такой имплементации.

Поэтому, на наш взгляд, в данном вопросе необходимо отталкиваться от общих принципов и норм международного права. В частности, имплементации государствами норм ответственного поведения государств должна

3 Применение норм ответственного поведения государств в ИКТ-среде и международное сотрудничество: реферат по результатам исследования. М.: Национальная ассоциация международной информационной безопасности, 2022. С. 7.

4 Письмо постоянных представителей Китая, Российской Федерации, Таджикистана и Узбекистана при Организации Объединенных Наций от 12 сентября 2011 года на имя Генерального секретаря. A/66/359. URL: [https://digitallibrary.un.org/record/710973/files/A\\_66\\_359-RU.pdf](https://digitallibrary.un.org/record/710973/files/A_66_359-RU.pdf) (дата обращения: 02.06.2022).

5 Письмо постоянных представителей Казахстана, Китая, Кыргызстана, Российской Федерации, Таджикистана и Узбекистана при Организации Объединенных Наций от 9 января 2015 года на имя Генерального секретаря. A/69/723. URL: <https://digitallibrary.un.org/record/786846?ln=en> (дата обращения: 02.06.2022).

осуществляться в соответствии с принципами государственного суверенитета, суверенного равенства государств, разрешения международных споров мирными средствами таким образом, чтобы не подвергать угрозе международный мир и безопасность и справедливость, отказа в международных отношениях от угрозы силой или ее применения как против территориальной неприкосновенности или политической независимости любого государства, так и каким-либо другим образом, несовместимым с целями ООН, уважения прав человека и основных свобод, невмешательства во внутренние дела других государств.

В силу необязательного характера рассматриваемых норм в плане имплементации должно признаваться право государств самостоятельно выбирать способы и формы обеспечения их выполнения исходя из принципа государственного суверенитета с учетом особенностей правовой системы. Кроме того, государства исходя из национальных интересов имеют право не выполнять или выполнять в ограниченном объеме отдельные добровольные и необязательные нормы ответственного поведения государств в ИКТ-среде.

Вместе с тем содействие имплементации должно основываться на общем понимании того очевидного обстоятельства, что выражение приверженности всеми государствами-членами ООН добровольным, необязательным нормам ответственного поведения государств в ИКТ-среде и принятие мер по их наиболее полному выполнению содействует достижению общей задачи предупреждения конфликтов в ИКТ-среде и мирному разрешению возникающих в этой области споров в соответствии с Уставом ООН. В случае же массового применения государствами избирательного подхода к выполнению добровольных, необязательных норм ответственного поведения государств в ИКТ-среде их ценность и эффективность как средства предотвращения конфликтов в ИКТ-среде будет существенно снижаться.

При имплементации добровольных и необязательных норм ответственного поведения государств в ИКТ-среде государства должны принимать во внимание рекомендации, содержащиеся в резолюциях Генеральной Ассамблеи ООН «Достижения в сфере информатизации и телекоммуникаций в контексте

международной безопасности», докладах Группы правительственных экспертов ООН по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности, Рабочей группы открытого состава по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности и Рабочей группы открытого состава по вопросам безопасности в сфере использования ИКТ и самих ИКТ.

Что касается конкретных механизмов добровольных и необязательных норм ответственного поведения государств в ИКТ-среде, то, по нашему мнению, они должны предусматривать:

- а) принятие государствами таких законодательных и иных мер, которые необходимы для имплементации норм ответственного поведения государств в ИКТ-среде;
- б) учет норм ответственного поведения государств в ИКТ-среде при разработке и корректировке национальных стратегий (доктрин, концепций) обеспечения безопасности в ИКТ-среде, законодательных и иных правовых актов;
- в) учет норм ответственного поведения государств в ИКТ-среде при разработке и заключении проектов двусторонних и многосторонних международных соглашений (договоров) в области обеспечения безопасности в ИКТ-среде.

В целях содействия имплементации добровольных и необязательных норм ответственного поведения государств в ИКТ-среде государства должны осуществлять диалог с частным сектором, научными и техническими кругами и гражданским обществом.

Учитывая, что имплементация добровольных и необязательных норм ответственного поведения государств в ИКТ-среде затрагивает компетенцию различных государственных ведомств, представляется целесообразным определение национального координатора по применению данных норм.

Важным фактором повышения эффективности имплементации добровольных и необязательных норм ответственного поведения государств в ИКТ-среде является обмен положительным опытом в данной сфере между государствами. Для этой цели могут использоваться различные форматы между-



народного сотрудничества: международные конференции, подготовка специальных докладов, проведение научных и аналитических исследований, экспертные встречи и семинары и т.д.

Одной из приоритетных форм для обмена положительным международным опытом служит подготовка обзорных докладов имплементации государствами добровольных и необязательных норм ответственного поведения государств в ИКТ-среде. При этом важно подчеркнуть, что подготовка обзора

ведущейся на национальном уровне работы по имплементации норм ответственного поведения государств в ИКТ-среде, его распространение в органах Организации Объединенных Наций и направление в иные страны-участницы является суверенным правом государств. В этой связи мы разделяем позицию МИД России о недопустимости введения механизма обязательных отчетов государств об имплементации добровольных и необязательных норм ответственного поведения государств в ИКТ-среде.

## Е.С. Зиновьева

*д.п.н., профессор, заместитель директора  
Центра международной информационной  
безопасности и научно-технологической  
политики МГИМО МИД России*

### АКТУАЛЬНЫЕ ТЕНДЕНЦИИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОГО СУВЕРЕНИТЕТА В МНОГОПОЛЯРНОМ МИРЕ

В условиях масштабной и повсеместной цифровой трансформации на современном этапе возрастает количество угроз международной информационной безопасности. Современные технологии, такие как использование больших данных, дополненной и виртуальной реальности, технологии искусственного интеллекта, блокчейна и интернета вещей, создают новые возможности для экономического роста и развития, но при этом порождают и новые, высокотехнологичные угрозы национальной и международной информационной безопасности. В современных условиях эти угрозы существенно обостряются. Россия после начала специальной военной операции на Украине сталкивается с беспрецедентным количеством кибер-атак. При этом нельзя не отметить успешную деятельность всех субъектов информационной политики России (государственных ведомств, бизнеса, академического и научного инженерного сообщества) в области отражения кибер-атак и обеспечения информационной безопасности государства. Однако, трансграничная природа глобального информационного пространства способствует тому, что угрозам от растущей кибер-нестабильности подвергается вся международная система. Формирование многополярного мира диктует необходимость в устойчивом развитии глобального цифрового пространства, выработке международных соглашений по обеспечению информационной безопасности.

Специальная военная операция стала вехой на пути к новому многополярному миропорядку. Как отметил Президент В.В. Путин, речь идет о «переходе от либерально-гло-



балистского американского эгоцентризма к действительно многополярному миру, основанному на подлинном суверенитете народов и цивилизаций»<sup>1</sup>. Действующая версия Концепции внешней политики, утвержденная Президентом в 2016 г., отмечает, что продвижение к многополярному мироустройству идет небесконфликтно, сопровождается обострением глобальных и региональных противоречий, межгосударственной конкуренцией, повышением роли фактора силы в мировой политике<sup>2</sup>. Все вышеперечисленные тенденции находят отражение и в цифровой сфере. При этом в основе внешней политики России лежат следующие принципы: самостоятельность, многовекторность, прагматизм, открытость, стремление к решению всех проблем политико-дипломатическими средствами с соблюдением международного права. Они сохраняют свое значение и в области международной информационной безопасности<sup>3</sup>. Особый акцент во внешней политике России в условиях многополярного мира делается на защиту и обеспечение государственного суверенитета, в том числе в цифровом пространстве.

В самом широком смысле под суверенитетом государства понимается полнота власти

1 <https://www.interfax.ru/russia/851061>

2 Концепция внешней политики Российской Федерации. Утверждена Указом Президента 30.11.2016 год. URL: <http://kremlin.ru/acts/bank/41451>

3 Дробинин А. Уроки истории и образ будущего: размышления о внешней политике России // Международная жизнь. 2022. URL: <https://interaffairs.ru/news/show/36410>

государства внутри страны и независимость на международной арене. Первоначально государственному суверенитету предполагался контроль государства над определенной территорией, ограниченной государственными границами, однако по мере развития и эволюции данной категории, суверенитет стал распространяться на новые пространства — воздушное пространство, континентальный шельф государства. Сегодня важнейшей задачей России становится защита и обеспечение научно-технологического суверенитета, важной составляющей которого является цифровой суверенитет.

В современных геополитических условиях крайне актуальной становится суверенизация всех областей жизнедеятельности, включая идейную сферу, политическую систему, культуру, науку, экономику, финансы и другие, при открытости к самому широкому взаимно обогащающему равноправному международному сотрудничеству, может гарантировать устойчивое развитие России и достойное место нашей страны в многополярном миропорядке<sup>4</sup>. В этих условиях важным направлением международного сотрудничества становится обеспечение цифрового суверенитета. Однако, суверенизация не означает закрытости. Наоборот, Россия остается открытой к международному сотрудничеству и ставит задачей формирование инклюзивного и демократичного режима информационной безопасности с учетом интересов всего международного сообщества, что особенно востребовано в текущих геополитических условиях складывания нового многополярного порядка.

Еще с 1998 года Россия продвигает инициативу выработки правил ответственного поведения государств в глобальном информационном пространстве. Россия исходит из обязанности государств соблюдать в процессе использования ИКТ — наряду с другими принципами международного права — такие принципы, как государственный суверенитет, суверенное равенство, разрешение споров мирными средствами и невмешательство во внутренние дела других государств. Тезис о важности уважения государственного суверенитета нашел отражение в работе Рабочей группы ООН первого и второго созывов.

Сегодня государства и эксперты согласны с тем, что наметилась тенденция к фрагментации глобального информационного пространства. При этом сохраняется стремление ряда государств стран Запада использовать свое технологическое лидерство для давления на другие страны в цифровом пространстве и разрушения их суверенитета в цифровом пространстве. На достижение данной цели и направлены продвигаемые США проекты, альтернативные российским подходам в цифровой сфере, среди которых — Декларация о будущем интернета от 2022 года, к которой на сегодняшний день присоединились порядка 60 государств. При этом, в числе угроз безопасности Интернета обозначена информационная политика так называемых авторитарных государств, которые запрещают доступ к глобальным он-лайн платформам и цифровым инструментам. Очевидно, что речь вновь идет о России и Китае, уже обозначенных в предыдущей редакции, а одна из задач данного инструмента — ограничение суверенитета всех стран в цифровом пространстве, за исключением США. При этом, политика крупных цифровых платформ, ограничивающих доступ к российским СМИ, в данном документе и в позиции США не принимается во внимание, несмотря на то, что важный акцент сделан на защиту прав человека в цифровой среде и свободу доступа к информации. Еще одной особенностью подхода является его экстратерриториальный характер, то есть ориентация на распространение принципов и ценностных ориентиров законодательства США на международный уровень, что ограничивает цифровой суверенитет государств, присоединившихся к данному документу. Нельзя не принять во внимание и незначительное число сторонников данного документа США, их менее трети всех государств — членов ООН. Следует отметить, что это лишь одна из последних, но не единственная инициатива, ориентированная на распространение западных ценностей на глобальное цифровое пространство — в их числе Парижский призыв к доверию и безопасности в киберпространстве от 2018 года, Программа действий по продвижению ответственного поведения государств в киберпро-

4 Дробинин А. Уроки истории и образ будущего: размышления о внешней политике России // Международная жизнь. 2022. URL: <https://interaffairs.ru/news/show/36410>

странстве ЕС от 2020 года, Инициатива по борьбе с вымогателями США от 2021 года.

В этом контексте выгодно отличаются продвигаемые Россией инициативы: в области выработки правил ответственного поведения государств в глобальном информационном пространстве, выработки Конвенции по противодействию использованию ИКТ в преступных целях, интернационализация управления Интернетом и передача функций по управлению Интернетом к Международному союзу электросвязи — все они ориентированы на уважение государственного суверенитета в информационном пространстве.

В условиях формирования многополярного мира США не могут навязывать свою волю мировому сообществу. В глобальной

информационной сфере формируются новые влиятельные центры силы, не готовые следовать в фарватере проводимой Вашингтоном политики, в их числе Китай, Индия, ЮАР, страны Ближнего Востока, Африки. Это значительная часть международного сообщества, которая отвергает колониальные практики, как в реальном, так и в виртуальном пространстве. В этих условиях особенно востребованным становится формирование международного режима информационной безопасности, основанного на уважении государственного суверенитета. Такой режим получит поддержку большинства международного сообщества и сможет отразить актуальные реалии современного многополярного мира.

## Г.Г. Шинкарецкая

д.ю.н., главный научный сотрудник  
Института государства и права РАН

### СУВЕРЕНИТЕТ ГОСУДАРСТВА В КИБЕРПРОСТРАНСТВЕ

Управление Интернетом — это сложная взаимосвязь субъектов, наделенных различными уровнями власти и общим желанием контролировать Интернет. Тем не менее, утверждается, что правительства имеют соответствующие возможности для руководства глобальным управлением Интернетом. Является ли «киберпространство» отдельной правовой областью, для которой необходимы новые правила (если таковые имеются), а старые правила бесполезны, неуместны или обречены на провал?

Первые годы существования Интернета озаменовались, по крайней мере, со стороны некоторых сторонников, смелым видением киберпространства как беззаконной анархической территории, свободной от правового регулирования.

Однако все более обыденная и рутинная практика законодательства и регулирования в киберпространстве заставляет задаться вопросом, есть ли вообще что-то юридически новое в Интернете. На самом деле Интернет более или менее подтвердил общие принципы международного права, хотя существуют, конечно, некоторые практические трудности в их применении в онлайн-среде.

Иногда говорят, что Интернет устранил государственные границы, и киберпространство — это свободный ареал взаимодействия пользователей. Однако на нашей планете есть много пространств, где не действует национальное разделение: открытое море, космос, Антарктика. В этих пространствах действуют физические и юридические лица разных государств на одинаковой основе, что определяется именно равенством субъектов международного права, с юридической точки зрения — равенством их суверенитетов.

Та же картина наблюдается в киберпространстве — мы наглядно видим деятельность физических и юридических лиц, государства как будто остаются на заднем плане, и на передний план выходят отношения, регулируе-



мые международным частным правом, иной раз весьма конфликтные, как, например, можете ли вы порочить кого-либо или нарушать законы о цензуре в третьей стране при публикации в Интернете, и в каких юрисдикциях вы заключаете контракт, а следовательно, чье право будет применяться в процессе разрешения потенциального спора.

Изучение «управления Интернетом» на международном уровне оказывается ценным для понимания природы международного управления в целом, характера международных регулирующих институтов, международных правовых структур и доктрин, поскольку они подвергаются все большему концептуальному, политическому и технологическому давлению в процессе роста Интернета.

Безусловно, Интернет порождает некоторые особые проблемы регулирования, тесно связанные с его техническим характером и практической эксплуатацией. Самая насущная из них — кто должен управлять самой архитектурой Интернета, в частности, системой доменных имен, особенно в том, что касается доменов верхнего уровня и распределения адресов Интернет-протокола.

Покровитель глобального понимания Интернета, правительство США, сделало акцент на необходимости практического подхода, ориентированного на частный сектор, и с опаской относится к любому движению в направлении создания межправительственной



структуры управления, продолжая активно продвигать модель управления через частный сектор. Другие правительства по-прежнему заинтересованы в том, чтобы играть более активную роль в управлении Интернетом испытанными международно-правовыми методами, что предоставило бы национальным правительствам прямое право голоса по таким вопросам, как создание новых доменов верхнего уровня и управление ими, а также более прямое участие в разработке политики глобального управления Интернетом. Активные дебаты по вопросам управления Интернетом идут в рамках постоянных органов Организации Объединенных Наций, а также и в ходе таких всемирных форумов, как Саммит по информационному обществу.

Технические аспекты управления Интернетом вызывают определенные опасения по поводу экономических, политических и культурных последствий. В процессе дебатов выясняется противопоставление взглядов технических экспертов взглядам дипломатов, представителей интересов общества, частным интересам. В процессе обсуждения выявляется не только то, как нормы разрабатываются и применяются в политически важной и спорной области, но также и необходимость приведения различных подходов к реализации различных политических целей и общих правовых норм.

Одним из новых аспектов применения международного права к управлению Интернетом является все более определенная тенденция рассматривать Интернет как средство достижения более широких целей государственной политики, включая цели многосторонних договоров и фундаментальные принципы международного права, такие как права человека.

Первые существенные договоренности относительно управления Интернетом были достигнуты на всемирных саммитах. Женевская декларация принципов была принята на первом этапе в качестве авторитетного политического документа, выражающего общее политическое видение Интернета, но учтем, что это и не правовой, и не обязывающий документ. В Декларации прямо сказано о фундаментальном значении международного права, в частности, Декларация призывает к международному сотрудничеству в области информации и коммуникационных технологий, кото-

рые прочно вошли в контекст государственной политики и осуществления прав человека. В Декларации в качестве первоочередных задач названы такие проблемы, решение которых в регулировании Интернета необходимо для обеспечения суверенитета государств, как борьба с терроризмом, пресечение детской порнографии и решение других очевидных социальных проблем.

Существует опасность вмешательства государства в целях ограничения такого использования Интернета, которое считается наносящим ущерб общественному порядку и благосостоянию в областях, где законность таких ограничений может быть оспорена, например, в регулировании политического дискурса. Мы видим, что для оспаривания вмешательства используются международно-правовые аргументы, и в действие вступает такой общепризнанный принцип международного права, как запрет вмешательства во внутренние дела государства. Этот принцип приобретает реальное звучание, учитывая, что распорядители доменов применяют свои правила на территориях других государств.

Изменения объективных обстоятельств, в частности, продвижение технологий, в свою очередь, могут спровоцировать пересмотр того, что мы воспринимаем как справедливое, беспристрастное и равноправное. Например, до того, как появилась технология аудиозаписи, вокальные исполнители не нуждались в нематериальном праве на свои выступления; технический прогресс означает, что исполнение теперь может быть легко присвоено и коммерциализировано третьими сторонами, что вызвало изменение фактического фона, который привел к формулированию отдельного права исполнителя сначала в национальных законах, а в конечном счете и в общем международном праве.

Современные ИКТ и особенно Интернет породили движение от технического прогресса к новым ценностям справедливости и права. Несмотря на его недавнее появление для большей части человечества, несомненно огромная важность Интернета как инструмента для реализации прав человека, поскольку дает людям доступ к участию в демократических процессах, инструменты для выражения своих убеждений, возможности получения адекватного образования, пользования бла-

гами научного прогресса и даже обеспечения достижения надлежащего уровня здоровья. Таким образом сам доступ к Интернету превращается в отдельное «право» — право на доступ к Интернету. Эта богатая палитра соображений в области прав человека и государственной политики возвращает нас к проблемам управления Интернетом.

В документах международных форумов управление Интернетом определяется как разработка и применение правительствами, частным сектором и гражданским обществом в пределах их полномочий общих принципов, норм, правил, процедур принятия решений и программ, которые определяют развитие Интернета и правила его использования. Рассматривая управление Интернетом как полностью международный и многосторонний процесс, Женевская декларация и Тунисская повестка дня предусматривают, что международное управление Интернетом частично касается самой основы Интернета. Но есть также много практических вопросов, касающихся международного публичного и частного права, его практики и администрирования. Именно оказавшись перед такими практическими вопросами, ученые теряют из виду самый важный институт международного права — суверенитет государства. Назовем некоторые из них:

- сложность определения географического положения действий, совершенных в Интернете, например, заключения контракта, акта клеветы или акта нарушения авторских прав и вытекающей отсюда сложности определения применимого национального законодательства;
- сложность определения национальной юрисдикции, распространяющейся на те или иные действия, в частности, определение методов применения существующих принципов на действия в онлайн-среде, и возможной адаптации их к решению практических проблем, связанных с транзакциями и возможным нарушением прав интеллектуальной собственности в Интернете;
- возможность избежать действия закона об авторском праве, просто переместив свой сервер или свою компанию в физическое место в такое государство, ко-

торое не является участником международных договоров об авторском праве;

- потенциальные обязательства государств по обеспечению авторских и других прав интеллектуальной собственности в цифровом домене и по содействию их соблюдению в других юрисдикциях, например, путем выдачи в случаях нарушения прав интеллектуальной собственности;
- толкование других связанных с транзакциями обязательств;
- простота создания личных идентификационных данных, которые оказываются вне правовых категорий, определенных в национальном законодательстве;
- возможность и законность прибегания к полной анонимности в Интернете; правомерность создания полностью вымышленной личности; вероятность привлечения отдельных лиц к ответственности за преступные действия, совершенные под прикрытием интернет-персоны;

Таким образом, Интернет высвечивает и обостряет проблемы, которые всегда присутствовали в международном управлении и вышли на первый план с появлением Интернета. Так, при осуществлении транзакций в Интернете бывает трудно различить границы между публичным и частным международным правом. Это, пожалуй, одна из самых трудных задач, возникающих в связи с управлением Интернетом. Уже есть немало споров, рассмотренных национальными судами, особенно по авторским правам.

Высказывается немало предложений об интернационализации ICANN — американской корпорации, базирующейся в Калифорнии и занимающейся распространением доменных имен. Однако текущая деятельность ICANN и без того является международной, проблема состоит в постановке самой ICANN под международное управление, что прямо диктуется принципом суверенного равенства государств.

Многие преимущества Интернета для более открытой глобальной дипломатии, для улучшения образовательных и культурных возможностей и для продвижения прав человека в целом являются результатом не международных институтов и сознательного

коллективного нормативного импульса, а неуклонного накопления практических инициатив и результатов деятельности на низовом уровне, отчасти и за счет деятельности частного сектора, такой как внедрение возможностей подключения, стимулируемых либерализацией телекоммуникационного сектора во многих странах.

Несмотря на общую тенденцию рассматривать Интернет как технологию, которую

необходимо контролировать, его также можно рассматривать как инструмент, укрепляющий национальное и глобальное управление. Интернет не угрожает государственному суверенитету. Однако перед государствами встает реальная задача совершенствования управления Интернетом, которое требует реструктуризации на фоне необходимости пересмотра отношения государств к информационно-коммуникационным технологиям.

## П.У. Кузнецов

*д.ю.н., профессор, заведующий  
кафедрой информационного права  
Уральского государственного  
юридического университета*

### **ОТДЕЛЬНЫЕ МЕТОДОЛОГИЧЕСКИЕ АСПЕКТЫ ПРАВОВОГО ОБЕСПЕЧЕНИЯ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В КОНТЕКСТЕ ЖИЗНЕОБЕСПЕЧЕНИЯ ЧЕЛОВЕКА**

О противоречии пространств научно-технического прогресса и права

Прежде всего, необходимо отметить, что обозначенные два пространства — это разные величины по своей природе. Наука и техника не имеет строгих границ проникновения в человеческую деятельность, а траектории развития природы научно-технического прогресса (НТП) и природы человека находятся в крайнем противоречии всегда. Это закономерность их коэволюции, т.е. совместного сосуществования.

Как известно, право имеет достаточно строгие и порой жесткие формализованные очертания, зависящие от государственной политики и потребностей человека. Правовая сфера в силу своей природы, обладая инерционной сущностью, принимает в свои границы далеко не все объекты человеческой деятельности, а только те, которые имеют традиционные для человека формы восприятия и востребованы обществом. Это константа, т.е. постоянная величина пространства права. При определении возможностей права это надо учитывать.

И еще, фундаментальные науки НТП и юриспруденция имеют разные по своей природе языковые и логические формы мышления. В отдельной части они имеют совместные точки соприкосновения, но во многом они несовместимы по содержанию. Это сказывается на противоречиях формирования понятийного аппарата воздействия регулирующих инструментов на общественные отношения в информационной сфере.

Как совместить жесткие императивы закономерностей развития научно-технического прогресса и жизненного пространства права? Думается с помощью мягких форм совмещения инструментальных средств и нелинейных



(возможно, синергетических) подходов в правовом регулировании, с помощью которых можно добиться успехов даже в самых, казалось бы, безнадежных ситуациях в период общественных бифуркаций, которые существуют в современном мире.

Здесь особенно нужны нестандартные подходы к использованию международных договоров, предусматривающих совмещение обязательных для исполнения и норм, заключаемых на уровне двусторонних и многосторонних договоров, имеющих необязательную силу, в том числе имеющих характер присоединения или, напротив, неприсоединения.

Иначе говоря, общество имеет возможность поставить НТП в регулируемые мягкие границы на практическом уровне, это допустимо хотя бы в рациональном смысле. Причем, речь идет не о самом развитии научных теорий и концептов, а об их применении на практике.

Как известно, НТП породил информационно-коммуникационные технологии (ИКТ), которые в настоящее время определяют ключи многопрофильного развития цивилизации, включая профиль международной информационной безопасности (МИБ). Прорывные технологии наиболее активно влияют на жизнь человека и практически меняют её ареал и траекторию развития. В этой аудитории не имеет смысла объяснять этот тезис. Это неоднократно подчеркивалось на предыдущих фо-

румах и конференциях по рассматриваемой тематике.

Цифровые формы современной жизни — интернет вещей, облачные технологии и, особенно искусственный интеллект, конечно, создают комфортные условия для общества. Однако они еще более ускорили негативные проявления НТП в их человеческом измерении.

Все это повлияло и на правовую сферу, включая юриспруденцию — юридическую науку. Правда, представители её по-разному реагируют на эти вызовы. Причем, такие различия носят самые крайние формы: от полного непонимания и неприятия до неосознанных «революционных» рефлексий и призывов перестроить (оцифровать) всю правовую систему.

Достаточно упомянуть нынешнее увлечение юристами темой проблем цифровой экономики. Удивительно, но как по свистку спортивного арбитра многие юристы «побежали» осваивать цифровую тему общественных процессов, не совсем осознавая её сущности.

Это обстоятельство парадокса научного правосознания тоже надо учитывать экспертам в области МИБ.

В этой связи нередко остро ставится вопрос о том, что лучше и эффективнее: правовое или технологическое регулирование правоотношений по поводу ИКТ? Не могу ответить на этот вопрос однозначно. Во всяком случае, на протяжении уже более 20 лет мы не можем на него ответить однозначно. Вероятно, выход находится на разумном сочетании этих форм регулирования. Право и Закон (как форма права) должны только допускать технологические средства в качестве регулятора в той или иной правовой форме.

### **Суверенитет как неустойчивая категория в информационной сфере**

Известно, что государственный суверенитет имеет достаточно жесткую привязку к исторически сложившимся реалиям жизни и возможностям самого суверена, т.е. властвующего субъекта. Возможностям, прежде всего, политического, экономического, информационного и даже исторического характера.

Как представляется, в информационной сфере суверенитет является неустойчивой

категорией в силу её неопределенности по географическим параметрам, а потому и невозможности установить жесткие границы самостоятельного влияния государства на обеспечение властных полномочий. Экономически сильные страны более активны в этом отношении, но и они далеко не всегда обеспечивают своё телекоммуникационное пространство в пределах своего влияния.

В рамках конференций НАМИБ нам уже неоднократно приходилось высказываться о том, что возможно использовать сочетанные формы укрепления телекоммуникационного (цифрового) суверенитета.

На дискуссионном уровне вполне допустимо обсуждать разные формы существования суверенного качества государства — например, *расширенного или делегированного суверенитета*, когда отдельные государства расширяют границы своего телекоммуникационного пространства или делегируют другим государствам свои полномочия по его обеспечению.

Однако, расширение границ совместного использования такого пространства и обеспечения его безопасности возможно путем межгосударственных договоренностей. В практике ШОС и БРИКС такие формы межгосударственных отношений вполне допустимы. Государства, входящие в состав этих международных организаций в той или иной форме участия, могут самостоятельно определять, где находятся границы распространения их влияния на телекоммуникационную среду и установления режима распространения информации.

### **Проблемы мировоззренческой безопасности**

Тема защищенности интересов личности, общества и государства в сфере мировоззрения давно стала актуальной. Во всяком случае, о мировоззренческой безопасности поднималась дискуссия еще более 20 лет назад на российско-белорусских конференциях по правовому обеспечению информационной безопасности, которые проводились в Санкт-Петербурге.

Тогда, в период надрыва общественных катаклизмов и преобразований эта тема звучала как нонсенс и скорее экзотика.

Сегодня она стала актуальной в связи с фронтальным характером современных гибридных войн.



Мировоззрение как необходимая составляющая человеческого сознания и его развития всегда обусловлено историческими переменами. Оно активно отражает, преломляет большие и малые, явные и скрытые процессы общественных изменений. В реальной жизни мировоззрение формирует индивидуальные и групповые интересы и множества вариантов их реализации.

Мировоззрение является интегральным и многоуровневым научным концептом, концентрацией обобщенных научных, профессиональных и событийных знаний. Кроме знаний о развитии мировой цивилизации на мировоззренческом уровне осмысливается весь уклад человеческой жизни, и самое главное, — выражаются системы ценностей и их значении — представления о добре и зле, о внутренних глубинных духовных смыслах человека, выстраиваются образы преемственности поколений и проекты будущего их развития, получают одобрение (или осуждение) те или иные способы жизни и т.д.

Ценности как идеальные духовные блага воплощают особое отношение людей ко всему происходящему в соответствии с их целями, потребностями и смыслами жизни. В ценностном измерении жизни формируются

материальные и нематериальные, нравственные, эстетические идеалы.

И последнее. Мировоззрение человека всегда начинается с кровью и молоком матери, с её мировосприятия и предпочтений в жизни. Но сегодня оно, к сожалению, формируется со смартфона в руках младенца и с его системы координат о том, что хорошо и что плохо.

Помните стихотворение В.В.Маяковского о «крохе, который пришел к отцу и спросила кроха, что такое хорошо и что такое плохо». Вот эта «кроха», к сожалению, сегодня уже не задает такой мировоззренческий вопрос. Она уже не нуждается в ответе на него, все ответы эта «кроха» получает в сети Интернет и в чем-то даже поучает своих родителей и формирует «семейное» мировоззрение.

Концепт «мировоззренческая безопасность» заслуживает своего возрождения на уровне научного осмысления и постановки научной задачи в т.ч. в рамках МИБ. Не будем забывать, что многие проблемы МИБ начинаются с проблем мировоззрения на уровне национальном. Особенно это стало очевидным сейчас во время проведения специальной операции, которая обнажила многие «спящие» мировоззренческие проблемы.

## **А.В. Морозов**

*д.ю.н., профессор, академик РАЕН,  
профессор кафедры компьютерного  
права и информационной безопасности  
МГУ им. М.В. Ломоносова*

### **ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ ПОДГОТОВКИ КАДРОВ ВЫСШЕЙ КВАЛИФИКАЦИИ В ОБЛАСТИ ПРАВОВОГО ОБЕСПЕЧЕНИЯ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

Указом Президента РФ от 12.04.2021 г. № 213 утверждены Основы государственной политики Российской Федерации в области международной информационной безопасности. Этот документ стратегического планирования требует повысить эффективность подготовки юридических кадров высшей квалификации, что заставляет работников сферы науки и высшего образования находить новые возможности в этой важнейшей сфере деятельности.

Как уже указывалось в материалах автора на проводимых ранее Национальной Ассоциацией международной информационной безопасности (НАМИБ) Международных Форумах «Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности» автор является руководителем магистерской программы, реализуемой кафедрой компьютерного права и информационной безопасности МГУ им. М.В. Ломоносова.

Реализация Указа Президента Российской Федерации от 01.05.2022 № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» требует комплексного подхода к подготовке кадров для обеспечения информационной безопасности критически важных организаций РФ на основе междисциплинарных знаний.

Одной из важнейших дисциплин, входящих в обязательный раздел учебного плана подготовки магистров, является дисциплина «Международная информационная безопасность». Структурно в указанную дисциплину входит 4 модуля (темы):

Тема 1. Международная информационная безопасность: подходы определению понятия.



Вызовы и угрозы безопасности в информационную эпоху. Информационно-технические и социо-гуманитарные аспекты международной информационной безопасности. Международная информационная безопасность: сравнительный анализ исследовательских дискурсов. Российский подход к определению национальной и международной информационной безопасности. Подход, зафиксированный в официальных документах ООН и других международных организаций.

Тема 2. Развитие ИКТ-среды как ключевой инфраструктуры информационного общества.

Основные характеристики ИКТ-среды. Международное управление Интернетом: роль США. Позиция России по вопросам международного управления Интернетом. Современные тенденции развития глобального информационного общества.

Тема 3. Объекты международной информационной безопасности критических информационных инфраструктур.

Новые объекты безопасности в информационную эпоху. Понятие «критическая информационная инфраструктура». Подходы к определению критических информационных инфраструктур в различных странах. Специфика информационных инфраструктур с точки зрения обеспечения их безопасности. Вызовы и угрозы национальной и международной безопасности, связанные с воздействием на

критические информационные инфраструктуры. Принципы классификации и источники угроз МИБ. Триада угроз международной информационной безопасности. Субъекты информационного воздействия.

Тема 4. Проблемы применимости международного права к информационной сфере.

Применение общих принципов международного права к борьбе в информационной сфере. Международное право вооруженных конфликтов и его применимость к действиям в информационной сфере. Международное гуманитарное право и его применимость к конфликтам с применением информационных средств. «Таллиннское руководство о применимости международного права к ведению кибер-войн» и подход Запада. Позиция России по вопросу применения права международных конфликтов к информационной сфере. Применимость международного договорного права в области разоружения к вопросу ограничения информационного оружия. Основные направления адаптации международного права к информационной сфере.

Безусловно, после изучения всего набора дисциплин учебного плана, учащиеся в магистратуре готовят и защищают перед государственной аттестационной комиссией выпускную квалификационную работу (ВКР) на заранее согласованную и утвержденную тему.

Я хотел бы привести в качестве примера две выпускные квалификационные работы, успешно защищенные под руководством доктора юридических наук, чл.-корр. РАН Батурина Юрия Михайловича. Это работа 2021 года Ушаковой Анастасии Николаевны «Формулирование аутентичных правовых норм в области международной информационной безопасности и их толкование» и работа 2022 года Бобровой Екатерины Олеговны «Отправные пункты правовой аргументации в сравнительном анализе российского и американского подходов к международной информационной безопасности».

Структура первой ВКР 2021 года выглядит следующим образом:

Глава 1. Проблемы формулирования правовых норм в области международной информационной безопасности.

1.1. Терминологические проблемы в переговорах по международной информационной безопасности.

1.2. Юридическая аутентичность и семантическая адекватность правовых норм в области международной информационной безопасности.

1.3. Рассогласованность профессионального восприятия и деформации юридического текста.

Глава 2. Особенности юридического толкования правовых норм по международной информационной безопасности.

2.1. Применение общих правил юридического толкования международных договоров к формулировкам правовых норм по информационной безопасности.

2.2. Научно-технический контекст юридического толкования правовых соглашений по международной информационной безопасности.

2.3. Семантико-правовой подход к юридическому толкованию многоязычных договоров.

Глава 3. Процедура согласования юридических формулировок по международной информационной безопасности.

3.1. Семантико-правовой подход к разработке «области переговорного согласия» и «области юридических компромиссов».

3.2. Рекомендации для участников переговоров по нахождению «области юридических компромиссов» толкованием правовых норм в сфере международной информационной безопасности.

Очень интересным у данной ВКР выглядит перечень приложений:

Приложение №1. Сопоставительная таблица свойств мышления участников переговоров.

Приложение № 2. Характеристики мышления участников переговоров по международной информационной безопасности (краткий обзор).

Приложение № 3. Словарь примеров трудностей перевода терминологии информационных технологий.

Приложение № 4. Контекстный словарь.

Структура второй ВКР 2022 года следующая:

Глава 1. Анализ коллизий в переговорах по МИБ.

1.1. Подход РФ к международной информационной безопасности.

1.2. Подход США к международной информационной безопасности.

1.3. Противоречия правовых подходов РФ и США к международной информационной безопасности

Глава 2. Поиск отправных пунктов юридической аргументации в переговорах по международной информационной безопасности между РФ и США.

2.1. Понятие «общего места» в юридической топики и толкование правовых формулировок в сфере международной информационной безопасности.

2.2. Несовместимость аргументов в переговорах по международной информационной безопасности.

2.3. Логика поиска правовых «общих мест» международной информационной безопасности для РФ и США.

Глава 3. Предложения по юридической аргументации в сфере международной информационной безопасности.

3.1. Двустороннее согласование юридической аргументации в сфере международной информационной безопасности.

3.2. Переход к трехстороннему соглашению в сфере международной информационной безопасности.

3.3. Конвенция ООН по международной информационной безопасности.

3.4. Совершенствование доктрины информационной безопасности РФ в части международной безопасности.

В качестве проблемы для подготовки кадров высшей квалификации (докторов и кан-

дидатов наук) по направлению международной информационной безопасности у юристов, я хотел бы обратить внимание на изменение номенклатуры научных специальностей в 2022 году, в результате которой специалисты высшей квалификации, ранее защищавшие свои работы в диссертационных советах по «Информационному праву» 12.00.13, теперь должны будут искать свое место в специальности 5.1.5. «Международно-правовые науки». Это вызовет определенные трудности, поскольку специалистов по международному информационному праву в диссертационных советах по специальности 5.1.5 попросту во все нет.

Подводя итог этого важнейшего направления подготовки кадров высшей квалификации, следует сказать также о необходимости взаимодействия в сфере международной информационной безопасности специалистов как минимум трех направлений деятельности — дипломатов, айтишников и юристов. Для продвижения инициатив Российской Федерации в виде проекта Конвенции ООН о противодействии использованию ИКТ в преступных целях необходимо взаимодействие указанных выше направлений деятельности. И, прежде всего, должны быть подготовлены юристы, способные разработать грамотный юридически обоснованный профессиональный текст международного документа и добиться успешного принятия его на высшем международном уровне.

## А.С. Марков

д.т.н., президент АО «НПО »Эшелон»,  
профессор МГТУ им. Н.Э. Баумана,  
профессор Финансового университета  
при Правительстве РФ

### ПРОБЛЕМНЫЕ ВОПРОСЫ ПОВЫШЕНИЯ ДОСТОВЕРНОСТИ ИДЕНТИФИКАЦИИ РЕСУРСОВ КРИТИЧЕСКИ ВАЖНОЙ ИНФРАСТРУКТУРЫ

Актуальность и востребованность тематики повышения достоверности идентификации ресурсов критически важной инфраструктуры (КВИ) обусловлены разрешением проблемных вопросов добровольных и обязательных норм, правил и принципов ответственного поведения государств, призванных способствовать обеспечению открытой, безопасной, стабильной, доступной и мирной ИКТ-среды (Далее — Норм ответственного поведения государств) [1, 2]. Напомним, что Нормы ответственного поведения государств были представлены в рамках доклада Группы правительственных экспертов по поощрению ответственного поведения государств в ИКТ-среде в контексте международной безопасности (A/76/135).

При проработке возможности имплементации Норм ответственного поведения государств был отмечен ряд сложностей, касающихся пунктов (нормы 13 f, g, h, i, j, k), затрагивающих технические аспекты их реализации [3-5].

Напомним эти пункты Норм ответственного поведения государств:

- f) государства не должны заведомо осуществлять и поддерживать деятельность в сфере ИКТ, если такая деятельность противоречит их обязательствам по международному праву, наносит преднамеренный ущерб критически важной инфраструктуре или иным образом препятствует использованию и функционированию критически важной инфраструктуры для обслуживания населения;
- g) государства должны принимать надлежащие меры для защиты своей критически важной инфраструктуры от угроз в сфере ИКТ, принимая во внимание резолюцию 58/199 Генеральной Ассамблеи;



- h) государства должны удовлетворять соответствующие просьбы об оказании помощи, поступающие от других государств, критически важная инфраструктура которых становится объектом злонамеренных действий в сфере ИКТ. Государства также должны удовлетворять соответствующие просьбы о смягчении последствий злонамеренных действий в сфере ИКТ, направленных против критически важной инфраструктуры других государств, если такие действия проистекают с их территории, принимая во внимание должным образом концепцию суверенитета;
- i) государства должны принимать разумные меры для обеспечения целостности каналов поставки, чтобы конечные пользователи могли быть уверены в безопасности продуктов ИКТ. Государства должны стремиться предупреждать распространение злонамеренных программных и технических средств в сфере ИКТ и использование скрытых вредоносных функций;
- j) государства должны способствовать ответственному представлению информации и факторах уязвимости в сфере ИКТ и делиться соответствующей информацией о существующих методах борьбы с такими факторами уязвимости, чтобы ограничить, а по возможно-



сти и устранить возможные угрозы для ИКТ и зависящей от ИКТ инфраструктуры;

- к) государства не должны заведомо осуществлять и поддерживать деятельность, призванную нанести ущерб информационным системам уполномоченных групп экстренного реагирования (также именуемым группами реагирования на компьютерные инциденты или группами реагирования на инциденты информационной безопасности) другого государства. Государство не должно использовать уполномоченные группы экстренного реагирования для осуществления злонамеренной международной деятельности.

В работе было предложено конкретизировать цель, задачи и направления именно технической реализации Норм ответственного поведения государств [4]. В связи с этим было подчеркнуто, что целью исследования остается повышение уровня международной информационной безопасности путем имплементации названных Норм ответственного поведения государств. Это позволило сформулировать основные задачи, как-то:

- исследование особенностей реализации околотехнических пунктов Норм ответственного поведения государств в ИКТ-среде;
- определение направлений развития международного технического регулирования в области применения Норм ответственного поведения государств в ИКТ-среде.

Легко заметить, что с технической точки зрения Нормы ответственного поведения го-

сударств можно объединить в три обобщенные направления:

1. Безопасность сферы КВИ (обеспечение внешней и внутренней безопасности и восстановление нормальной работы), касающейся в общем плане следующих пунктов:

- f) государства не должны осуществлять деятельность, приводящую к ущербу КВИ (в первую очередь социально-значимой КВИ) иных государств;
- g) государства должны принимать надлежащие меры для защиты своей КВИ;
- h) государства должны удовлетворять просьбы об оказании помощи, поступающие от других государств, КВИ которых становится объектом злонамеренных действий, и смягчать последствия злонамеренных действий, проистекающих с их территории.

2. Безопасность разработки и цепей поставок (обеспечение безопасности продукции и средств защиты информации):

- i) государства должны принимать разумные меры для обеспечения целостности каналов поставки, предупреждать распространение злонамеренных программных и технических средств;
- j) государства должны способствовать ответственному представлению информации и факторах уязвимости, а также информации о существующих методах борьбы с такими факторами уязвимости.

3. Безопасность ситуационных центров:

- к) государства не должны осуществлять деятельность против других CERT/CSIRT и использовать их для злонамеренной деятельности.

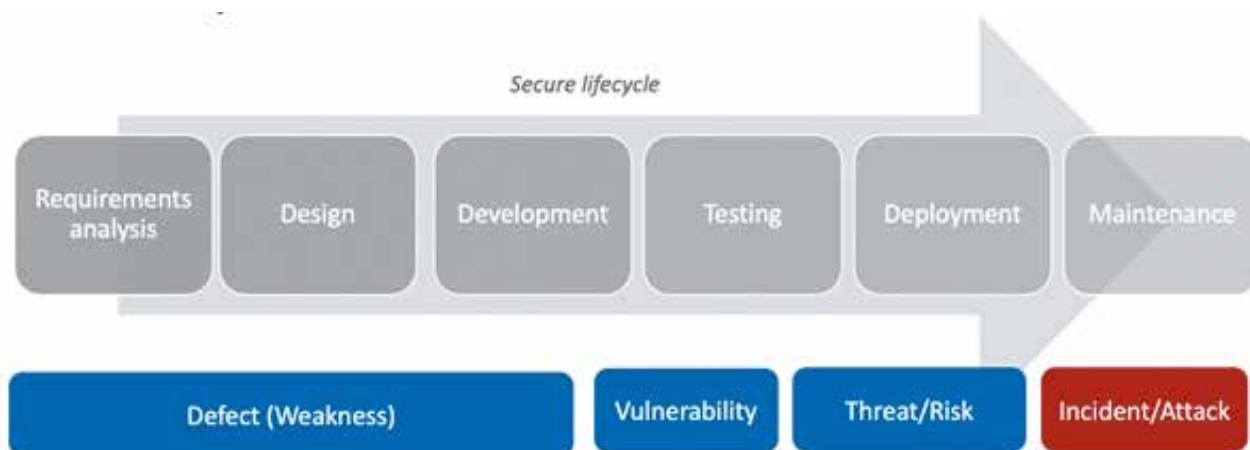


Рис. 1. Основные факторы информационной безопасности

Таблица 1.

## Меры международной информационной безопасности

| Классы контрмер        | Контрмеры                                                                                                                               |
|------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|
| Превентивные меры      | Повышение оперативности обмена информации об уязвимостях в продуктах<br>Повышение уровня доверия к средствам защиты информации          |
| Детективные меры       | Повышение оперативности обмена информации об инцидентах<br>Повышение доверия и результативности расследований компьютерных преступлений |
| Восстановительные меры | Повышение уровня взаимопомощи в чрезвычайных и кризисных ситуациях                                                                      |
| Сдерживающие меры      | Противодействие уровню анонимности правонарушителя                                                                                      |

При решении вопросов международной информационной безопасности следует определиться с базовыми факторами. В политической сфере зачастую основной упор делается на конфликты — инциденты в области информационной безопасности. В то же время авторы считают, что следует решать проблему в комплексе, то есть учитывать все факторы информационной безопасности, как-то: угрозы, уязвимости и дефекты безопасности (рис. 1). К примеру, исключив дефекты составляющих объекты КВИ в рамках международной сертификации, мы исключим

соответствующие уязвимости в средствах защиты и соответствующие угрозы ресурсам КВИ, а значит, исключаем и сам инцидент международной информационной безопасности.

Учитывая основную цель исследования как повышение уровня международной информационной безопасности и определив факторы безопасности: дефекты (ошибки безопасности), уязвимости, угрозы/риски, атаки/инциденты, мы можем названные выше три направления распределить по основным классам контрмер (табл. 1)

Таблица 2.

## Стандарты информационной безопасности

| Нормы                                                                                                    | Возможные соглашения                                                                                                                      | Пункты Норм | Стандарты                                                         |
|----------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------|-------------|-------------------------------------------------------------------|
| Повышение оперативности обмена информации об уязвимостях в продуктах                                     | По открытым базам уязвимостей и эксплойтов                                                                                                | f,g,j       | MITRE (в РФ имеется БДУ ФСТЭК России)                             |
| Повышение оперативности обмена информации об инцидентах                                                  | Об интеграции CERT                                                                                                                        | f,g,k       | ISO/IEC 18044                                                     |
| Повышение доверия и результативности расследований компьютерных преступлений, в том числе атрибуции атак | Об интеграции экспертов по компьютерным преступлениям                                                                                     | f,g         | ISO/IEC 21043                                                     |
| Повышение уровня взаимопомощи в чрезвычайных и кризисных ситуациях                                       | Об облачных инфраструктурах, о трансграничных атаках                                                                                      | f,h         | ISO/IEC 27031, 22301, NIST SP 800-34<br>ISO/IEC 27032             |
| Повышение уровня доверия к средствам защиты информации                                                   | Об оценке соответствия при предоставлении исходного кода, о соблюдение правил разработки безопасных программ и целостности цепей поставки | f,g,i       | ISO/IEC 15408,<br>ISO/IEC 27034<br>ISO/IEC 27036<br>ISO/IEC 28000 |
| Противодействие уровню анонимности правонарушителя                                                       | С провайдером услуг в КВИ, соглашение к разработчику КВИ                                                                                  | f,g         | н/д                                                               |

**Таблица 3.**  
**Способы идентификации пользователя**

| Характеристика                               | Уровень определения | Комментарии                                                                                                  |
|----------------------------------------------|---------------------|--------------------------------------------------------------------------------------------------------------|
| MAC-адрес                                    | неприемлемый        | В пакете меняется на каждом узле<br>Можно получить, запустив код у клиента                                   |
| IP-адрес                                     | средний             | Проблема анонимизаторов и пр.<br>Ведение белых списков для авторизации                                       |
| Особый протокол                              | неприемлемый        | У клиента отсутствуют или подменяются промежуточным протоколом                                               |
| User Agent и подобные                        | высокий             | Возможна подмена или скрытия, использование анонимных браузеров (TOR)                                        |
| Переменные сессии                            | высокий             | Совокупность генерируемых глобальных переменных клиента и сервера (включая идентификационные характеристики) |
| Cookies и варианты                           | высокий             | Можно использовать уникальный идентификатор<br>Могут быть запрещены, очищены                                 |
| Browser fingerprint (в том числе user agent) | высокий             | Дополнительные нагрузки (хранение, вычисление)<br>Могут быть запрещены, очищены                              |

Опираясь на табл. 1, мы можем предложить возможные частные международные соглашения, оценить надлежащие меры относительно имеющихся международных стандартов в области информационной безопасности, а также оценить степень недостающих международных стандартов (табл. 2).

Из табл. 2 мы видим пробелы в области международной стандартизации — отсутствие стандартов, способствующих снижению анонимизации, а также базового стандарта, определяющего основные положения международного технического (нормативно-правового) регулирования в области международной информационной безопасности.

Следует напомнить, что уже имеются прецеденты технического регулирования в области международной информационной безопасности в следующих двух формах технического регулирования [6]:

1. Обязательная международная сертификация СЗИ (на соответствие ISO/IEC 15408);
2. Добровольная международная сертификация СМИБ (ISO/IEC 27001).

Таким образом легко видеть два краеугольных вопроса международной информационной безопасности:

1. Обеспечение суверенитета ИКТ, делимитация границы ИКТ, демаркация границы ИКТ;
2. Решение проблемы анонимности субъектов КВИ (в сфере ИКТ).

Первый вопрос в настоящее время широко обсуждается и его решению посвящен ряд фундаментальных трудов [1, 7-9].

Второй вопрос может иметь комплексное (политическое, организационное и организационно-техническое и др.) решение. Например, он непосредственно касается атрибуции кибератак на ресурсы КВИ [6, 10, 11]. Чтобы избежать недопониманий в комплексировании норм и мер безопасности — в данном исследовании был проведен краткий анализ организационно-технических решений на уровне взаимодействия серверов и клиентов мета-сети интернет. В качестве примера в табл. 3 приведены способы борьбы с анонимизацией на уровне клиента.

Анализ таблицы 3 показывает, что эффективность идентификации зависит от комплекса применяемых технологий, 100% идентификации пользователей не дает ни один из способов, но имеет смысл предъявлять требования к серверам мета-сети интернет, а не к клиентам.

### Выводы

Проводимые исследования позволяют определить направления повышения идентификации ресурсов КВИ, например, путем следующего:

1. Политические соглашения по соответствию нормативным требованиям;

2. Организационные решения, к примеру ведение белых списков и мониторинг (по аналогии gosmonitor.ru), внедрение «хороших практик» (по аналогии с практиками Роскомнадзора), поддержка единой точки идентификации, организация блокировки, требования к приложениям клиентов (по анонимизации), усиление аутентификации (MFA) и др.

3. Гарантированные технические решения, например, развитие PKI-инфраструктуры.

Промежуточные итоги исследования можно сформулировать как следующие:

1. Анонимность в интернет продолжает расти несмотря на ограничительные меры отдельных государств;

2. Вопросы границ киберпространства пока не нашли исчерпывающего международного решения;

3. Имеется востребованность комплексной международной системы технического регулирования;

4. Надлежащие меры могут быть определены международными стандартами;

5. Решению проблемы анонимизации может способствовать разработка соответствующих стандартов;

6. Решению проблемы имплементации Норм ответственного поведения государств в ИКТ-среде может способствовать разработка общего стандарта регулирования (менеджмента) международной информационной безопасности [8];

7. Наиболее эффективными являются требования к серверам мета-сети, при безусловном комплексном решении сетевых проблем идентификации и аутентификации источника нарушений международной информационной безопасности.

Можно согласиться, что развитие национальных ИТ-технологий является архиважной составляющей национального суверенитета [12, 13].

## Литература

1. Международная информационная безопасность: теория и практика / Крутских А.В., Бирюков А.В., Бойко С.М., Волкова С.Г., Зиновьева Е.С., Зинченко А.В., Матюхин Д.В., Смирнов А.И. Учебник для вузов: в 3-х томах / Под общ. ред. А.В. Крутских. — М.: МГИМО, 2021. — Том 1 (2-е изд., доп.) — 384 с.
2. Шерстюк В.П. Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности. безопасность и устойчивость ИКТ-среды ради стабильности и процветания. // В сб: докладов участников Пятнадцатого международного форума. — М.: НАМИБ, 2021. С. 12–15.
3. Методологические вопросы применения норм, правил и принципов ответственного поведения государств, призванных способствовать обеспечению открытой, безопасной, стабильной, доступной и мирной ИКТ-среды / Под ред. А.Стрельцова и Э.Тикк. — Исследовательский проект международного исследовательского консорциума информационной безопасности — М.: НАМИБ, 2020 34 с.
4. Применение норм ответственного поведения государств в ИКТ-среде и международное сотрудничество / Стрельцов А.А. и др.; Предисловие В.Шерстюк — М.: НАМИБ, 2022. — 32 с.
5. Voluntary, non-binding norms for responsible state behaviour in the use of information and communications technology. / By ed. E.Tikk -NY.: UNODA, 2017. — 296 p.
6. Ромашкина Н.П., Марков А.С., Стефанович Д.В. Международная безопасность, стратегическая стабильность и информационные технологии. М.: ИМЭМО РАН, 2020. 98 с. DOI: 10.20542/978-5-9535-0581-9.
7. Крутских А.В., Стрельцов А.А. Международное право и проблема обеспечения международной информационной безопасности // Международная жизнь. 2014. № 11. С. 20–34.
8. Стрельцов А. А. Суверенитет и юрисдикция государства в среде информационно-коммуникационных технологий в контексте международной безопасности // Международная жизнь. — 2017. — №. 2. — С. 87–106.
9. Стрельцов А.А., Пилюгин П.Л. К вопросу о цифровом суверенитете // Информатизация и связь. 2016. № 2. С. 25-30.
10. Марков А.С. Актуальные вопросы атрибуции компьютерных атак. // В сб. до-

- кладов участников Пятнадцатого международного форума. — М.: НАМИБ, 2021. С. 69–76.
11. Смирнов А.И. Проблема атрибуции кибератаки в контексте международной информационной безопасности. В кн.: Международная информационная безопасность: Новая геополитическая реальность. / Алборова М.Б. и др. / Под ред. Е.С.Зиновьевой, М.Б.Алборовой. — М.: Аспект Пресс, 2021. С. 61–66.
12. Ромашкина Н.П. Глобальные военно-политические проблемы международной информационной безопасности: тенденции, угрозы, перспективы // Вопросы кибербезопасности. 2019. — № 1 (29). — С. 2–9.
13. Добродеев А.Ю. Кибербезопасность в Российской Федерации. Модный термин или приоритетное технологическое направление обеспечения национальной и международной безопасности XXI века // Вопросы кибербезопасности. 2021. № 4 (44). С. 61–72.



## А.К. Жарова

*д.ю.н., старший научный сотрудник  
сектора уголовного права, уголовного  
процесса и криминологии Института  
государства и права РАН*

### ПРАВОВОЕ ОБЕСПЕЧЕНИЕ АТРИБУЦИИ КИБЕРАТАК

Мир ИКТ-сферы создает взаимную зависимость государств от ошибок, уязвимостей, программных закладок, которые возможны в информационных технологиях. Уязвимости являются свойством информационных технологий, создать технологию, абсолютно устойчивую к внешним атакам невозможно в принципе. На межгосударственный и международный уровень вышли проблемы атрибуции кибератак, поскольку ее результатом может стать межгосударственный конфликт.

Основой ИКТ-сферы являются интернет-технологии, ее невозможно разделить на территории, принадлежащие государствам, она подобна космосу, который принадлежит всем. Проводя аналогию с космосом, необходимо отметить, что у всех технологий, находящихся в космосе возможно установить ее собственника или разработчика, ими могут быть государства или частные компании. Однако в отличие от космоса в ИКТ-сфере установить точную принадлежность той или иной технологии определенному государству или частному лицу крайне сложно, как и сложно установить территорию, с которой произошло нападение на ИКТ-инфраструктуру государства.

С одной стороны, главной силой обеспечения безопасности должны выступать суверенные государства, а не отдельные индивиды, но в ИКТ-сфере ситуация складывается иным образом. Технологическая составляющая ИКТ-сферы позволяет физическим и юридическим лицам оказывать существенное влияние на ИКТ-отношения. Мы знаем достаточно примеров влияния ИТ-гигантов на регулирование интернет-отношений. Хакеры, как отдельные лица, так и организованное их сообщество, также могут нанести существенный вред и осуществить компьютерную атаку на ИКТ.

Проблему защиты от кибератаки составляет сложность определения источника нападения, которым может быть программное



обеспечение, начавшее распространять вредоносную информацию или проводить атаку на информационную инфраструктуру.

Для поиска лица, ответственного за проведение кибератаки, необходимо определить разработчика программной технологии, ее тестировщика, а также ее пользователя, поскольку вредоносные действия могут произойти как по причине программных закладок в технологии, так и в силу наличия уязвимостей, которые свойственны всем аппаратно-программным технологиям.

В случае программных закладок в технологии подлежит доказыванию преднамеренность действий разработчика, создавшего свою технологию с возможностями ее несанкционированного использования третьими лицами.

В случае применения уязвимости, встает другой вопрос — подлежат ли эти действия наказанию в соответствии с административным или уголовным законом?

Сложность выявления источника, лица, территории проведения и противодействия компьютерным атакам демонстрируют проблемы атрибуции компьютерных атак.

В связи тесным технологическим и правовым пересечением, атрибуция компьютерной атаки включает исследование двух аспектов: технического и правового, объединенных одной целью — собирание доказательств проведения компьютерной атаки и причастного

лица. Исследования подтверждают, что провести атрибуцию компьютерной атаки очень сложно, многое зависит от примененных для проведения кибероперации технологий, а также от технологий и средств, потраченных на определение источника компьютерной атаки и лица ее реализовавшее.

Много потенциально опасных событий существует в любой ИКТ-среде — это отказы аппаратных средств, нарушения целостности программного обеспечения, вторжения в аппаратно-программный комплекс, угрожающие безопасности<sup>1</sup>. В связи с этим Государства в лице уполномоченных органов должны быть способны проводить мониторинг угроз и понимать, может ли система обеспечения безопасности адекватно бороться с ними.

Проблему атрибуции компьютерной атаки невозможно решить без внимания к вопросам кибербезопасности еще на стадии разработки, поскольку на последующих стадиях, например, на стадии применения информационных технологий исправление уязвимостей и нахождение программных закладок не всегда возможно. Например, устройства можно скомпрометировать еще на стадии разработки, создать уязвимости или программные закладки.

Таким образом, критически важно знать поставщиков, разработчиков или производителей, а также тех, кто испытывает и сертифицирует технологию.

Такие вопросы должны находиться под контролем органов государственной власти.

Для обеспечения информационной безопасности государства видят один путь — это создание условий подчинения своему закону всех лиц, которые используют информационные технологии на его территории<sup>2</sup> и их разрабатывают.

Таким образом, одним из методов обеспечения информационной безопасности и принуждения к выполнению требований национального законодательства является привязка информационных технологий к территории своего государства<sup>3,4</sup>.

Поскольку невозможно снизить уровень взаимосвязанности современных обществ, лучшим вариантом является усовершенствование механизмов сдерживания и способов защиты.

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

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

2 Жарова А.К. О соотношении персональных данных с ip-адресом. российский и зарубежный опыт // Вестник УрФО. Безопасность в информационной сфере. 2016. № 1 (19). С. 61-67.

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

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

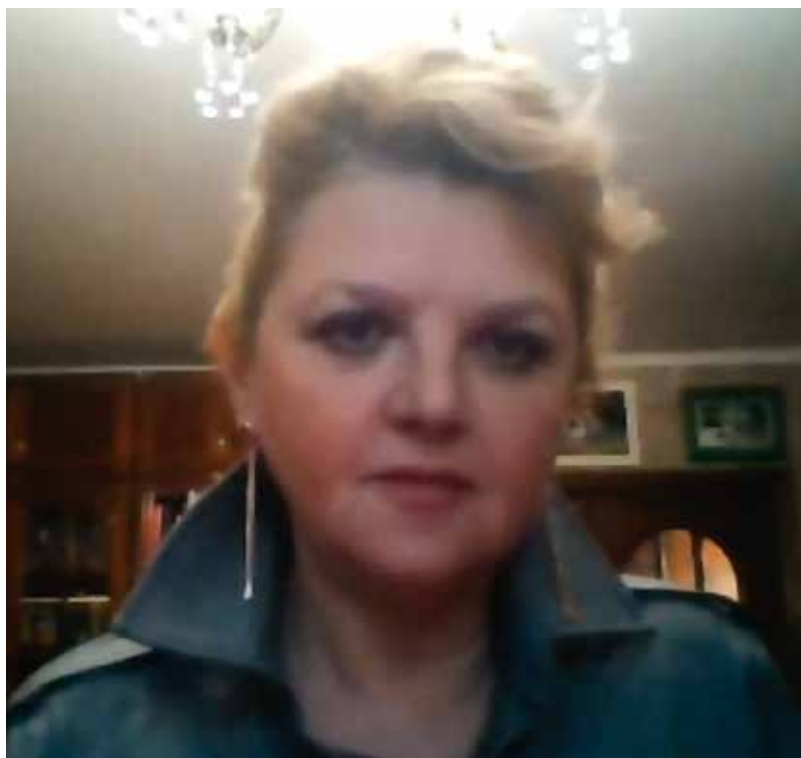
## Н.П. Ромашкина

*к.п.н., профессор, Центр международной безопасности Института мировой экономики и международных отношений имени Е.М. Примакова (ИМЭМО) РАН*

### **ФОРМИРОВАНИЕ МЕЖДУНАРОДНО-ПРАВОВОГО РЕЖИМА ПРЕДОТВРАЩЕНИЯ КОНФЛИКТОВ В ГЛОБАЛЬНОМ ИНФОРМАЦИОННОМ ПРОСТРАНСТВЕ: НОВЫЙ ФОРМАТ**

Текущая кризисная ситуация обозначила большое количество проблем в глобальной среде информационно-коммуникационных технологий (ИКТ), в том числе, юридического обеспечения действий в киберпространстве. Еще недавно о многих этих проблемах эксперты из разных стран говорили чисто теоретически, но сейчас речь идет о практическом применении кибернетического оружия, других информационных и киберсредств в условиях кризиса. И сегодня, как никогда ранее, максимально актуально говорить о новом формате, требующем активных действий по предотвращению конфликтов в глобальном информационном пространстве. А для этого необходимо формирование международно-правового режима<sup>1</sup>.

Характеристики современного международного пространства даны Президентом России В.В. Путиным в Обращении к участникам и гостям X Московской конференции по международной безопасности 16 августа 2022 г: «Ситуация в мире динамично меняется, формируются контуры многополярного мироустройства. Всё больше стран и народов выбирают путь свободного, суверенного развития с опорой на свою самобытность, традиции, ценности... Этим объективным процессам противодействуют западные глобалистские элиты, провоцируя хаос, разжигая застарелые и новые конфликты, реализуя политику так называемого сдерживания, а по сути — подрыва любых альтернативных, суверенных путей развития... США и их вассалы грубо вмешиваются во внутренние дела суве-



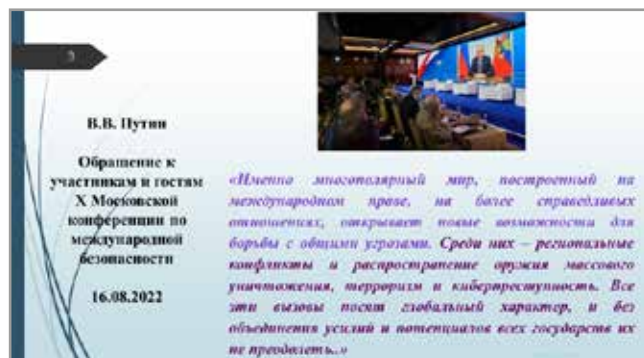
ренных государств: организуют провокации, государственные перевороты, гражданские войны. Угрозами, шантажом и давлением пытаются заставить независимые государства подчиниться своей воле, жить по чужим для них правилам»<sup>2</sup>.

Таким образом, процесс противодействия современным угрозам, в число которых входят все более широкое использование ИКТ во враждебных военно-политических целях и киберпреступность, напрямую связан сегодня с процессом построения многополярного мира, основанного на принципах международного права. И это в полной мере отвечает заявленной теме нашего Форума «Многополярный мир в глобальной ИКТ-среде».

Очень опасной современной тенденцией, характеризующей новый формат процесса предотвращения конфликтов в глобальном информационном пространстве, является существенный рост фактов применения различных ИКТ-возможностей во враждебных военно-политических целях в условиях кризиса. В условиях военных действий. И это происходит на фоне роста количества вооруженных конфликтов в различных точках Земного шара, в том числе, на границах России,

1 Ромашкина Н.П., Марков А.С., Стефанович Д.В. Международная безопасность, стратегическая стабильность и информационные технологии / отв. ред. А.В. Загорский, Н.П. Ромашкина. – М.: ИМЭМО РАН, 2020. – 98 с. <https://www.imemo.ru/publications/info/romashkina-np-markov-as-stefanovich-dv-mezhdunarodnaya-bezopasnosty-strategicheskaya-stabilnosty-i-informatsionnie-tehnologii-otv-red-av-zagorskiy-np-romashkina-m-imemo-ran-2020-98-s>.

2 Обращение к участникам и гостям X Московской конференции по международной безопасности. 16 августа 2022 года. <http://www.kremlin.ru/events/president/transcripts/69166>.



что, безусловно, подрывает ее безопасность. Так называемый, коллективный Запад уже не только на доктринальном уровне, на уровне заявлений и документов, а уже на деле, открыто демонстрирует свою позицию по использованию киберпространства как сферы военных действий<sup>3</sup>.

На фоне таких тенденций 24 февраля 2022 г. Национальный координационный центр по компьютерным инцидентам (НКЦКИ) предупредил об угрозе увеличения интенсивности компьютерных атак на российские информационные ресурсы, в том числе, объекты критической информационной инфраструктуры (КИИ) в период проводимой военной операции на Украине.

Специалисты НКЦКИ рекомендуют российским организациям усилить бдительность при мониторинге вредоносной активности, направленной на объекты, находящиеся в зоне их ответственности, организовать процесс приоритетной обработки информации об аномалиях, обнаруживаемых в работе объектов КИИ. «Любой сбой в работе объектов КИИ

по причине, не установленной достоверно, в первую очередь необходимо рассматривать как результат компьютерной атаки... В случае выявления признаков целенаправленных компьютерных атак незамедлительно информировать НКЦКИ для своевременной выработки мер противодействия»<sup>4</sup>. Кроме того, координационный центр обратил внимание на рост угроз как из информационного пространства недружественных России стран, так и из российского информационного пространства. Мы видим, что эти прогнозы, к сожалению, оказались верными.

Но сегодня речь идет не только о росте угроз кибератак на информационное пространство России, но и на другие структуры критически важной государственной инфраструктуры.

Так, 24 февраля 2022 г. по сообщению телеканала NBC Президенту США Джозефу Байдену был представлен ряд вариантов проведения Соединенными Штатами массированных кибератак, направленных на то, чтобы подорвать способность России поддерживать

3 Ромашкина Н.П. Глобальные военно-политические проблемы международной информационной безопасности: тенденции, угрозы, перспективы / Н. П. Ромашкина // Вопросы кибербезопасности. – 2019. – № 1 (29). – С. 2–9. DOI: 10.21681/2311-3456-2019-1-2-9. [https://cyberrus.org/wp-content/uploads/2019/03/02-09-129-19\\_1.-Romashkina.pdf](https://cyberrus.org/wp-content/uploads/2019/03/02-09-129-19_1.-Romashkina.pdf).

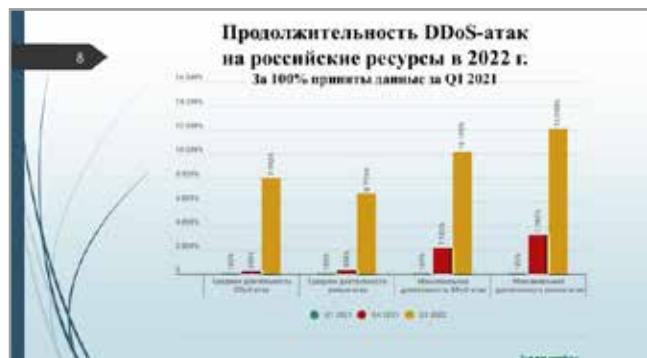
4 НКЦКИ: существует угроза кибератак на российские информационные ресурсы. 24.02.2022. [https://safe-surf.ru/specialists/news/675925/?sphrase\\_id=45691](https://safe-surf.ru/specialists/news/675925/?sphrase_id=45691). <https://safe-surf.ru/upload/ALRT/ALRT-20220224.1.pdf>. Центр кибербезопасности РФ предупреждает об угрозе роста интенсивности кибератак. 24 февраля 2022. <https://tass.ru/obschestvo/13846783>.



**Минобороны Украины обратилось за помощью к хакерскому сообществу**

24.02.2022. Информационство Reuters:

- Глава киевской ИТ-компании Cyber Unit Technologies Егор Аумев по просьбе руководства МО Украины: «Украинское киберсообщество! Пришло время участвовать в киберобороне нашей страны».
- «Два подразделения добровольцев из хакерского сообщества: оборонное и наступательное. Оборонное подразделение – обеспечение безопасности объектов КН. Наступательное подразделение – помощь ВСУ проводить разведоперации».
- На вечер 24 февраля получены сотни заявок от добровольцев.

**Применение космических информационных технологий во враждебных внешнеполитических целях**

- Какие юридические обоснования подобных действий существуют в международном праве и в нормативно-правовой базе США?
- Можно ли это рассматривать как участие в военных действиях, а, следовательно, в качестве военного вмешательства?
- Можно ли это рассматривать как применение силы или угрозу применения силы в соответствии с Уставом ООН?



свои военные операции на Украине<sup>5</sup>. По данным телеканала, специалисты из разведывательных и военных ведомств предлагают «использовать американское кибероружие» в невиданных ранее масштабах. Среди предлагаемых вариантов — «нарушение интернет-соединения по всей России, отключение электроэнергии и вмешательство в железнодорожное сообщение, чтобы помешать России пополнить запасы своих сил». Кроме того, сообщалось, что киберкомандование США, Агентство национальной безопасности, ЦРУ и другие агентства должны будут сыграть свою роль в этих операциях.

США годами закладывали основу для таких возможных киберопераций против России, Китая и других противников. Однако такой масштаб атак ранее если и оценивался специалистами как теоретически возможный, но точно не озвучивался официальными лицами США. При этом речь идет о превентивных кибератаках, независимо от того, предпримет ли Россия кибератаки на Соединенные Штаты.

С конца февраля и по сей день российские интернет-ресурсы подвергаются лавинообразным, очень мощным по силе и продолжительности компьютерным DDoS-атакам.

ИТ-специалисты говорят о ситуации как об эпидемии. Охват и интенсивность атак огромны. В качестве целей атак выступают сайты госорганов и государственных информационных систем, банков и коммерческих предприятий, Роскосмоса, РЖД, Госуслуг, телеком-провайдеров, СМИ, спортивных и общественных организаций, образовательных и медицинских учреждений и так далее.

«Лаборатория Касперского» сообщает, что по косвенным признакам видно, что в начале всплеска DDoS-атак в них принимало участие большое количество так называемых хактивистов, непрофессиональных хакеров. Со временем их доля в общем числе атакующих снизилась. При этом сами атаки стали более мощными, подготовленными и длительными»<sup>6</sup>.

Крайне опасными в настоящее время являются угрозы, связанные с применением космических информационных технологий, спутников стран НАТО и их партнеров во враждебных военно-политических целях. Речь идет о передаче со спутников, в том числе, спутников военного назначения, разведывательной информации формально нейтральным государством для поддержки военных действий одной из сторон военного конфликта и для

5 Biden has been presented with options for massive cyberattacks against Russia. <https://www.nbcnews.com/politics/national-security/biden-presented-options-massive-cyberattacks-russia-rcna17558>.

NBC: спецслужбы предложили Байдену варианты кибератак против России. 24 февраля 2022. <https://tass.ru/mezhdunarodnaya-panorama/13846677>.

6 Отчеты о DDoS-атаках. <https://securelist.ru/category/ddos-reports/>.





уничтожения военнослужащих и военной техники другой стороны.

Так, США открыто заявляют на самых разных уровнях, включая Президента США, что они обеспечивают армию Украины разведывательной информацией со своих спутников, в том числе, спутников военного назначения. Это информация о расположении военных объектов, военной техники и военных подразделений армии России, в том числе, подразделений Донецкой народной республики и Луганской народной республики. Министерство обороны РФ подтверждает эту информацию.

Таким образом, получается, что военные спутники, которые являются частью военной инфраструктуры США, используются во время военных действий, в которых Соединенные Штаты формально не участвуют, для предоставления Украине разведанных о расположении подразделений армии России.

В связи с этим возникают вопросы.

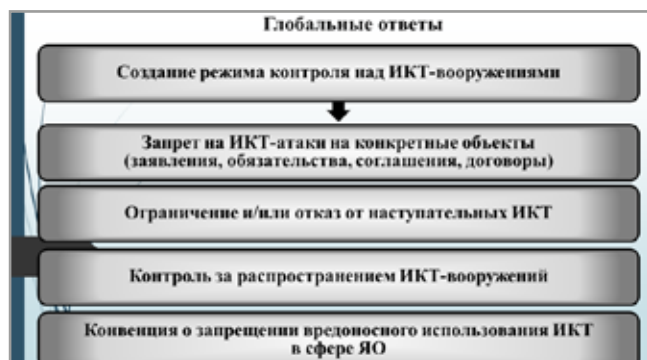
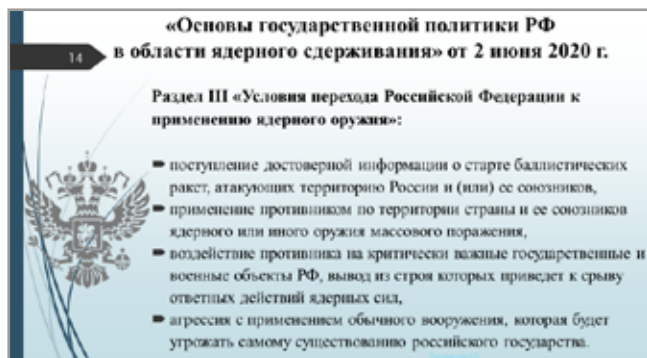
- Какие юридические обоснования подобных действий существуют в международном праве и в нормативно-правовой базе США?
- Можно ли это рассматривать как участие в военных действиях, а, следовательно, в качестве военного вмешательства?

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

Глобальное враждебное информационное воздействие оказывается на мировое сообщество и в другой области, которую можно назвать не только политической, но и этической, моральной. Это существенно усложняет проблему психологического воздействия на граждан с применением информационно-коммуникационных технологий в период кризиса. Вот только один из примеров.

21 апреля 2022 г. на сайте Государственного Департамента США появилась информация под названием «Что такое «Специальная военная операция?»» (*What Is a «Special Military Operation?»*)<sup>7</sup>. После серии фото звучит, по сути, призыв к гражданам США присоединиться к антироссийской пропаганде с использованием нового предлагаемого Госдепом ИКТ-ресурса. Таким образом, гражданам США навязывается необходимость распространения информации, не подтвержденной никакими доказательствами. Следовательно, гражданам США убедительно предлагается использовать личные средства связи для ведения пропаганды в худшем смысле этого слова. При этом речь идет о рассылке сообщений даже не в средствах массовой информации, а на личные номера и адреса граждан

7 APRIL 21, 2022, What Is a «Special Military Operation?». <https://stories.state.gov/what-is-a-special-military-operation/>.



России без их предварительного согласия. Логично рассматривать подобные действия в качестве вмешательства в частную жизнь граждан и РФ, и США.

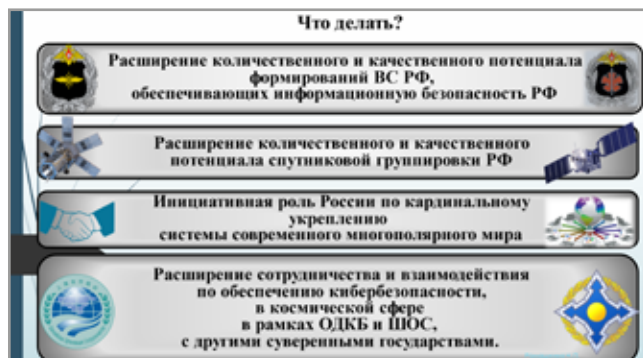
Возникает множество вопросов, в частности:

- Какие юридические обоснования подобных действий существуют в международном праве?
- Какие нормы законодательства США позволяют такие действия?

Все эти наряду с другими вызовами в современных условиях существенно повышают угрозу сокращения, так называемой, «лестницы» эскалации конфликта, а, следовательно, снижает уровень и кризисной, и стратегической стабильности<sup>8</sup>. А это может привести к таким страшным последствиям, которые не выгодны ни одной стране в мире.

При этом важно, что проблема эскалации конфликта усложняется решением НАТО о применении Статьи 5 Устава Альянса к кибернападениям.

Условия перехода Российской Федерации к применению ядерного оружия представлены



в Военной доктрине и в документе «Основы государственной политики РФ в области ядерного сдерживания» от 2 июня 2020 г.

Для повышения стабильности, с целью предотвращения конфликтов, в том числе, в глобальном информационном пространстве целесообразно:

- расширение количественного и качественного потенциала формирований ВС РФ, обеспечивающих информационную безопасность РФ;
- расширение количественного и качественного потенциала спутниковой группировки РФ;
- расширение сотрудничества и взаимодействия по обеспечению кибербезопасности, в частности, в космической сфере в рамках ОДКБ и ШОС, с другими суверенными государствами;
- инициативная роль России по кардинальному укреплению системы современного многополярного мира.

Мир, безусловно, будет другим после окончания военной операции. И рано или поздно крупнейшим ядерным державам придется договариваться и о стратегической стабильности, и о формировании международно-правового режима предотвращения конфликтов в глобальном информационном пространстве. И сегодня уже совершенно ясно, что это напрямую связанные между собой процессы. Но такие усилия требуют новой стратегии действий и новых инструментов.

<sup>8</sup> Ромашкина Н.П. Стефанович Д.В. Стратегические риски и проблемы кибербезопасности // Вопросы кибербезопасности. 2020. № 5. С. 77–86. DOI 10.21681/2311-3456-2020-05-77-86. [https://cyberrus.com/wp-content/uploads/2020/12/77-86-539-20\\_7.-Romashkina.pdf](https://cyberrus.com/wp-content/uploads/2020/12/77-86-539-20_7.-Romashkina.pdf).

## **А.А. Морозов**

*к.ю.н., эксперт в области международной  
информационной безопасности*

### **ПРАВОВОЙ АСПЕКТ ОПРЕДЕЛЕНИЯ ГРАНИЦ ИНФОРМАЦИОННОГО ПРОСТРАНСТВА В СФЕРЕ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

В последние годы особенно остро перед всеми государствами мира, включая Россию, встает проблема определения границ в информационном пространстве.

Как отмечает ряд ученых и экспертов, информационное пространство создается деятельностью человека и его существование без этого невозможно. Существует сразу несколько проблем определения границ в информационном пространстве.

Построение системы международной информационной безопасности подразумевает принятие мировым сообществом принципов сетевой нейтральности, уважения информационного суверенитета, равноправия и децентрализованного управления интернетом.

Информационный суверенитет является ключевым понятием в обеспечении информационной безопасности государства. Выработка определения данного понятия позволит провести границу между государствами в информационном пространстве. К сожалению, в настоящее время в российском законодательстве, как и законодательстве других стран, данный термин не определен и рассматривается только в контексте общего суверенитета государства.

Таким образом, информационный суверенитет по-прежнему является понятием, раскрываемым через описывающие его свойства. Например, для его ущемления могут быть использованы информационно-коммуникационные технологии в террористических, экстремистских и иных целях, а технологическое неравенство государств осложняет его достижение.

Российское законодательство определяет информационное пространство как совокупность информационных ресурсов, созданных субъектами информационной сферы, средств взаимодействия таких субъектов, их



информационных систем и необходимой информационной инфраструктуры. Такое определение дано Стратегией развития информационного общества в Российской Федерации на 2017–2030 годы, утвержденной Указом Президента Российской Федерации от 9 мая 2017 г. № 203.

Данное определение, с одной стороны, является достаточно объемным, а с другой, не позволяет провести ту самую границу между государствами.

В качестве примера. Согласно Федеральному закону «О персональных данных» от 27 июля 2006 № 152-ФЗ персональные данные — любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Персональные данные российского гражданина защищаются законодательством Российской Федерации, включая уголовное. В тоже время такие данные могут быть размещены на облачных сервисах, которые, в свою очередь, не обязательно размещены на территории России. Либо доступ к ним будет осуществляться через чужие средства взаимодействия.

Главный вопрос здесь, будет ли такая информация являться информационным пространством Российской Федерации. По определению информационного пространства получается, что оно считается таковым только



в совокупности ресурсов, субъектов и средств взаимодействия, в дополнение имеем ещё их информационные системы и информационную инфраструктуру. Но субъекты могут быть гражданами либо юридическими лицами одного государства, ресурсы принадлежать другому, а средства взаимодействия третьему. Таким образом, потенциально мы можем получить ситуацию, где у информационного пространства, задействованного в обработке определённой информации, имеется больше одного владельца.

Следующей проблемой определения границ в информационном пространстве является то, что имеющееся определение является в значительной степени техническим, то есть обозначающим средства и способы обработки информации, в тоже время, не включающее себя саму информацию. Информация входит в понятие «информационная сфера» — совокупность информации, объектов информатизации, информационных систем, сайтов в информационно-телекоммуникационной сети «Интернет», сетей связи, информационных технологий, субъектов, деятельность которых связана с формированием и обработкой информации, развитием и использованием названных технологий, обеспечением информационной безопасности, а также совокупность механизмов регулирования соответствующих общественных отношений. Данное понятие раскрывается Доктриной информационной безопасности Российской Федерации, утвержденной Президентом Российской Федерации от 5 декабря 2016 г. № 646.

Но даже в этом понятии не учитывается не вещественный характер информации, она представлена больше как содержание для информационных систем, сайтов и прочих объектов информатизации, в которых циркулирует.

При определении границ информационного пространства необходимо учитывать его двойственную природу. Процессы, происходящие в нём, могут быть направлены на компьютерные системы, тогда можно говорить о цифровом пространстве, или, как принято в ряде зарубежных стран, «киберпространстве». Либо процессы информационного пространства направляются на сознание людей, в таком случае речь идет об информационно-психологической, или «идеологической» составляющей информационного пространства.

Эти оба аспекта с одной стороны, надо отделять друг от друга, для удобной организации работы, проведения исследований, обучения специалистов. С другой стороны, нельзя упускать единство данных противоположностей.

Тут необходимо отметить определенные успехи российского права, особенно на международном уровне. МИДом России при координирующей роли аппарата Совета Безопасности Российской Федерации, с участием заинтересованных федеральных органов исполнительной власти, заключаются межправительственные соглашения в области обеспечения международной информационной безопасности с государствами по всему миру.

В данных международных договорах содержатся положения об основных угрозах в области обеспечения международной информационной безопасности.

Согласно ним, угрозами международной информационной безопасности являются использование ИКТ в следующих целях:

- для осуществления актов, направленных на нарушение суверенитета, безопасности и территориальной целостности государств;
- для нанесения экономического и другого ущерба, в том числе путем оказания деструктивного воздействия на объекты информационной инфраструктуры;
- в террористических целях, в том числе для пропаганды терроризма и привлечения к террористической деятельности;
- для совершения преступлений, в том числе связанных с неправомерным доступом к компьютерной информации;
- для вмешательства во внутренние дела государств, нарушения общественного порядка, разжигания межнациональной, межрасовой и межконфессиональной вражды, пропаганды расистских и ксенофобских идей и теорий, порождающих ненависть и дискриминацию, подстрекающих к насилию и нестабильности, а также для дестабилизации внутрисполитической и социально-экономической обстановки, нарушения управления государством;
- для распространения информации, наносящей вред общественно-политической и социально-экономической си-

стемам, духовной, нравственной и культурной среде других государств.

Из приведенного перечня угроз можно сделать вывод о том, что существует понимание единства «цифрового» и «психологического» аспектов при использовании ИКТ в информационном пространстве. В то же время, присутствует отделение одного от другого.

Подводя итог вышесказанному, хочу сделать следующие выводы.

1. Нечеткость понятия информационного суверенитета по-прежнему не позволяет однозначно определить границы в информационном пространстве. Государства должны договориться о том, что они контролируют в информационном пространстве, а на что их власть не распространяется.

2. Определение информационного суверенитета осложняется использованием совокупности новых ИКТ, имеющих трансграничный характер — облачные, туманные вычисления, сети связи и владельцы данных объектов, осуществляющие свою деятельность в различных правовых системах.

3. Двойственная природа угроз при использовании ИКТ, что вызывает необходимость договариваться с государствами при разграничении информационного пространства по двум направлениям одновременно.

4. В заключении хочу отметить, что работу по разграничению информационного пространства, для достижения успеха, необходимо вести одновременно по трем вышеуказанным направлениям, что должно находить отражение в правовых актах государства.

#### **Список использованной литературы**

1. Соглашение между Правительством Российской Федерации и Правительством Республики Индонезии о сотрудничестве в области обеспечения меж-

дународной информационной безопасности от 14 декабря 2021 года;

2. Соглашение между Правительством Российской Федерации и Правительством Киргизской Республики о сотрудничестве в области обеспечения международной информационной безопасности от 25 февраля 2021 года;
3. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» // Собрание законодательства Российской Федерации от 2006 г. , № 31 , ст. 3451 (Часть I);
4. Указ Президента Российской Федерации от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы» // Собрание законодательства Российской Федерации от 15 мая 2017 г. № 20 ст. 2901;
5. Указ Президента Российской Федерации от 12 апреля 2021 г. № 213 «Об утверждении Основ государственной политики Российской Федерации в области международной информационной безопасности» // Собрание законодательства Российской Федерации от 19 апреля 2021 г. № 16 (часть I) ст. 2746;
6. Указ Президента Российской Федерации от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // Собрание законодательства Российской Федерации от 12 декабря 2016 г. № 50 ст. 7074;
7. Резолюция Генеральной Ассамблеи ООН от 5 декабря 2018 года 73/27. «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности».



**Е.М. Скворцова**

Эксперт Министерства обороны  
Российской Федерации

## **К ВОПРОСУ ОБ УГРОЗАХ СУВЕРЕНИТЕТУ В ИКТ-СРЕДЕ: ОТРИЦАНИЕ КОНЦЕПЦИИ, ПОЛИТИЧЕСКАЯ АТРИБУЦИЯ И КИБЕРСАНКЦИИ**

Уже много лет в международном сообществе обсуждается проблема суверенитета в ИКТ-среде. Общего понимания до сих пор не выработано, но практическая реализация этого феномена является общепризнанным фактом.

Исходя из этого положения, предлагается рассмотреть *угрозы суверенитету в ИКТ-среде*, которые, на наш взгляд, внесут вклад и в общее понимание сущности феномена. Представляется, что причина выявленных проблем кроется в разночтениях по поводу восприятия содержания ИКТ-среды в целом, и суверенитета в ИКТ-среде в частности.

*Первая угроза* возникает из-за различий во взглядах по отношению к ИКТ-среде. Так, либеральные институционалисты и киберлибертарианцы убеждены в том, что Интернет является глобальным достоянием. Исходя из этого, они отрицают полезность концепции суверенитета в ИКТ-среде. Сторонники либерального институционализма и киберлибертарианства сходятся в определении суверенитета в ИКТ-среде как контроля над информацией, коммуникациями, данными и инфраструктурой, связанной с Интернетом. Они по-разному выстраивают аргументацию, но приходят к одному заключению — концепция суверенитета в ИКТ-среде вредна для международного права.

Представители идейных течений видят в суверенитете в ИКТ-среде препятствие для применимости существующего международного права к поведению государств в киберпространстве и выработке новых норм международного права применительно к киберпространству. Они полагают, что продвижение норм суверенитета в ИКТ-среде и применение международного права к киберпространству — понятия взаимоисключающие.

*Либеральные институционалисты* в суверенном праве государств регулировать национальный сегмент видят потенциальные угрозы



фрагментации киберпространства и отключения глобального Интернета.

*Киберлибертарианцы* считают, что наметившиеся тенденции в области суверенитета в ИКТ-среде неизбежного приведут к ограничениям свободы слова в киберпространстве. По их мнению, право человека на доступ к сети Интернет закономерно проистекает из Статьи 10 Конвенции о защите прав и основных свобод 1950 г. Этим они аргументируют убеждение, что государства обязаны поощрять и содействовать возможности свободно высказывать свое мнение в сети Интернет, а ограничение возможности высказываться приравнивают к ущемлению прав человека на образование, участие в общественно-политической сфере, на мирные собрания и объединения. Они подчеркивают вклад Интернета в развитие демократии и реализации права свободы слова и СМИ и убеждены, что право доступа к Интернету должно быть возведено в ранг конституционного. Киберлибертарианцы утверждают, что ограничение прав человека в киберпространстве в пользу обеспечения национальной безопасности государств является неоправданным. В связи с этим критикуется ряд государств за их подход к управлению Интернетом.

Таким образом, либеральные институционалисты видят в суверенитете в ИКТ-среде вызов международному праву и предпосылки для фрагментации киберпространства,

а киберлибертарианцы убеждены, что в киберпространстве не должно быть никаких репрессивных и ограничивающих свободу Интернета правил, и воспринимают суверенитет в ИКТ-среде как нарушение прав человека.

В результате **отрицание полезности концепции** суверенитета в ИКТ-среде снижает чувствительность к вопросам национальной безопасности государств, дискредитирует их подходы к управлению национальным сегментом сети Интернет.

Третьим идейным течением в отношении суверенитета в ИКТ-среде являются *государственники*. Приверженцы этой точки зрения рассматривают сеть Интернет как часть государственной территории и подходят к суверенитету в ИКТ-среде как к важнейшему элементу национальной безопасности. Однако, идейное течение государственников не является консолидированным, и его сторонники делятся на придерживающихся суверенитета внутреннего и суверенитета внешнего.

Внутренний суверенитет в ИКТ-среде предполагает полноту государственной власти и контроль над потоками информации и информационной инфраструктурой в пределах своих границ.

*Внутренний суверенитет* в ИКТ-среде успешно реализуется во многих государствах, например, в России, Китае, Иране и др. Его успешность и жизнеспособность обусловлена применением мер, ориентированных на внутреннего пользователя.

*Внешний суверенитет* в ИКТ-среде рассматривается как независимая политика государства в глобальном информационном пространстве. Внешнего суверенитета придерживаются в США, Великобритании, ЕС и др. Меры обеспечения внешнего суверенитета в ИКТ-среде не столь однозначны и требуют пристального внимания. Речь идет о таких мерах как политическая атрибуция и киберсанкции.

**Политическая атрибуция** является *второй угрозой* суверенитету в ИКТ-среде. Ее преподносят как суверенное право государств на обеспечение суверенитета в ИКТ-среде. Озабоченность вызывает смысл, который США и страны Запада вкладывают в понятие. Так, в изначальном значении атрибуция означает *определение*, в данном случае, виновника кибератаки и ее характеристик. Однако, предпринимаются попытки легитимации полити-

ческой атрибуции как механизма *возложения ответственности* за злонамеренный инцидент с использованием ИКТ на физическое или юридическое лицо. Вместе с тем, возложение ответственности относится к полномочиям наднациональных совещательных органов, например, ООН и др.

Политическая атрибуция и киберсанкции являются взаимосвязанными понятиями. Политическая атрибуция подменяет тщательное и непредвзятое расследование киберинцидентов и используется в качестве основного механизма по введению киберсанкций.

*Киберсанкции* являются *третьей угрозой* суверенитету в ИКТ-среде. В настоящее время функционируют два механизма киберсанкций — США и ЕС. Американские киберсанкции впервые были применены в 2015 г. в связи со вступлением в силу Указа № 13694 «Блокирование собственности определенных лиц, участвующих в значительных вредоносных действиях в киберпространстве». За ними последовали такие документы, предусматривающие применение киберсанкций, как Указ № 13757 «Принятие дополнительных мер для решения чрезвычайной ситуации в стране в связи со значительными вредоносными действиями в киберпространстве» 2016 г., Закон «О противодействии противникам Америки посредством санкций» 2017 г., Закон «О противодействии российскому влиянию в Европе и Евразии» 2017 г. и многие другие.

Механизм киберсанкций ЕС был создан в 2019 г., хотя первые упоминания в официальных документах встречаются еще в 2017 г. Впервые киберсанкции ЕС были применены в 2020 г.

Политическая атрибуция и киберсанкции являются реальными угрозами суверенитету в ИКТ-среде по ряду причин. Киберсанкции и политическая атрибуция:

- 1) представляют собой односторонние адресные меры, несанкционированные ООН;
- 2) применяются как альтернатива урегулированию споров путем переговоров, посредничества, примирения, арбитража, судебного разбирательства и другими мирными средствами;
- 3) сами по себе не решают проблему политического урегулирования конфликтов в ИКТ-среде;

- 4) являются инструментами принуждения одного государства другому с целью получения преимуществ различного характера;
- 5) направлены на преднамеренное причинение репутационного, политического, экономического вреда другому государству;
- 6) являются катализаторами обострения межгосударственных противоречий до уровня угрозы поддержанию мира и стабильности;
- 7) несут риски злоупотребления по отношению к неугодным государствам;
- 8) не дают шанса правонарушителю согласиться или отказаться выполнить обязательства, вытекающие из правонарушения;
- 9) несоразмерны с нарушениями в ИКТ-среде;
- 10) нелегитимны в связи с нерешенностью проблемы атрибуции;
- 11) противоречат положениям доклада Группы правительственных экспертов 2015 г. и резолюции Генеральной Ассамблеи ООН, согласно которым выдвигаемые против государств обвинения должны быть обоснованными;
- 12) непрозрачны в связи с непониманием механизма ввода и отмены, что не прибавляет стимулов для изменения поведения государств в киберпространстве;
- 13) представляют угрозу внутреннему суверенитету в ИКТ-среде;
- 14) не универсальны для обеспечения суверенитета в ИКТ-среде для всех государств и вызывают конфликт интересов;

- 15) создают потенциальные угрозы фрагментации киберпространства.

Таким образом, киберсанкции и политическую атрибуцию нельзя отнести к несиловым и оборонительным мерам обеспечения суверенитета в ИКТ-среде. Они являются категориями наступательного характера, обеспечивая экономическое, политическое и репутационное ослабление неугодного государства. В связи с этим, киберсанкции и политическая атрибуция в силу своей необъективности и конфликтогенного потенциала не могут рассматриваться в качестве действенных мер по обеспечению суверенитета в ИКТ-среде.

Реализация мер по обеспечению внешнего суверенитета в ИКТ-среде, таких как политическая атрибуция и киберсанкции, нарушает суверенитет в ИКТ-среде других государств.

Суверенитет в ИКТ-среде является неотъемлемой частью национальной безопасности, а также оказывает значительное влияние на международную безопасность.

Обеспечение суверенитета в ИКТ-среде требует признания односторонних ограничительных мер *незаконным вмешательством во внутренние дела государств* и эскалацией межгосударственных конфликтов.

Также насущной необходимостью является выработка действенных мер недопущения и предотвращения конфликтов в киберпространстве, в том числе возникающих в связи с обеспечением суверенитета в ИКТ-среде и формирование соответствующего механизма в ООН. Считаем целесообразным на уровне ООН закрепить *принцип универсальности мер по обеспечению суверенитета в ИКТ-среде*.

## А.Н. Курбацкий

Белорусский государственный  
университет

### СУВЕРЕНИТЕТ И МОЛОДЕЖЬ

Я уже не раз на площадке Гармиша упоминал о проблемах построения суверенитета в небольших молодых странах. Сегодня я хотел бы коснуться одной общей проблемы обеспечения суверенитета, верной практически для любого государства.

Всеобщая цифровизация потребовала массовой разработки софта, и в «программисты» массово хлынула молодежь, начиная уже со школьной скамьи.

Действительно, зачем толковым школьникам идти на инженерные, естественнонаучные, конструкторские, сложносистемные специальности, если можно быстро вписаться в «технологический конвейер» разработки софта и гарантированно получать зарплату, которая намного выше зарплаты инженеров, конструкторов, проектировщиков сложных систем? И этот технологический конвейер быстро и массово превращает, среднестатистического программиста в ремесленника, даже, наверное, более точно в ИТ-пролетариат. Причем это не локальный ИТ-пролетариат, а глобальный ИТ-пролетариат (можно сказать даже глобально управляемый), формируемый по клише «граждан мира». Хотя, с резким торможением глобализации перспективы гражданства мира стали не такими уж и очевидными и ясными.

Известный английский историк А. Дж. Тойнби в свое время ввел понятие «опасные классы». Он использовал его при описании процессов конца 18-начала 19 веков, когда вырванное из сельской местности население превратилось в «опасные классы». За десятилетия удалось их превратить в более-менее устойчивый пролетариат. Возможно сейчас процессы с опасными классами повторяются, в частности, с айтишниками, которые оказываются мало приспособленными к реалиям современной жизни. Но глобализация с цифровизацией превратила их в «граждан мира» (как им очень хотелось), но в виде недоформированного ИТ-пролетариата (что их жестко и неприятно приземлило).

Сейчас затруднительно адекватно использовать термины айтишник, программист.



Всеобщая цифровизация практически быстро размывает эти понятия. На постсоветском пространстве понятие айтишник, а иногда даже и программист часто рассматривается как нечто единое, объединяющее и тестировщиков, и кодировщиков, и специалистов по искусственному интеллекту, анализу больших данных, и системных архитекторов и т.д. В современной мировой практике этой цельности нет — все это совершенно разные категории специалистов. Поэтому, когда иногда говорят о новом классе — айтишников, то такого класса строго говоря и нет. Есть, наверное, достаточно массовый айтишный пролетариат (ИТ-пролетариат), которому очень хотелось бы идентифицировать себя с хайтеком. Но, если специалисты в области искусственного интеллекта, анализа больших данных, системные архитекторы, бизнес-аналитики, получившие серьезное образование, будут востребованы, то профессии тестировщика и кодировщика и близкие к ним, но с модными названиями могут быстро исчезнуть. В частности, искусственный интеллект способен этому сильно помочь. А своего рода миф о том, что нужно так много программистов отчасти поддерживается тем, что просто создается очень много некачественного кода (софта).

Мы всегда должны помнить, что в эпоху всеобщей цифровизации роль технологического суверенитета резко возрастает. Но без молодежи невозможно развивать технологи-



ческий суверенитет. А молодежь мы упускаем. То есть молодежь вроде бы и стремится к новым технологиям, мы вроде бы и поощряем такое стремление, но этот процесс какой-то однобокий. Возьмем опять ИТ-сферу на постсоветском пространстве.

В университетах, где готовят ИТ-специалистов, много учебных центров и классов по Microsoft, Oracle, Cisco, SAP и т. п. Но это не научно-исследовательские центры, а банальные центры навыков, компетенций по простому кодированию, тестированию, внедрению и эксплуатации. Конечно, это неплохо, если бы в итоге не подменялись основные университетские курсы. Студенты видели, что в таких центрах разработки не нужны серьезная математика, физика. Терялась мотивация. Наиболее способные молодые специалисты плавно перетекали из центров разработки в центры за пределами страны, где этапы жизненных циклов разработки более интересны. Как правило, они не возвращались. Например, для нашей небольшой страны это существенные потери. Как выясняется, нередко в подобной эмиграции главное даже не заработки, а возможность творчества вместо ремесла и промышленного программирования. По сути, такая модель ускорила разрушение инженерного, конструкторского, общесистемного образования. Утрачивалась мотивация к изучению математических, физических, сложносистемных дисциплин. Действительно, студенту незачем тратить время на их глубокое освоение, если достаточно получить навыки по кодированию и тестированию софта на основе несложных технологических платформ и легко найти работу в одной из конвейерных компаний по разработке софта. По сути образование подстраивалось под такую модель и планомерно разрушалось при активном участии тех же западных конвейеров.

Вспомним, что традиционные западные обыватели мало интересуются глобальными вещами. Их интерес в основном локален. Например, решения муниципальных властей для них интереснее решений властей штата или земли, не говоря уже о решениях федеральных властей. Конечно могут быть исключения, но они лишь, как обычно, подтверждают общность. Точно таким же формируется у нас и молодое поколение, особенно айтишное. Действительно система образования и воспи-

тания не воспроизводит сейчас системность во взглядах и оценках. Хорошая системность предполагает умение анализировать и синтезировать информацию, в том числе и по-глобальному. Советская система образования и воспитания, пусть и несколько односторонне, все-таки этому способствовала. Теперь же, в связи со старением и уходом поколений-носителей такой концепции, такая система образования и воспитания полностью исчезает. А новая не создана, вернее лихорадочно, бессистемно создается как ухудшенная калька с быстроразрушающейся западной системы, причем, зачастую, даже не с исконно западной, а как калька с восточно-европейской кальки. И у молодежи формируется основная парадигма, зачем думать о глобальном, системно, главное, чтобы в локальном мирке было все хорошо и как следствие нынешние молодежные установки: «жизнь в моменте», «хорошо в моменте», «хорошо здесь и сейчас» и тому подобное.

И именно айтишный пролетариат является основным носителем таких установок. И понятно почему. Они работают практически полностью в западном (американском) конвейере, причем выполняя в основном самые примитивные операции, то есть работают как современный ИТ-пролетариат, даже не как инженеры, технологи, не говоря уже о конструкторах или архитекторах. То есть совершенно не элита.

По такой модели мы получили лишь ускорение потери суверенитета технологического, и, как следствие, разрушение странового суверенитета.

Хотя последние несколько лет наконец-то многие в мире спохватились, что нужен суверенитет для стран. Глобалистский мир оказался не столь уж безопасен и привлекателен, как был распиарен за последние лет тридцать, граждане мира, как мировые кочевники, не столь уж и конструктивны и креативны — собственно, все как всегда: хороша только виртуальная картинка, в существенно иных условиях идеи глобализма могли бы быть и продуктивны, но народ не тот, элиты не те и тому подобное. Модно стало говорить о цифровом суверенитете, суверенитете в области высоких технологий, суверенитете в области ИКТ и так далее. Соответственно, откликаясь на моду, хайп (а сейчас многое пытаются де-



лать на волнах хайпа) стали писать концепции и стратегии для разного вида суверенитета. Хотя после стольких лет построения глобалистского мира (как видим теперь не очень-то удачного), строить суверенитеты многим странам крайне затруднительно.

Для небольших стран хотелось бы отметить следующее.

В условиях достаточно жесткого противостояния и противоборства нет смысла стремиться к топовым с точки зрения глобальных экспертов, существующих, как обычно, на средства ТНК, ИКТ-решениям. Те же топовые чипы 2–3 нано зачем нужны на данном этапе для оборонки, государства, индустрии, социальной сферы и т.п. Можно и 90 нано обойтись. Не нужно путать требования потребительского рынка и требования для решения государственных, страновых задач. Тот же Apple, или Microsoft, или Samsung, создавая гаджеты и сервисы для конечного потребителя решают совершенно иные задачи. Им нужно удержать лидерство на рынке, чтобы сохранить миллиардные прибыли, отсюда и 2–3 нано в чипах, и все новые и новые операционные системы, и все новые и новые приложения. Бег по кругу, новый системный и прикладной софт требует нового железа, новое железо требует нового софта — и за все расплачивается конечный потребитель. А решение задачи сохранения суверенитета страны в текущей ситуации такой безудержной гонки совершенно и не требует. И чипы нужны попроще, но надежнее, и операционные системы нужны не навороченные, и приложения нужны не такие уж многофункциональные. Классический пример с MS Word. Обычный пользователь использует

не более 5% возможностей редактора. А, например, госслужащим и им подобным и 5% много. Точно также и с большинством софта. Нужны гораздо более простые, но стабильные и надежные системы. И тогда, чтобы создать такие системы нужны не сотни тысяч ИТ-пролетариата, а сотни, ну может быть тысячи высококвалифицированных разработчиков и относительно небольшое количество ИТ-пролетариев. Еще раз подчеркну, страна для своего суверенитета и транснациональный ИТ-бизнес решают совершенно разные задачи и преследуют совершенно разные цели. Можно еще напомнить, что массы ИТ-пролетариата бизнесу нужны и для того, чтобы раздувать значимость фирмы, создавать иллюзию гигантизма, особенно, если твоя фирма на IPO в Нью-Йорке или Лондоне, или хотя бы в Гонконге. Понятно, что массовый инвестор больше поверит в фирму с десятками тысяч работников, чем в небольшую команду.

Но коль уж мы от цифровизации никуда не денемся, то нужна цифровизация хорошо продуманная, просчитанная, с глубоким прогнозированием последствий, а не безудержная, с агрессивной рекламой, что создает у людей совершенно ложные ориентиры. В подавляющем случае это делается опять же непрофессионально айтишным пролетариатом, втянутым в разработку на волне хайпа о неограниченной цифровизации всего и вся. А для того, чтобы это понимать, молодежи нужно соответствующее образование. И выбора нет — либо мы такое образование очень оперативно сформируем, либо окончательно потеряем думающую молодежь, и, соответственно, окончательно потеряем и суверенитет.



## **КРУГЛЫЙ СТОЛ № 2**

### **ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ**

**Модератор:**

*Манахова А.С.*, советник вице-президента по информационной безопасности  
ПАО «ГМК «Норильский никель»

**РОССИЙСКИЕ ПОДХОДЫ К  
ВОПРОСАМ ЗАЩИТЫ КРИТИЧЕСКОЙ  
ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ  
В КОНТЕКСТЕ РЕАЛИЗАЦИИ  
МЕР УКРЕПЛЕНИЯ ДОВЕРИЯ В  
ИНФОРМАЦИОННОМ ПРОСТРАНСТВЕ  
НА ПРИМЕРЕ ОБСЕ**

Проблематика обеспечения защиты критической информационной инфраструктуры (КИИ) многогранна. Это широкий спектр вопросов ее безопасности, межведомственного взаимодействия, подготовки кадров, импортозамещения и т.д. Безусловно, есть и дипломатическое измерение, задача которого — в налаживании международного сотрудничества.

В условиях нарастающего геополитического излома мы все видим реалии положения дел в глобальном информационном пространстве. С учетом экспоненциального роста (в подавляющих случаях — анонимных, тщательно маскируемых) злонамеренных действий против объектов КИИ, актуальность решения данной проблемы в интересах всех без исключения государств у России не вызывает сомнений.

В дополнение к основному треку обсуждения вопросов обеспечения международной информационной безопасности (МИБ) — Рабочей группе открытого состава ООН по вопросам безопасности в сфере использования информационно-коммуникационных технологий (ИКТ) и самих ИКТ 2021–2025 отмечаем в последние несколько лет значительный в последние несколько лет рост внимания к проблематике КИИ и на крупных региональных площадках, в частности в Европе и Азии.

Межгосударственным форматом обсуждения вопросов безопасности в сфере МИБ и использования ИКТ в Организации по безопасности и сотрудничеству в Европе (ОБСЕ) является Неформальная рабочая группа (НРГ) по выработке мер укрепления доверия (МД) в информационном пространстве, учрежденная в соответствии с решением Постоянного Совета ОБСЕ от 26 апреля 2012 года № 1039. За 10 лет существования НРГ единственным, по сути, осязаемым результатом можно назвать выработку и согласование



в 2013 и 2016 годах корпуса из шестнадцати МД, направленных на сокращение рисков возникновения конфликтов в результате использования ИКТ.

Меры укрепления доверия разрабатываются в целях содействия обеспечению международной безопасности и стабильности. Каждая мера в отдельности и все в целом служат именно этой цели — недопущению эскалации напряженности между государствами.

Предыдущий 2021-й и нынешний годы характеризуются новыми тенденциями в деятельности НРГ. Подходы к операционализации ряда мер дрейфуют от обеспечения национально ориентированных интересов безопасности в сторону выработки на их основе методик закрепления коллективной региональной безопасности стран западного блока. Среди ключевых навязываемых сюжетов — продвижение политической атрибуции инцидентов в информпространстве, связанных с КИИ, и скоординированное реагирование на них в логике «миропорядка, основанного на правилах». Фактически группа используется «коллективным Западом» для отработки своих подходов с прицелом на последующую их универсализацию в ООН.

В связи с этим складывается впечатление, что некоторые государства-участники ОБСЕ начинают забывать истинные цели создания МД, которые изначально разрабатывались в военной сфере с целью предот-

вращения непредумышленных конфликтов путем повышения транспарентности действий стран в контексте международной безопасности. Главным критерием эффективности МД являются практические результаты, достигнутые международным сообществом по недопущению возникновения кризисных ситуаций и напряженности в межгосударственных отношениях. К сожалению, выдающихся успехов на данном направлении достичь пока не удалось.

В ходе операционализации МД № 15 государствам-участникам ОБСЕ предлагается предпринять необходимые шаги для поощрения и облегчения регионального и субрегионального взаимодействия между законно уполномоченными органами власти, отвечающими за безопасность критических инфраструктур, и/или участвовать в этом взаимодействии с целью обсуждения существующих возможностей и решения проблем, стоящих перед национальными и трансграничными ИКТ-сетями, от которых зависят критические инфраструктуры. Рассматриваются практики государств-участников, дающие обзор различных определений национальных секторов критической инфраструктуры, возможных контролирующих органов и процедур управления кризисными ситуациями. В них приводятся различные действия и программы, направленные на повышение потенциала на двустороннем, субрегиональном и региональном уровнях, упоминаются договоренности и форматы сотрудничества с частным сектором. Ландшафт ОБСЕ в данной области очень сложен и разнообразен, законодательные рамки и степень зрелость национальных структур реагирования на инциденты в критической инфраструктуре различны.

В мае 2022 года НРГ начала обсуждение вопроса дальнейшей проработки МД № 15 и решения тех проблем, которые стали актуальными в свете новых условий безопасности и нарастающих киберугроз против национальных критических инфраструктур. Суть весенней активизации — новая, предложенная США инициатива, касающаяся создания на региональном уровне механизма осуществления коллективного реагирования в случае серьезного компьютерного инцидента в отношении объектов КИИ государств-участников ОБСЕ.

Забегая вперед отмечу, что эта инициатива при предлагаемых сейчас Западом подходах видится нами как очередной санкционный инструмент и может быть использован в политических целях для дискредитации «неудобных» государств.

Более того, подход, при котором возможно применение военной силы в качестве средства реагирования на инциденты в сфере кибербезопасности в случае возникновения значительного или крупного кризиса использовать чрезвычайно опасно. Это связано с отсутствием определения терминов: «инцидент в сфере кибербезопасность», «значительный кризис» и других.

Не сформулированы юридические критерии квалификации инцидентов в качестве «вооруженного нападения» с использованием ИКТ. Не ясно, каким образом выявляются и распознаются источники компьютерных атак для определения их адресного пространства и иной принадлежности. В условиях вероятности неверного определения источника атаки возникает риск ошибочного применения военной силы, что, в свою очередь, может спровоцировать квалификацию такой силовой реакции на инцидент как акт агрессии.

МД № 15 — синтетическая, многослойная. В ней заложены, в частности, обмен информацией об угрозах, связанных с ИКТ, и разработка совместных мер реагирования на общие вызовы, включая процедуры регулирования кризиса в случае широкомасштабного или транснационального сбоя в функционировании критических инфраструктур, зависящих от ИКТ.

В настоящее время международное сообщество показывает свою заикленность на тематике «компьютерных атак, осуществляемых под руководством правительств», забывая о существовании организованной преступности, террористических группировок и отдельных хакерах.

В условиях, когда существующие механизмы атрибуции источника вредоносных воздействий не позволяют однозначно идентифицировать причастность государства к осуществлению компьютерных атак, а разведисты никогда не будут добровольно раскрыты, считаем важным сосредоточить свои усилия не на бездоказательном обвинении государств, а на налаживании и повыше-



нии статуса межгосударственного взаимодействия в области реагирования на компьютерные инциденты.

Одним из основополагающих вопросов обеспечения МИБ является обмен информацией об инцидентах на межгосударственном уровне. Поскольку современные компьютерные атаки носят трансграничный характер, эффективное противодействие им возможно только в случае отлаженного сотрудничества между профильными экспертами государств, ИКТ которых оказались затронуты и/или являлись источниками вредоносной активности. Базисом такого сотрудничества является оперативный обмен технической информацией о произошедших инцидентах. Как известно, время реагирования на компьютерный инцидент напрямую влияет на размер ущерба, причиненного атакованной системе.

Важно иметь единую точку взаимодействия сторон в области обмена информацией об инцидентах, в противном случае, исходя из имеющегося опыта, взаимодействие может оказаться неэффективным. Независимо от международной обстановки, такой контактный пункт должен сохранять политическую нейтральность, продолжая осуществлять взаимодействие с другими контактными пунктами в области реагирования на угрозы безопасности при использовании ИКТ и самих ИКТ. Контактные пункты должны снижать эскалацию между государствами при возникновении конфликтов.

В этих целях Российская Федерация принимает активное участие в создании глобального реестра контактных пунктов под эгидой ООН, а также разработке четких правил и процедур взаимодействия уполномоченных органов и перечня базовой информации, в том числе технического характера, необходимой для реагирования на компьютерные атаки и инциденты.

Именно реализация вышеуказанных процессов в конечном итоге ведет к облегчению регионального и субрегионального взаимодействия между законно уполномоченными органами власти, отвечающими за безопасность критических инфраструктур.

Одним из направлений работы по реализации МД № 15 является принятие национальных систем классификации инцидентов в сфере ИКТ в зависимости от их масштабов и серьезности.

Шкала классификации компьютерных инцидентов может быть реализована как инструмент предупреждения и выстраиваться по принципу определения общего уровня угроз безопасности государства (по поступающей из разных источников информации), а может исходить из характеристик компьютерного инцидента (масштаб, последствия, используемое вредоносное программное обеспечение, тип инцидента и т.д.).

Основываясь на российском опыте, такая шкала является вспомогательным инструментом для принятия решения высокопоставленными лицами при реагировании на компьютерные инциденты. Убеждены, что при реагировании ключевым является не классификация инцидентов, а именно принимаемые меры. По нашему мнению, шкала является важным инструментом для выработки между техническими специалистами и политиками общего понимания серьезности последствий компьютерного инцидента для государства и общества на национальном уровне и предназначена для использования внутри страны. Применение такого инструмента необходимо для определения роли и места каждого национального ведомства в случае реагирования на масштабный инцидент.

При разработке шкалы классификации компьютерных инцидентов необходимо определять четкие границы между уровнями опасности для предотвращения субъективной оценки того или иного инцидента, которое может привести к риску ошибочного восприятия, эскалации и конфликту.

В то же время меры по предупреждению компьютерных атак и ликвидации их последствий на уровне государства всегда конкретны, зависят от обстановки и могут сильно меняться в ходе инцидента. По сути дела, окончательная классификация происходит только после выяснения всех обстоятельств и растянута во времени. Таким образом, для целей предотвращения развития конфликта и устранения недопонимания без создания объективных и независимых средств определения источников компьютерных атак на КИИ такая шкала применима только как вспомогательный инструмент на национальном уровне.

Новой тенденцией 2022 года является повышающаяся доступность инструментария для осуществления компьютерных атак. В на-

циональных информационных пространствах ряда государств происходит бесконтрольное распространение таких инструментов, инструкций по методам их организации и выработке практических навыков применения. Фактически сформировалось предоставление инструментария в рамках сервисных моделей Malware-As-a-Service, Attack-as-a-Service. В этой связи большие сомнения вызывает необходимость присвоения ответственности за осуществление злонамеренных компьютерных атак тому или иному государству. И, здесь возникает вопрос, как доказать социально-политическую выгоду того или иного актора при эскалации напряженности во взаимоотношениях между двумя сторонами, особенно если это будет выгодно третьей стороне, которая

по формальному признаку не участвует в конфликте?

По нашему мнению, политическая атрибуция не отвечает основным целям Устава ООН, в частности поддержанию мира и международной безопасности. В связи с этим в целях демилитаризации международного информационного пространства Российская Федерация в очередной раз призывает государства сконцентрировать усилия на прагматичном и деполитизированном межгосударственном взаимодействии в области реагирования на компьютерные инциденты. Эффективное и оперативное противодействие новым вызовам, постоянно возникающим в информационных пространствах государств, возможно решить лишь совместными усилиями.

## Тимур Аитов

к.ф.-м.н., зампред комиссии по цифровым финансовым технологиям Совета ТППРФ Совета ТППРФ по финансово-промышленной и инвестиционной политике

### ЦИФРОВАЯ ЭКОНОМИКА В УСЛОВИЯХ САНКЦИЙ. СТРАТЕГИИ ПРОРЫВА

«...Конечно, ситуация сегодня непростая: вся страна прошла своего рода пен-тест («пенетрейшн тест» — как его называют «безопасники», тест на проникновение, на поиск уязвимостей). Обнаружили, что эти уязвимости есть, но в целом ситуация под контролем. Как действовать дальше? Как строить, развивать инфраструктуру? За какую ниточку тянуть, чтобы решить все проблемы? Есть ли такая нитка? Об этом в докладе.

Напомню, цифровая инфраструктура страны зарождалась в 90-х годах, когда было ФАПСИ, которое занималось инфо-телекоммуникационными системами (ИТКС), строило ЛВС для органов государственной власти и сети данных для более широкого круга пользователей. Тогда уже появились биржи — и они работали удаленно. А в 93-ем году в банках уже можно было пользоваться сервисами ЭЦП на каналах модемной связи (интернета еще не было...).

После реорганизации ФАПСИ в 2000-х годах стали появляться госпрограммы по созданию цифровой инфраструктуры. Это были малосвязанные между собой программы. Упомяну «Электронную Россию», «Электронную Москву» (которая не входила в «Электронную Россию»), запустили и «Электронный округ» (Зеленоград), слабо связанный с предыдущими двумя программами.

Наиболее ярко проблема межведомственного взаимодействия и отсутствия единого хозяина проявилась в проекте создания карты «УЭК» — «универсальной электронной карты». Под неё было выделено и финансирование, и выпущен даже специальный закон (в течение месяца сразу в трех чтениях), но через несколько лет программу тихо свернули без каких либо результатов.

Эксперты тогда уже отмечали в этом проекте не только проблему межведомственного взаимодействия, но и отсутствие комплексного подхода к проектированию архитектуры цифро-



вой инфраструктуры и четкого целеполагания. Примечательно, что в обсуждениях перспектив УЭК участвовали и представители РПЦ.

До сих пор у цифровой инфраструктуры страны нет единого владельца — единого ведомства, которое, как регулятор, ведало бы всеми процессами долгосрочного развития, проектирования и создания инфраструктуры цифровой экономики. Некоторые важнейшие функции находятся под контролем ФСБ, некоторые у ФСТЭК, много делает Минцифра — но она не покрывает все задачи. Некоторые сферы вообще не имеют четкого регуляторного покрытия. Как пример — это защита банковских данных. Здесь ЦБ делает много по части информационной безопасности, но именно регулятора по защите всех клиентских баз при построении и операций с ними в стране сегодня не существует.

Отмечу Центробанк, который взял на себя роль активного создателя цифровой инфраструктуры в финансовой отрасли. АО «НСПК» и карта «Мир», «СБП» и новая Система Передачи Финансовых Сообщений (СПФС), а также проекты по линии Ассоциации Финтех — всё находится в надежных руках ЦБ и здесь достижения ЦБ значительны. Но не все задачи финансистов совпадают со стратегией развития цифровой инфраструктуры страны по масштабам. Кроме того, даже в случае четкого руководства остаются узкие места, которые при усложнении обстановки и новых ата-

Шестнадцатый Международный Форум  
«Партнерство государств, бизнеса и гражданского общества при  
обеспечении международной информационной безопасности»

**Цифровая экономика в условиях санкций.  
Стратегии прорыва**

 **Тимур Литов, канд.фин.-мат.наук,**  
руководитель Центра компетенций «Цифровизация финансовых технологий» Фонда  
развития цифровой экономики, заместитель председателя Комиссии по цифровым  
финансовым технологиям Совета ТПП РФ  
timur@decdfund.ru

Москва, 19-21 сентября 2022

Страна прошла **«пентест»** - тест на  
проникновение -  
**уязвимости есть, но ситуация под  
контролем**

Как действовать дальше? Как развивать инфраструктуру?  
За какую ниточку тянуть, чтобы все проблемы решить?  
**Есть ли такая «ниточка»?..**

*об этом в докладе*

**Инфраструктура зарождалась в 90-х**

ФАПСИ занималось инфо-телекоммуникационными системами (ИТКС),  
строило ЛВС для органов госвласти и сети данных для более  
широкого круга пользователей



☐ тогда уже появились биржи — и они работали удаленно.  
☐ в 93-ем году в банках уже можно было пользоваться сервисами ЭЦП  
на каналах модемной связи (интернета не было...)

После закрытия ФАПСИ в 2000-х годах появились  
госпрограммы по созданию цифровой  
инфраструктуры  
это были малосвязанные между собой программы



☐ Появилась «Электронная Россия», потом «Электронная Москва» (которая не входила  
в «Электронную Россию»), был «Электронный округ» (Зеленоград), слабо связанный с  
предыдущими двумя программами.

*На публичных мероприятиях были острые дискуссии..*

как могут превратиться в уязвимости. Упомяну ORACLE на котором многие крупные банки работают, но который ушел из страны и который этим может создать проблемы всем. Даже ЦБ, который его тоже использует.

Что нам нужно сейчас? Кто-то должен «вести вопрос» целиком и отвечать за долгосрочную стратегию развития и общую архитектуру цифровую инфраструктуру (ЦИ). Нужен особый Регулятор, который отвечал бы за всю цифровую инфраструктуру, выражал общенациональные интересы в части развития ЦИ, был бы равноудалённым от всех нынешних и будущих потребителей сервисов и который стал бы еще Главным Архитектором Инфраструктуры.

Этим регулятором должен быть некий Федеральный центр Стратегического планирования, анализа и контроля (ФЦ СПАК) — уровня Госплана СССР — важно, что он не должен функционально заменять Госплан, а, скорее, давать акцент в сторону целеполагания и проектирования целевой архитектуры.

Каждый инфраструктурный проект в перечне «Госплана 2.0» должен иметь одну из трех меток.

- Метка #1: это проект, который имеет особое значение для защищенности России. И еще — про этот проект можно сказать нечто конкретное о его окупаемости в масштабах нашей страны. Проект с меткой #1 делаем обязательно самостоятельно, никому не передаем!

- Метка #2: это проект который ведем с дружественными нам странами из ШОС, БРИКС, ОДКБ и других содружеств, которые, возможно, еще и МИД России будет «подбрасывать» потому что есть такая специфика момента: ИТ связано с МИД России через эти проекты. Проекты с меткой #2 выгодно и правильно делать сообща в содружестве стран.

Примером проекта с меткой М#2 является сервис СПФС. Как мы его делали? СПФС сделали сами, скопировали при этом СВИФТ, а теперь приглашаем других. Надо было наоборот — сначала обсудить в сообществе стран, снять ограничения и недостатки СВИФТ (а они у него есть!), а потом уже делать.

- Метка #3 («черная») — это сервисы недружественных стран, ими все равно придётся пользоваться. Не сможем мы обойтись сразу без многих инфраструктурных сервисов мирового масштаба, уровня GAFA (Google, Amazon, Facebook, Apple). Вот Android нам грозит выключить — но сразу ничего не произойдёт, и надо пользоваться тем, что сегодня дают провайдеры западных стран. Но! Диверсифицировать, дублировать сервисы и помнить — что в любой момент их могут отключить.

В заключение хочу отметить: надо проанализировать всё то, что было и найти недостатки, почему не выполнено? А в будущую про-

**Наиболее ярко проблема межведомственного взаимодействия проявилась при создании карты «УЭК» «универсальной электронной карты»**

Под УЭК было выделено и финансирование и принят специальный закон, но через несколько лет программу тихо свернули без каких либо результатов...



- Эксперты отмечали не только проблему межведомственного взаимодействия, но и отсутствие комплексного подхода и четкого целеполагания
- В обсуждениях участвовали и представители РПЦ

**До сих пор у инфраструктуры нет единого владельца –**

**единого ведомства, которое, как регулятор, ведало бы всеми процессами создания инфраструктуры цифровой экономики..**

- некоторые важнейшие функции находятся под контролем ФСБ,
- некоторые у ФСТЭК,
- конечно, есть «Минцифра», которая делает много, но она не покрывает все задачи..
- некоторые сферы не имеют четкого регуляторного покрытия:



как пример - это защита банковских данных. ЦБ делает много по части ИБ, но именно регулятора по защите всех клиентских баз при построении и операций с ними сегодня не существует

**ЦБ взял роль создателя инфраструктуры отрасли**

АО «НСПК» и карта «Мир», «СБП» и новая Система Передачи Финансовых Сообщений (СПФС), а также проекты по линии Ассоциации «Финтех» - всё находится в его надежных руках и здесь достижения ЦБ значительны

- Но даже в случае четкого руководства остаются узкие места, которые при усложнении обстановки и новых атаках могут превратиться в уязвимости



Упомяну ORACLE на котором многие крупные банки работают, но который ушел из страны и который этим может создать проблемы всем. Даже ЦБ

**Что нужно сейчас для прорыва ?**

**кто-то должен «вести вопрос» целиком - нужен особый Регулятор:**

- который бы отвечал за ВСЮ цифровую инфраструктуру
- который был бы равноудаленным от всех нынешних и будущих потребителей сервисов
- который стал бы Главным Архитектором Инфраструктуры...

**По сути это будет орган**

**«Стратегического планирования, анализа и контроля» уровня Госплана СССР**

Новый Госплан 2.0 должен не подменять Госплан СССР функционально, а скорее, делать акцент

- в сторону целеполагания и
- проектирования целевой архитектуры

**Инфраструктурный проект в перечне «Госплана 2.0» должен иметь одну из трех меток**

- Метка #1 означает проект, который имеет особое значение для защищенности России
- И еще - про этот проект с М#1 что-то определенное можно сказать о его окупаемости в масштабах нашей страны

Проект с меткой #1 делаем обязательно самостоятельно, никому не передаем!

грамму создания инфраструктуры заложить историю и опыт того же ФАПСИ — которое много сделало хорошего.

**Стенограмма дискуссии при обсуждении доклада**

В ходе обсуждения доклада и возникшей дискуссии Аитов отметил следующее.

Название «цифровой Госплан» оно образное — и никого не должно вводить в заблуждение. Это совсем не ведомство, которое будет «планировать тапочки» для страны, это «Федеральный центр Стратегического Планирования, Анализа и Контроля», ФЦ СПАК — который должен проектировать цифровую инфраструктуру страны на долгосрочную перспективу, формулировать долгосрочное видение развития ЦИ и стратегические цели в этой области ( в особенности, дело касается компонент Федерального уровня). В ФЦ СПАК будут работать эксперты, покрывающие ос-

новные предметные области экономики, и при этом умеющие и грамотно проектировать соответствующую инфраструктуру. Конечно, этот центр должен будет осуществлять авторский надзор и контроль за реализацией проектов.

Часть толковых экспертов можно забрать из министерств, а у министерств останутся присущие им регуляторные функции. Этот ФЦ СПАК превратится в своего рода «мозговой центр», который будет заниматься стратегическим целеполаганием и проектированием будущего цифровой инфраструктуры страны. Как главный архитектор и визионер этот Центр обязан будет создать и отобразить общую картину — всю архитектуру, все ее уровни, отразить в соответствующих документах все направления долгосрочного развития. Должна быть создана и концепция развития технологической инфраструктуры на 5 или на 10 лет вперед — ее сегодня у нас нет.



**Инфраструктурный проект  
в перечне нового «Госплана 2.0» должен иметь  
одну из трех меток**

- ❑ **Метка #2:** это проект который ведем с дружественными нам странами из **ШОС, БРИКС, ОДКБ** и других содружеств
- ❑ Возможно, **МИД** будет давать идеи содружеств, потому что есть такая специфика момента: ИТ связано с МИД через эти проекты

**Проекты с М#2 выгодно делать сообща в содружестве стран**



ПРИМЕР М#2 СПФС  
Мы **СПФС** сделали сами, скопировали **СВИФТ**, а теперь приглашаем других. Надо наоборот – сначала обдумать в сообществе стран, снять ограничения и недостатки СВИФТ, а потом уже делать

**Инфраструктурный проект  
в перечне нового «Госплана 2.0» должен иметь  
одну из трех меток**

- ❑ **Метка #3** («черная»): это сервисы недружественных стран - ими все равно придётся пользоваться
- ❑ сложно сразу обойтись без многих инфраструктурных сервисов мирового масштаба, уровня **GAFA** (**Google, Amazon, Facebook, Apple**).
- ❑ Android грозят выключить, но сразу ничего не произойдёт - надо пользоваться тем, что сегодня дают провайдеры западных стран..

**..Но! Диверсифицировать, дублировать сервисы и помнить, что в любой момент их могут отключить**

Как работать ФЦ СПАК с субподрядными организациями задают вопрос? Как пойдет процесс? В любом крупном проекте есть Главная организация, а есть субподрядчики, различного рода эксперты, которые выполняют частные, возможно, даже ведомственные задачи. Такова общепринятая практика, ничего нового здесь нет. Отдельные фрагменты инфраструктуры можно вообще полностью отдать на откуп министерствам, ведомствам, другим организациям, но при этом обязательно задать интерфейсы, с помощью которых эти «чёрные ящики» будут связываться и общаться друг с другом.

**В заключение**

- ❑ **НАДО** проанализировать всё то, что было и **НАЙТИ недостатки**, почему не выполнено?
- ❑ В будущую программу создания инфраструктуры заложить не только средства, но и историю и опыт того же **ФАПСИ** - которое много сделало хорошего



## КОНСТРУКТИВНАЯ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

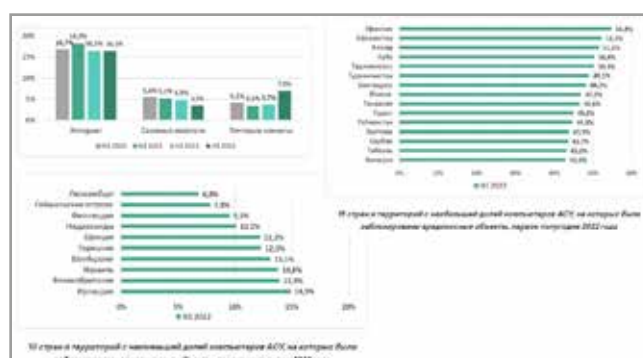
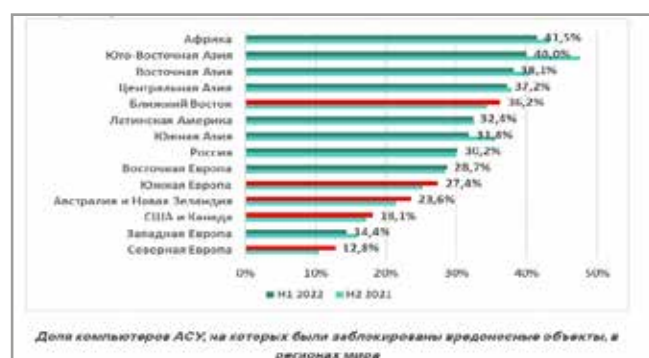
Моя презентация посвящена перспективному направлению Лаборатории Касперского, одной из технологий, которые позволят сделать мир безопаснее и более защищенным. Речь пойдет про Конструктивную информационную безопасность как основу Кибер-иммунитета. В западных документах это направление так же прописано как Secure by Design, безопасность, предусмотренная на этапе разработки и проектирования.

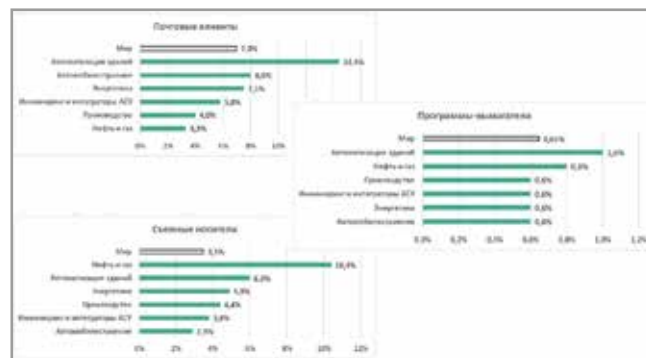
Но начать я хотел бы с некоторых цифр, по которым видно насколько агрессивна и опасна современная сеть интернет. Мы много лет фиксируем развитие вредоносного фона, от разовых вредоносных программ к массовым эпидемиям и сейчас к постоянному наличию в сети большого количества «зловредов». По данным Лаборатории Касперского, за 2 квартал 2022 года, мы отразили более 1 миллиарда 164 миллионов атак с различных интернет ресурсов и сервисов. Это цифры только с компьютеров которые защищают наши программы (KSN) и вы можете себе представить насколько же много реально угроз в сети интернет, насколько агрессивна интернет среда.



Если говорить про промышленные компьютеры, то ситуацию так же невозможно назвать здоровой. Почти на трети компьютеров были заблокированы вредоносные объекты. И хотя цифры похожи на температуру 36 градусов, (от 32,5 до 33,8) это показатель «плохого самочувствия» и уязвимости инфраструктуры.

При этом, конечно, есть страны, в которых показатели гораздо выше средних, вот, например страны Африки, Юго-Восточной Азии, Ближнего Востока. Красным помечены страны, в которых замечен рост зараже-





ний по сравнению с показателями прошлого года.

Далее детализируя данные, можно увидеть на этом слайде страны с наибольшим и наименьшим процентом атакованных компьютеров АСУ. Эфиопия, Афганистан, Алжир по этому показателю превысили 51%. Страны с наименьшим показателем Люксембург, Сейшельские острова и Финляндия не превысили 10%. Как видим, очень большой разброс по странам, в зависимости от современности инфраструктуры и возможности поддерживать безопасность и защищенность критически важной инфраструктуры.

По векторам атак — так же достаточно стабильный ряд — на первом месте угрозы связанные с сетью Интернет, далее Съёмные носители и Почтовые клиенты. Хотя видно, что в этом году Почтовые клиенты вышли на второе место.

Сами угрозы представлены преимущественно Вредоносными скриптами и фишинговыми страницами. Вирусы, в данном исследовании, были обнаружены в 2,4% случаев атак. Гораздо чаще троянцы — шпионы, бэкдоры, кейлогеры и даже вредоносные скрипты в документах MS Office и Pdf.

Так же не одинакова ситуация по отраслям. Программами вымогателями наиболее часто была атакована инфраструктура умного города / интернета вещей / автоматизации зданий. При этом инструментом атаки чаще были почтовые

клиенты. С помощью съёмных носителей, флешек, более частыми были попытки заражения нефтяной и газовой отрасли.

Мобильные угрозы не дают покоя пользователю системы Андроид, в этом рейтинге вы видите, что все перечисленные угрозы касаются именно этой операционной системы, что видно, по названиям вредоносных файлов. И значит шансы столкнуться с этим вредоносным ПО достаточно большие.

Хотя и для пользователей Mac OS так же есть свой список вредоносных программ.

Какой же выход, при столь большом количестве угроз?

Мы считаем, что наибольший эффект будет от механизмов встроенного иммунитета. Тот случай, когда вопросы информационной безопасности продумываются и интегрируются в производимое оборудование на этапе конструирования. От «наложенной» безопасности — к принципам «Secure by Design».

Эти требования необходимо учитывать сейчас, на этапе массовой цифровизации, обязательно синхронизируя активности разработчиков программ и аппаратной части, на уровне устройств и ЭКБ. Используя принципы вложенности уровней доверия.

Таким образом возможно достичь высокий уровень защищенности компьютерных систем, появится возможность противостоять неизвестным угрозам. Во время пандемии, мы все увидели, насколько важно иметь лекар-





Выполнение требований доверия и информационной безопасности может обеспечить продукт, получивший название **Secure-by-Design** (Конструктивная Информационная Безопасность, или Информационная безопасность, предусмотренная конструктивно).

При таком подходе системы и устройства приобретают свойства безопасности ещё на этапе проектирования, в ходе которого учитываются аспекты, ранее относимые, в основном, к разработке специализированных СЗИ: формирование требований по информационной безопасности, модели угроз и нарушений и т.д.

Таким образом, основным средством защиты является сама архитектура устройства, программного обеспечения (ПО) или системы, обеспечивающая их надежное функционирование в агрессивной информационной среде.

Создать такое окружение, которое просто не позволит программам исполнять недекларируемые возможности (код) и предотвратит эксплуатацию уязвимостей.



**—Стандарты разработки информационных систем ТК362/РГ-8**

Лаборатория Касперского — Участие в создании современных стандартов (ГОСТов) разработки информационных систем, устойчивых к деструктивным воздействиям

Методология разработки доверенных приложений secure-by-design  
Система оценки зрелости безопасности  
Принцип многочисленных независимых уровней безопасности (MILS)  
Доверенные операционные системы. Термины, определения, классификация  
IoT. Системы с разделением доменов

ство, но еще важнее, наверно, иметь иммунитет. Это справедливо для биологических вирусов и похоже аналогично для кибер-угроз.

Подводя итог, хотел бы еще раз выделить наши рекомендации:

1. Необходимо обратить внимание и вывести на уровень регламентирующих документов, что при разработке ПО и компьютерного оборудования необходимо руководствоваться принципами Конструктивной, интегрированной информационной безопасности «Secure by Design» для формирования необходимого кибер-иммунитета. Мы проводим такие работы на уровне разработки стандартов в ТК 362 / РГ 8.
2. Необходима поддержка в части развития кадрового потенциала. Нужно больше людей науки, специалистов и разработчиков, которые ориентированы на использование принципов

«Конструктивной ИБ», руководствуясь ими при разработке ПО и оборудования. Это решается через целевую поддержку образования и включения в программу высшего образования соответствующих разделов и дисциплин.

3. В Лаборатории Касперского, мы активно используем возможности программы «Вознаграждение за найденные ошибки». Это касается исключительно наших программ и приносит свой положительный эффект, в этом мы смогли сами убедиться. Мы рекомендуем со стороны государства создать аналогичную программу выплаты легального вознаграждения за найденные ошибки в наиболее важных программах. Как в государственных системах, так и в наиболее часто используемых. Многим разработчикам это поможет улучшить их программы,

найти не декларируемые возможности или ошибки. Без последствий взлома и ущерба — выплатить вознаграждение за выявление таких уязвимостей.

Спасибо за внимание! Надеюсь, что совместно сделаем мир безопаснее!

**Программа Bug Bounty**

«Лаборатория Касперского» реализует свою программу bug bounty с 2016 года и делает это в партнерстве с известной платформой HackerOne. Компания также поддерживает проект Disclosure.io, который предоставляет собой безопасную площадку (Safe Harbor) для исследователей уязвимостей, освобожденных негативными юридическими последствиями своих раскрытий.

**Это может означать:**

- Независимые исследователи достигли высшей точки в своем возрасте.
- Любые исследователи за исключением сотрудников «Лаборатории Касперского» и связанных с ней организаций, а также членов их семей.

**Продукты, доступные для анализа:**

- Kaspersky Internet Security 2018
- Kaspersky Endpoint Security 11
- Kaspersky Endpoint Security for Linux
- Kaspersky Password Manager

**Вознаграждение:**

- \$150 000** за обнаружение и ответственное раскрытие наиболее серьезных уязвимостей (самостоятельный отчет с проверкой концепции).
- \$5 000 – \$20 000** за обнаружение уязвимостей, позволяющих реализовать менее серьезные варианты удаленного выполнения кода.
- \$1 000 – \$5 000** за обнаружение брешей в ПО, позволяющих повысить полномочия привилегий или предоставить и раскрытие конфиденциальных данных.

Политика и правила: [bug.bounty.kaspersky.com/en/faq/bug-bounty-program](http://bug.bounty.kaspersky.com/en/faq/bug-bounty-program)



**П.Л. Пилюгин**

*к.т.н., Центр проблем информационной безопасности ВМК МГУ  
им. М.В. Ломоносова*

## **О МНОГОУРОВНЕВОЙ ПОЛИТИКЕ БЕЗОПАСНОСТИ ПРИМЕНИТЕЛЬНО К КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЕ**

Почему формирование политики тема выступления?

Когда обсуждают вопросы информационной безопасности — используют разные уровни обобщения понятий и определений.

А применение их для современных систем и сетей требует большей точности и конкретности.

Предлагаю на основе политики безопасности рассмотреть взаимосвязь понятий современных сетей в соответствии с принятыми стандартами.

Почему политика многоуровневая?

Ниже приведены различные употребления этого понятия.

Обычно под многоуровневым представлением политики безопасности понимается:

(1) либо реализация уровней безопасности для управления доступом (мандатный доступ),

(2) либо разная детализация политики для различных уровней управления в организации,

(3) либо повышение защищённости при эшелонированной системе защиты,

(4) либо разные уровни защищённости.

В настоящем выступлении предлагается учитывать многоуровневую модель взаимодействия открытых систем ISO/OSI.

Корректен ли такой поход? Действительно, если рассмотреть разные задачи обеспечения информационной безопасности: защиту от НСД, от утечки (криптографические протоколы и VPN), защиту сетей (VLAN, межсетевой экран) и многие другие. Везде для политик и отдельных решений безопасности понятийный аппарат локализован в пределах одного уровня эталонной модели взаимодействия открытых систем OSI.

Вместе с тем, осмысленные требования безопасности возникают только в сфере семантически значимых информационных агрегатов на прикладном уровне — документов, сообщений, сведений, измерений и т.п. (рисунок 1).



Могут ли быть отдельно сформулированы требования к безопасности сети?

Да, но при этом требования к защите сети (например, настройка межсетевого экрана) формулируются опять из предположения необходимости обеспечения безопасности информации прикладного уровня.

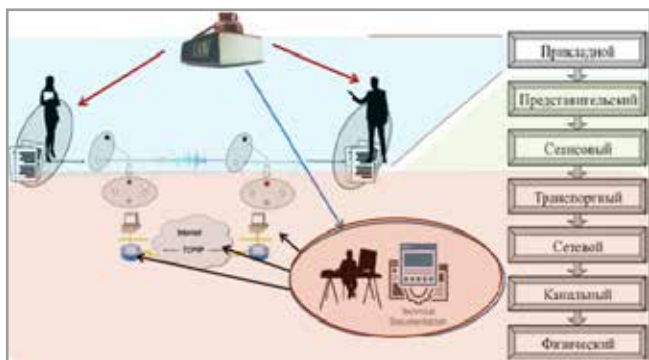
Давайте посмотрим какие понятия используют на каждом уровне. В первой колонке приведен список уровней эталонной модели OSI, во второй данные которыми манипулируют на данном уровне (рисунок 2).

Обратите внимание, что уровни 5–7 манипулируют строками символов — семантически значимой информацией.

Далее информация может разбиваться на части: дейтаграммы, пакеты (причем IP пакеты — это в сети интернет), кадры или фреймы и электрические сигналы. Для каждого вида информации существуют свои атрибуты и протоколы обработки.

Примеры таких протоколов приведены в последней колонке и это малая их часть. Например, только для 3-го сетевого уровня, где используются известный всем IP-адрес таких протоколов несколько сотен, все они описаны в технической документации.

Можно было бы для описания политик безопасности контроля информационных взаимодействий, ограничиться рассмотрением только прикладного уровня, если предположить, что все нижележащие уровни



**Рисунок 1. Уровень семантически-значимых документов.**

сетевой модели TCP/IP абсолютно безопасны с точки зрения НСД или хотя бы, что информация верхнего уровня изолирована от них (например, криптогоморфизм по схеме Гентри). Однако первое предположение невозможно, а второе пока практически не реализуемо. Поэтому необходимо последовательно формулировать политики безопасности по уровням сверху вниз и оценивать влияние безопасности нижележащих уровней на верхние.

Информационные объекты прикладного уровня — могут реализовывать информационные потоки между собой через один или несколько узлов транспортного уровня. А узлы транспортного уровня на, соответственно, узлах сетевого уровня и т.д. Напомню, что на каждом уровне используются свои информационные объекты и свои протоколы. На рисунке (рисунок 3) для определённости рассматриваются: уровни прикладной, транспортный и сетевой политиками. Модели TCP/IP принятой в сети интернет, что соответствует основным сетевым уровням модели OSI, о чем мы говорили раньше.

Субъекты, объекты и узлы транспортного (межсетевого) уровня можно представить как реализации (проекции) элементов уровня приложений на транспортный (сетевой) уровень сети.

Собственно на этом уровне информация (сообщения, документы и пр.) разбиваются на сегменты — дейтаграммы (пакеты) — эти информационные объекты не анализируются в зависимости от контента и не содержат атрибутов информации верхнего уровня, так как основная задача этого уровня надежная (и/или скоростная) транспортировка.

|                                                     |                                             |                                                          |                                         |                                                                      |
|-----------------------------------------------------|---------------------------------------------|----------------------------------------------------------|-----------------------------------------|----------------------------------------------------------------------|
| 7. Прикладной (application)                         |                                             | Доступ к сетевым службам                                 | URL                                     | HTTP(S), FTP(S), RPC, POP3                                           |
| 6. Представительский (представления) (presentation) | Данные (строки из байтов)                   | Представление (кодировка) и шифрование данных            |                                         | ASCII, EBCDIC                                                        |
| 5. Сетевой (session)                                |                                             | Управление сеансом связи                                 |                                         | RAP                                                                  |
| 4. Транспортный (transport)                         | Сегменты (segment) / Дейтаграммы (datagram) | Прямая связь между конечными пунктами и надежность       | Порт                                    | TCP, UDP, SCTP, PORTS                                                |
| 3. Сетевой (network)                                | Пакеты (packet)                             | Определение маршрута и логическая адресация              | IP-адрес                                | IPv4, IPv6, IPsec, AppleTalk                                         |
| 2. Канальный (data link)                            | Биты (bit) / Кадры (frame)                  | Физическая адресация                                     | MAC-адрес (физический адрес компьютера) | PPP, IEEE 802.22, Ethernet, DSL, ARP, L2TP, сетевая карта            |
| 1. Физический (physical)                            | Электронные сигналы, Биты (bit)             | Работа со средой передачи, сигналами и двоичными данными |                                         | USB, кабель ("витая пара"), коаксиальный, оптоволоконный, радиоканал |

**Рисунок 2. Информационные объекты разных уровней сети.**

Это позволяет формулировать для них политики исходя из политики уровня приложений и механизмы защиты (межсетевые экраны, правила маршрутизации, протоколы управления маршрутизацией, например, BGP и пр.) должны обеспечивать выполнение политики безопасности.

Хотя такая политика не учитывает содержание передаваемой информации, но может не разрешить информационный поток на транспортном или сетевом уровне еще до начала передачи семантически значимой информации.

С другой стороны существует возможность нарушений безопасности, в результате НСД к дейтаграммам на транспортном, к пакетам на межсетевом и к кадрам на сетевом уровнях стека.

Например, пакеты сетевого уровня и UDP дейтаграммы транспортного уровня, могут быть посланы от чужого имени — атака имперсонацией. А более надежный (хотя и более медленный) транспортный протокол TCP также может быть атакован атакой «человек по середине» в результате десинхронизации соединения.

Противостоять этим атакам (если такая угроза есть) должны механизмы защиты соответствующего уровня, контролируя соответствующие информационные объекты. На уровне приложений — сообщения, на транспортном — дейтаграммы, на межсетевом пакеты и на сетевом кадры.

Формулирование политик безопасности сверху-вниз, начиная с уровня приложений, особенно важно для критических информационных структур (КИИ).

Ведь для безопасности КИИ инцидентом является состояние, не допускающее нор-

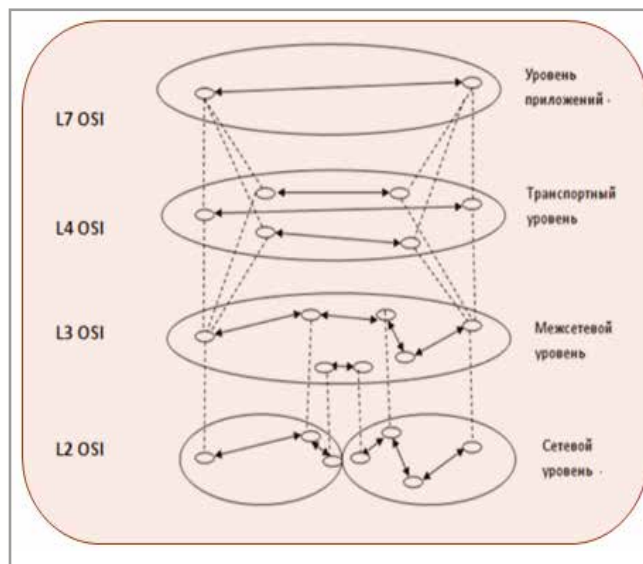
мальное функционирование самого критического объекта. Начальный критерий такого состояния находится за пределами собственно КИИ его признаки в КИИ отображаются, прежде всего, на прикладном уровне.

Вообще следует отметить, что для КИИ может быть изменена парадигма обеспечения информационной безопасности, так как конфиденциальность может не играть главенствующей роли, в отличие от задачи обеспечения доступности и целостности.

Кроме того, оценивание текущего состояния безопасности КИИ и детектирование компьютерных атак, например, с помощью сигнатур или аномалий трафика, выполняется на базе анализа признаков сетевого и транспортного уровня. Поэтому вопрос о том насколько атака соответствует инциденту в условиях КИИ становится далеко не тривиальным.

В качестве выводов можно сформулировать:

1. Если обеспечение безопасности использует многоуровневую политику и контролирует потоки информации между сущностями каждого уровня.
2. Политики безопасности должны формулироваться для каждого уровня стека протоколов эталонной модели ISO/OSI, дополнять друг друга и учитывать на каждом уровне требования политик более высокого уровня.



**Рисунок 3. Уровни сетевых взаимодействий.**

3. Такой подход применим и для трансграничной маршрутизации в глобальной сети.

Это позволяет,

во-первых, формулировать согласованные требования политики безопасности используя определения сущностей и понятия соответствующего уровня;

во-вторых, предотвращать возможные атаки с нижележащих уровней;

в-третьих, выявить возможные слабости системы защиты и

в-четвертых, обнаруживать новые потенциально опасные события безопасности на более ранней стадии и на более низких уровнях.



## Джон К. Мэллори

Массачусетский технологический университет, США

### ВОЕННАЯ КИБЕРСТАБИЛЬНОСТЬ И КРИТИЧЕСКАЯ ИНФОРМАЦИОННАЯ ИНФРАСТРУКТУРА

#### Международный контекст

- В международных отношениях (МОП) выделяют фазы конфликта:
  - Спор
    - Государства формулируют жалобы
  - Кризис
    - Неминуемый риск начала вооруженного конфликта
  - Военные действия
    - Государство участвует в вооруженном конфликте
  - Поселение
    - Государство разрешает споры и прекращает военные действия
- Межгосударственные отношения могут иметь 4 состояния
  - Мирное время
  - Серая зона
    - Враждебные действия ниже порога вооруженного конфликта
  - Кризис
    - Неминуемый риск начала вооруженного конфликта
  - Военное время
- Нормы биобезопасности и МД должны учитывать контекст
  - Риск эскалации выше по мере приближения к порогу вооруженного конфликта
  - Операции в "серой зоне" могут привести к кризису

Круглый стол по вопросам военной киберстабильности

13

Джон К. Мэллори



#### Обзор

- Введение
- Соображения по поводу мирового порядка
- Мировая система
- Цели
- Правоприменение
- Кибер-нормы
- Меры по укреплению доверия
- Выводы

Круглый стол по вопросам военной киберстабильности

2

Джон К. Мэллори

#### Введение

- Кризис в Украине показывает необходимость кибернорм военного времени и мер по укреплению доверия
  - Участие крупных держав в качестве первичных и вторичных сторон
- До настоящего времени кибердипломатия делала упор на добровольные нормы мирного времени
  - Стабилизирующая функция кибернетических норм и МД часто остается не проанализированной
  - Механизмы правоприменения, как правило, расплывчаты
- В данной беседе предлагаются некоторые кибернормы военного времени и меры укрепления доверия (МД)
  - Обеспечение соблюдения зависит от согласованных собственных интересов государств
  - Анализ их функций связывает их с желаемыми результатами стабильности, такими как:
    - Стратегическая стабильность
    - Сдерживание конфликтов
- Международному сообществу рекомендуется продолжить их изучение, доработку и распространение для укрепления стабильности во время войн.

Круглый стол по вопросам военной киберстабильности

3

Джон К. Мэллори

#### Соображения по поводу мирового порядка

- Прокси-война между Россией и НАТО после вторжения России в Украину
  - Определение: "Агрессивная война" по международному праву (МП)
    - Война, ведущаяся против суверенного государства без оправдания: самообороны в соответствии с Уставом ООН
    - Обычно проводится для завоевания и покорения территорий
  - Ко-военственность обычно требует принятия прямых военных действий в конфликте
    - Военная помощь, поставки и т.д. не являются прямыми действиями, и государства, оказывающие такую поддержку, не теряют нейтрального статуса
  - Однако военная помощь в агрессивных войнах является асимметричной по отношению к нейтралитету
    - Помощь жертве не делает государство воюющей стороной -> НАТО не является воюющей стороной
    - Предоставление агрессору делает государство воюющей стороной -> Китай не предоставляет военную помощь
  - Когнитивная борьба в глобальной информационной сфере благоприятствует Украине, а не России
    - Против России: Нарушение Устава ООН путем развязывания войны
    - Против России: Гуманитарная катастрофа в Украине (например, перемещение населения, военные преступления)
      - Для Украины: Борьба за свободу и демократию
      - За Украину: Антиколониальная борьба
- Экономические санкции стран НАТО (и других) против России привели к экономическим потерям после спора в результате пандемии Ковид-19
  - Россия переходит от экономической интеграции с Европой (и ОЭСР) к интеграции с Китаем (и другими регионами, такими как Индия, Африка)
    - Большое устойчивое воздействие на Россию, небольшое переходящее воздействие на мировую экономику
  - Энергетический кризис в Европе, высокие цены во всем мире
  - Широкомасштабная инфляция
  - Разворачивается синхронизированная глобальная экономическая рецессия
- Государства по-прежнему испытывают стресс из-за продолжающейся пандемии Ковид-19
  - Улучшение ситуации с разработкой немедикаментозных вмешательств, вакцин и терапевтических средств
  - Однако снижение экономических показателей в Китае из-за блокировок

#### Мировая система

- Международные отношения: Ухудшение отношений и углубление геополитического конфликта между ведущими державами усугубляется:
  - Операции по оказанию вредоносного влияния
  - Враждебные кибер-кампании
  - Недобросовестная торговая практика
  - Операции в "серой зоне"
- Война по доверенности: крупная держава напрямую втянута в войну, где другая основная сторона поддерживается альянсом другой крупной державы.
  - Опасный потенциал для разжигания прямого конфликта между государствами, обладающими ядерным оружием
  - Прецеденты: Советское вторжение в Афганистан, война во Вьетнаме, война в Корее
- Оценка: Стратегические балансы дестабилизированы:
  - Российские военные потери обычного потенциала
  - Активизация кибервзаимодействия в военное время
  - Восприятие враждебных намерений
  - Дилеммы отсутствия безопасности
- Заключение: Сдерживание (а лучше прекращение) войны в Украине важно для стратегической стабильности, снижения конфликтов, управления дилеммами отсутствия безопасности и снижения киберрисков.

Круглый стол по вопросам военной киберстабильности

5

Джон К. Мэллори

## Цели

- Сформулировать набор кибернорм и МД для военной киберстабильности в военное время
- Мотивировать новое внимание международной дипломатии к кибернетическим нормам и МД во время кризиса и войны
  - ГГООНГР и РГОС ООН сделали акцент на нормах мирного времени
  - Государства-«единомышленники» подчеркивают важность противостояния киберагрессии, будь то политическая, экономическая или криминальная агрессия
- **Преимущества:**
  - Поддержание стратегической стабильности
  - Снизить риск распространения конфликта за пределы локальной войны
  - Укрепление уверенности в поддержке деэскалации конфликта
  - Защитить гражданское население от вреда

Круглый стол по вопросам военной киберстабильности

6

Джон К. Маллери

## Исполнение

- **Нормы и МД в военное время должны быть самоусиливающимися**
  - Возможны только тогда, когда они отвечают интересам всех государств, независимо от степени их вовлеченности в конфликт.
- **Допущения:**
  - Крупные державы стремятся избежать прямого военного конфликта и войны с другими государствами, обладающими ядерным оружием.
  - Государства - рациональные акторы.
  - Кибератаки могут подняться до уровня "вооруженного нападения", если последствия будут серьезными
  - Государства понимают нормы военного времени и МД как помощь в снижении риска непреднамеренной войны крупных держав из-за неправильного восприятия, просчета или случайности.

Круглый стол по вопросам военной киберстабильности

7

Джон К. Маллери

## Кибер-нормы

- **NC<sup>4</sup> ISR:**
  - Не вмешиваться в ядерную C<sup>4</sup> ISR других государств.
- **Военные системы:**
  - Невоюющие стороны не должны снижать способность военных систем воюющих сторон функционировать посредством прямых кибератак.
- **Критические инфраструктуры:**
  - Воюющие стороны не должны нарушать способность критической инфраструктуры невоюющих сторон функционировать.
  - Невоюющие стороны не должны нарушать способность критической инфраструктуры воюющих сторон функционировать.
  - Государства не должны минимизировать критически важные инфраструктуры, чтобы эти имплантаты не были захвачены третьей стороной.
  - Защита международной критически важной инфраструктуры от кибер-атак с помощью передовых методов и своевременного анализа угроз, сообщений об уязвимостях и быстрого устранения последствий.
- **Обязанность оказывать помощь:**
  - Преследовать преступные или террористические элементы, занимающиеся несанкционированными вредоносными кибер-операциями или операциями влияния со своей территории, и работать с другими государственными субъектами для противодействия таким угрозам в других местах.
  - Сотрудничать с другими государствами для защиты от враждебных кибер-операций или операций влияния против функций общественного здравоохранения, проводимых как государствами, так и негосударственными субъектами.

Круглый стол по вопросам военной киберстабильности

8

Джон К. Маллери

## Меры по укреплению доверия

- **Коммуникация:** Поддерживать каналы связи и координации для понимания восприятия контрагентов, управления кризисами, защиты от кибератак третьей стороны и ведения переговоров по урегулированию конфликтов.
  - Национальные органы командования - управление кризисом, избегание просчетов
  - Mi-to-Mi - Деонфликтрование, избегание заблуждений
  - Правоохранительная деятельность - пресечение преступлений, предотвращение неправильного присвоения имущества
  - CERT-to-CERT - Предотвращение и реагирование на инциденты
  - Дипломатия - управление и урегулирование конфликтов
- **Умеренность:** Невуюющим сторонам следует умеренно вести кибершпионаж и воздерживаться от подрывных кибератак против воюющих сторон во время войны, поскольку цель может интерпретировать эти действия как подготовку поля боя или прямые атаки и может отреагировать на более высоком уровне эскалации, чем в мирное время.
  - Военные системы
- **Критически важные инфраструктуры**
  - **Сдерживание каталитических акторов:** Координация и совместные действия для выявления и преследования третьих сторон, стремящихся спровоцировать более широкий конфликт (например, террористов).
  - **Правоохранительные органы:** Координация и совместные действия по выявлению и преследованию киберпреступников, чья деятельность угрожает критически важным инфраструктурам (например, атаки на критически важную инфраструктуру с использованием программ-выкупов).
- **Кибербезопасность:** Сообщать и помогать устранять уязвимости в критических инфраструктурах, которые могут быть использованы каталитическими субъектами или преступниками.
  - Распространять исправления
  - Исключить исправления безопасности из санкций на программное обеспечение
- **Киберзащита:** Координировать и совместно действовать для поддержки киберзащиты международных критических инфраструктур.
  - Телекоммуникация, энергетика, финансы

Круглый стол по вопросам военной киберстабильности

9

Джон К. Маллери

## Выводы

- Кризис в Украине показывает необходимость кибернетических норм военного времени и мер по укреплению доверия
  - Участие крупных держав в качестве первичных и вторичных сторон
- В данной беседе предлагаются некоторые кибернормы военного времени и меры укрепления доверия (МД)
  - Обеспечение соблюдения зависит от согласованных собственных интересов государств
  - Анализ их функций связывает их с желаемыми результатами стабильности, такими как:
    - Стратегическая стабильность
    - Сдерживание конфликтов
- Он рекомендует международному сообществу продолжить их изучение, доработку и распространение для укрепления стабильности во время войн.

Круглый стол по вопросам военной киберстабильности

10

Джон К. Маллери



**КРУГЛЫЙ СТОЛ № 3**  
**ПРОТИВОДЕЙСТВИЕ ИСПОЛЬЗОВАНИЮ**  
**ИКТ ДЛЯ РАСПРОСТРАНЕНИЯ ИДЕОЛОГИИ**  
**НЕОНАЦИЗМА**

**Модератор:**

*Оганесян А.Г.*, член президиума НАМИБ, главный редактор журнала  
«Международная жизнь»

## С.В. Коротков

К.В.Н., генерал-майор, начальник  
аналитического отдела НАМИБ

### О НЕОНАЦИЗМЕ КАК УГРОЗЕ НАЦИОНАЛЬНОЙ И МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1. Начну с вопроса. Почему США и политические деятели Евросоюза поддерживают или в лучшем случае закрывают глаза на возрастание влияния неонацистских организаций на Украине?

Ответ очевидно можно найти в совпадении интересов США и их союзников в отношении привилегированного места «золотого миллиарда» к остальному 7 млрд. населению планеты, которое должно, по их мнению и желанию, продолжать в качестве «людей низшего сорта» обеспечивать их благополучное сытое существование.

Национальная исключительность, эта политическая фанаберия, проповедуемая США и в целом коллективным Западом, именно она создает чувство вседозволенности, столь характерное для нынешней политики Вашингтона и Брюсселя.

Когда же находятся оппоненты, исключительность позволяет не стесняться в средствах борьбы с ними.

Так, наиболее узнаваемые политические деятели Запада, демонстрируя «правоту по рождению», начинают огульно обвинять Китай в игнорировании прав человека, Россию в природной агрессивности, арабов и африканцев — в посягательстве на устои западного общества, изображаемом как конфликт цивилизаций.

Подобные подходы на государственном уровне постоянно и последовательно popularизируются СМИ западного мейнстрима, по каналам мировых агентств, наиболее влиятельных газет. Через актив социальных медиа внедряются в глобальную информационную сферу, индоктринируя миллионы журналистов и миллиарды читателей.

Проблема в том, что этот **поток информации и мнений авторитетных в своей среде западных ньюсмейкеров формирует по сути официальную поддержку ксенофобии, которую наиболее оголтелые и необразованные активисты неизбежно**



**трансформируют в неонацистскую идеологию** и политическую практику. Главное, что доминирование в глобальном информационном пространстве позволяет «манипулировать общественным сознанием» в заданном направлении.

Так **поток западной информации и нарратива, основанного на собственной исключительности, провоцирует тенденцию к распространению крайне националистических и неонацистских взглядов.** В результате фундаментальные принципы распространения массовой информации — точность, объективность, терпимость к чужим взглядам и убеждениям полностью девальвируются. Все это создает угрозу существования важнейшей глобальной системы — международных массовых коммуникаций, ее фрагментации, трансформации ее в сферу острых идейных конфликтов. А это прямой путь уже к конфликтам горячим.

Украина тому пример.

**В украинское общественное сознание за последние двадцать лет ментально внедрена новая, более агрессивная идеология воинствующего укрнеонацизма!**

Нетерпимость на национальной почве, кристаллизовавшись в виде неонацистских радикальных организаций, используется как орудие для влияния на внутривнутриполитические процессы в государствах-оппонентах (некоторые объявлены как противники) Запада. А на

Украине именно этот инструмент использовался для смены законного режима и поддержания власти самозванцев.

Ныне же взрощенная таким образом **анти-российская ксенофобия** на Украине, трансформировавшись в неонацистские движения, становится главным мотивом политики режима Зеленского. Политики, которая сделала братскую страну **инструментом сначала сдерживания российского влияния, а потом военно-стратегического давления на Россию, порождая явную угрозу ее национальной, в том числе и информационной, безопасности.**

По сферам применения структурно его можно разделить на государственный, военный и бытовой.

**На государственном уровне** осуществляется поддержка и продвижение официальной государственной доктрины о превосходстве украинцев над другими народами с мерами по дискриминации Русской православной церкви. Особое внимание уделяется контролю над всеми средствами массовой информации и в целом за всеми информационными ресурсами и киберпространством.

Стержнем неонацистской идеологии является **тотальная милитаризация** всех сфер общественной жизни и народного хозяйства. Основной украинского силового блока и главной ударной силой против России являются многочисленные радикальные ультраправые организации, в том числе интегрированные с ВСУ. Их лозунгом является **«Культ силы не может соседствовать с культом жалости»**. А религией неонацистских организаций определен языческий культ. **Такой подход обеспечивает практическое внедрение идеологии расчеловечивания** с проявлением ксенофобии и расизма в крайних формах.

**Бытовой нацизм** играет исключительную роль в воспитании новой «укрнеонацистской молодежи», что реализуется практически с детского сада и школы.

Ультраправые организации на Украине занимают центральное место в государственной информационной политике, имея соответствующие информационные ресурсы, которые финансируются олигархическими структурами и рядом ведущих политиков, многочисленными иностранными фондами.

Запад последовательно проводит медийную поддержку этого курса, основанного на тезисе о собственной исключительности и генетической русофобии.

Примеры множатся.

Крупнейшее немецкое издание (Bild) безо всякой рефлексии или, напротив, совершенно осознанно публикует «обращение к россиянам», выполненное в духе нацистских листовок Восточного фронта («Русский солдат, политрук лжет тебе, сдавайся, в плену тебя будут кормить»). Процитируем одно лишь окончание материала: «Граждане России не заслуживают санкций, нищеты и страданий. Вы должны иметь возможность жить в своей стране счастливо, как и украинцы в своей, так и люди на Западе. Будьте храбрыми! Покажите своему президенту, что вы думаете о его войне. Мы приветствуем вас из Германии». А миллиардер Джордж Сорос сравнил оборону Киева режимом Зеленского с обороной немцами Будапешта от наступающей Красной армии в 1944-м, причем сравнил в положительном ключе.

Европейские политики не стесняются откровенно человеконенавистнических высказываний в адрес России. Так, польский премьер Моравецкий назвал Русский Мир «раковой опухолью», «смертельной угрозой» и «чуждовидной идеологией», подлежащей «полному искоренению».

**Западные СМИ поддерживают украинский неонацизм и одновременно стремятся заретушировать или признать «несуществующими» наиболее откровенные его проявления.**

Международная правозащитная организация Amnesty International в начале августа опубликовала доклад, в котором рассказала о военных преступлениях украинской армии. Зеленский немедленно обвинил правозащитников в попытке «амнистировать» Россию и «переложить ответственность на жертву».

Сначала организация выразила «глубокое сожаление о страданиях и гневе, которые вызвал доклад о боевых методах украинских военных», но уже через неделю Amnesty International заявила, что документ перепроверят некие «независимые эксперты». В немецком бюро Amnesty International сообщили, что результаты доклада «не были переданы с той

деликатностью и точностью», которую ждали от организации (на Западе и на Украине).

Более того, западные СМИ, используя свое доминирование в информпространстве, стремятся списать варварство украинских неонацистов на Россию. Например, в эфире телекомпании Das Erste в июне утверждали, что чудовищный удар по донецкому рынку нанесли российские военные.

**Российская дипломатия пытается обратить внимание на проблему тесной связи Запада и украинского неонацизма.** Постпред РФ при ООН Василий Небензя 9 августа на брифинге в Совбезе ООН заявил: «Украина встала в один ряд с Сирией, Ираком, Ливией, Афганистаном. ...И если на Ближнем Востоке, в Северной Африке и Афганистане США и сателлиты подпитывали оппозиционные силы, которые быстро либо сами превратились в террористов, либо стали поддерживать с террористами тесные связи, то на Украине идет прямая поддержка и тренировка националистических и неонацистских образований».

Запад, однако, игнорирует такого рода заявления, ибо и сам все прекрасно знает. Верх же цинизма это попытки приклеить ярлык «фашистского государства» на саму Россию, что недавно сделал глава евродипломатии Ж.Боррель, слова которого затем попытались неуклюже выдать за «неправильный перевод». Как говорится, с больной головы на здоровую.

Можно констатировать что те кто управляет на Западе глобальными массово-коммуникационными процессами не осознают какие угрозы несет подобная глобальная ксенофобия Вашингтона, а также «подкаблучного» Брюсселя по причине коллективно наложенного вето на альтернативное здравое мнение. Остается надежда на присущий народам инстинкт самосохранения своего существования. Пробуждение и активизация общественного самосознания к осознанным действиям может быть обеспечена комплексом мер, прежде всего в ИКТ-среде, на международной арене в увязке с достижением заявленных целей СВО на Украине, и в первую очередь по денафикации сферы культуры, прессы и образования.

Достижение победы в современных условиях решается в значительной степени не только в ходе боевых действий на суше, воз-

духе и море. Прокси война предполагает завоевание информационного превосходства в киберпространстве — главном и решающем поле битвы или нформпротивоборстве. От успеха действий в информационном пространстве непосредственно зависит достижение целей СВО на Украине, особенно в самый сложный период постконфликтного урегулирования с завершением военной фазы.

## **2. Некоторые выводы на основе проведенного анализа.**

**Стало** очевидным, что неонацизм стал инструментом внешней политики Запада в интересах сохранения благополучия «золотого миллиарда». Его стремительная эволюция произошла за период после распада СССР. Русофобия — характерная черта современного нацизма.

В настоящее время со стороны США и его союзников расширяется поддержка агрессивного национализма. Для этой цели создана и задействована обширная сеть западных НКО, НПО, поддерживающие неонацизм, и гигантский сегмент интернет-ресурсов.

Важнейшей целью России и ее стратегических партнеров является разрушение единства среди западных государств в отношении проведения политики по поддержке идеологии неонацизма.

Сохранение России как мирового центра многополярного мира зависит от ее внутривнутриполитической и социальной стабильности.

**О приоритетных мерах содействия реализации внешней политики Российской Федерации в интересах формирования международной системы применения норм ответственного поведения государств в ИКТ-среде в целях противодействия распространению идеологии неонацизма.**

Содействие реализации мер в интересах сотрудничества по вопросам формирования системы применения норм ответственного поведения государств в ИКТ-среде в целях противодействия распространению идеологии неонацизма **целесообразно обеспечить организацией на соответствующем уровне информационного обеспечения**, необходимого для осуществления деятельности по продвижению государственной политики в области обеспечения МИБ, адекватной оценки ее состояния на международной арене, формирования, выдачи и распространения досто-

верной информации, предупреждения нежелательных и/или негативных (опасных) ситуаций в ИКТ-сфере, связанной с деструктивной деятельностью неонацистских организаций.

Практика показывает, что такое **информационное обеспечение организуется путем информационного сопровождения и информационной поддержки**, которые являются наиболее эффективными традиционными инструментами доведения и внедрения целенаправленной информации до международных организаций и общественности.

**Информационное сопровождение** является необходимым процессом информационного обеспечения, нацеленный на пользователей информации, занятых в ИКТ-сфере. При этом основными формами при осуществлении этой деятельности являются: целевые пресс-конференции, пресс-туры, пресс-релизы. То есть мероприятия, которые приобретают все большее значение в ходе СВО на Украине.

Особое место отводится специальным мероприятиям, к которым относятся: проведение информационных акций в социальных сетях; организация тематических видеоконференций и вебинаров; привлечение и мотивация журналистов к созданию авторских целевых материалов; подготовка и публикация статей с экспертными оценками преступной деятельности неонацистских организаций в ИКТ-среде; подготовка дайджестов новостей на сайтах НКО (НПО) и партнерских организаций с e-mail рассылкой; использование социальных сетей, блогов и онлайн-платформ в интересах противодействия распространению идеологии неонацизма.

**Информационная поддержка** представляет собой в рамках информационного обеспечения вид публичной деятельности, связанный с использованием антинеонацистской информации.

**Эффективность мероприятий в значительной мере зависит от информационных поводов международного значения**, которые являются мощным фактором нанесения поражения неонацистской идеологии как на Украине, так и в мире в целом.

Достижением внешней политики Российской Федерации является многогранная дея-

тельность, в результате которой в очередной раз в декабре 2021 г. Генеральная ассамблея ООН большинством голосов приняла российский проект резолюции, осуждающий героизацию нацизма и расизма. Против проголосовали только США и Украина. Резолюция носит название «Борьба с героизацией нацизма, неонацизмом и другими видами практики, которые способствуют эскалации современных форм расизма, расовой дискриминации, ксенофобии и связанной с ними нетерпимости», ее поддержали 130 государств. Воздержались от голосования 49 стран, в их числе Франция, Германия, Нидерланды и Польша<sup>1</sup>.

Вот почему так необходимо проведение международного трибунала на территории Донбасса в отношении украинских неонацистов и широкое доведение вынесенных судебных решений за военные преступления до мирового сообщества.

**Информационное обеспечение борьбы с неонацизмом должно быть организовано и проводиться в рамках решения следующих важнейших задач:**

- формирование международно-правового режима предотвращения конфликтов в глобальном информационном пространстве;
- обеспечение суверенитета государств в мирной, открытой, безопасной, стабильной и доступной ИКТ-среде;
- защита национальных ценностей в глобальном информационном пространстве;
- обеспечение безопасности объектов критической информационной инфраструктуры;
- развитие регионального сотрудничества в системе международной информационной безопасности.

**При этом целесообразно определить реализацию следующих сопутствующих задач:**

- противодействие распространению идеологии неонацизма, экстремизма и терроризма, а также использованию глобальной ИКТ-среды для вмешательства во внутренние дела суверенных государств;
- продвижение российских инициатив по подготовке проекта концепции Кон-

<sup>1</sup> <https://www.rbc.ru/rbcfreenews/61bbbc249a794742c3416537>



венции ООН об обеспечении международной информационной безопасности и по подписанию проекта Конвенции ООН о сотрудничестве в области противодействия информационной преступности (A/C.3/72/12).

**Субъектами для сотрудничества**, в отношении которых предполагается проведение мероприятий содействия, необходимо рассматривать все возможные потенциальные международные площадки. Приоритетными являются ШОС и БРИКС.

К другим значимым площадкам для реализации мероприятий в информационном пространстве следует отнести Африканский союз, Лигу Арабских государств, ССАГПЗ, ОИГ, Ассоциацию государств Юго-Восточной Азии.

Появились новые перспективные возможности для повышения эффективности и результативности противодействия распространению идеологии неонацизма за счет планирования и реализации совместных действий по защите общего информационного пространства в рамках Союзного государства России и Белоруссии, ОДКБ.

**На международном уровне следует обсудить целесообразность создания эффективного независимого процедурного механизма для справедливого судебного наказания за киберпреступления**, связанные с использованием информационно-коммуникационных технологий в интересах неонацистских организаций.

Таким образом, насущной проблемой становится взятие мировым сообществом на себя обязательств выработки (адаптации) и соблюдения норм ответственного поведения государственных акторов в информационном пространстве, основанных на принципах Устава ООН и других норм международного права: соблюдение суверенного равенства; разре-

шения международных споров и противоречий мирными средствами без того, чтобы не подвергать угрозам международный мир, безопасность и справедливость; отказ от угрозы силой или ее применения в международных отношениях.

Важным аспектом при реализации комплексной задачи противодействия идеологии нацизма следует учесть продолжение практики внешнеполитической деятельности по борьбе с героизацией нацизма. Примером является анализ и учет такой практики в зарубежных странах.

В докладе МИДа России 2019 года «О ситуации с героизацией нацизма, распространении неонацизма и других видов практики, которые способствуют эскалации современных форм расизма, расовой дискриминации, ксенофобии и связанной с ними нетерпимости» на основе данных из международных национальных источников обобщена фактологическая информация о проявлениях в любых формах героизации нацистского движения, неонацизма, расизма, расовой дискриминации, ксенофобии и связанной с ними нетерпимости в фокусных странах, а также примеры наилучшей практики по борьбе с этими явлениями на законодательном и практическом уровнях.

Сохранение России как мирового центра многополярного мира зависит от ее внутриполитической и социальной стабильности. В этом плане важно **ускорить принятие в этом году** Основ государственной политики по сохранению и укреплению традиционных российских духовно-нравственных ценностей, а также осуществление корректировки Основ государственной культурной политики в соответствии с действующей Стратегией национальной безопасности и внесенными изменениями в Конституцию Российской Федерации.

**КРУГЛЫЙ СТОЛ № 4**  
**ФОРМИРОВАНИЕ МЕЖДУНАРОДНОГО**  
**ПРАВОВОГО РЕЖИМА ПРЕДОТВРАЩЕНИЯ**  
**КОНФЛИКТОВ И ПРОТИВОДЕЙСТВИЯ**  
**ПРЕСТУПНОСТИ В ИКТ-СРЕДЕ**

**Модератор:**

*Мирошников Б.Н., к.ю.н., член-корреспондент Российской инженерной академии,  
генерал-полковник, Вице-президент НАМИБ, вице-президент ГК «Цитадель»*

## **ФОРМИРОВАНИЕ МЕЖДУНАРОДНО-ПРАВОВОГО РЕЖИМА ПРОТИВОДЕЙСТВИЯ ПРЕСТУПНОСТИ В ИКТ-СРЕДЕ**

В условиях отсутствия базовых параметров и механизмов обеспечения международной информационной безопасности (МИБ) мировое сообщество остается уязвимым для всего комплекса угроз в этой сфере. Под вопросом — перспективы глобального процесса цифровизации в целом, эффективность и динамика которого зависит от обеспечения безопасности.

Преступность в информационном пространстве носит поистине глобальный характер, значительно повышается и усложняется её уровень. «Киберпреступники» способны нанести серьезный урон экономической деятельности государств, благополучию миллионов людей. При этом речь может идти о потерях, сопоставимых с эффектом от военных действий. В этом смысле киберпреступность уже можно рассматривать в качестве одного из ключевых элементов стратегической стабильности.

На фоне проведения специальной военной операции по защите ДНР и ЛНР наметилась тенденция подстрекательства недружественными государствами к противоправным действиям, и размещение этими странами готового вредоносного ПО в открытом доступе сети Интернет.

Именно Вашингтон по просьбе украинского режима занимается рекрутированием т.н. «патриотически» настроенных кибернаемников и подготовкой киберкриминальных хакерских кадров. Это укладывается в западную концепцию наращивания потенциала или так называемого технического содействия. Получается, что рекрутированные международные хакеры обслуживают политические интересы нескольких отдельных стран, прикрываясь как щитом другими. Кроме того, в бизнес-модель ведущих американских IT гигантов заложена система сбора данных её пользователей.

Одним из наиболее ярких примеров такой деятельности является уже озвученная



Сбербанком деятельность т.н. колл-центров по телефонному мошенничеству финансовых средств граждан с территории Украины (Бердянска) в противоправной схеме которого задействованы целый ряд стран — Великобритания, США, ФРГ, Нидерланды, Польша и Эстония. К слову, Российская Федерация проинформировала Интерпол о данных криминальных схемах.

Таким образом киберпреступность используется в качестве маскировки государствами своего политического курса на проведения противоправной деятельности. Возникает вопрос, куда же денется эта подготовленная США и их союзниками армия хакеров, после окончания специальной военной операции по денацификации Украины? С высокой долей вероятности можно предположить, что все оставшиеся потом без работы хакеры могут пополнить ряды профессиональных киберпреступников.

Как это не парадоксально, в этих условиях по причине трансграничного характера преступлений, совершенных в сфере ИКТ, еще более актуальной и востребованной для государств стала работа Специального межправительственного комитета ООН по разработке всеобъемлющей международной конвенции по противодействию использованию информационно-коммуникационных технологий в преступных целях. Данный переговорный механизм был учрежден по инициативе России и при

соавторстве 46 государств резолюцией Генеральной Ассамблеи ООН 74/247 и нацелен на создание мировым сообществом первого в истории юридически обязательного инструмента по борьбе с киберкриминалом.

Главным итогом 2022 года уже можно считать полноценный запуск практической работы над универсальной конвенцией, который долго откладывался по различным причинам. Излишняя политизация и попытки навязать односторонние правила уступили место многосторонней и конструктивной дипломатии с тесным привлечением ведущих экспертов со всего мира. Заработал предложенный Россией открытый, инклюзивный и транспарентный процесс переговоров по комплексной борьбе с киберкриминалом под эгидой ООН. Спецкомитет задает новые ориентиры, объединив самый передовой опыт в области противодействия информационной преступности.

За прошедший год Спецкомитет под председательством Ф. Мебарки (Алжир) провел 3 субстантивные сессии в марте (Нью-Йорк), июне (Вена) и сентябре (Нью-Йорк).

В ходе сессий, приняли участие профильные эксперты из более чем 160 государств и 200 неправительственных организаций, представляющих политические и правоохранные структуры, а также академическое, научное и бизнес-сообщество.

В соответствии с одобренной программой мероприятий Спецкомитет последовательно рассмотрел вопросы целей и охвата будущей универсальной Конвенции. Консенсусом утверждена её структура, состоящая из преамбулы и 7 глав.

В ходе сессий государства-участники обменялись мнениями относительно наполнения глав будущей конвенции, касающихся «криминализации», «общих положений», «процессуальных мер и правоохранительной деятельности», «международного сотрудничества», «технической помощи», «мер предупреждения», «механизма осуществления конвенции», а также «заключительных положений» и «преамбулы».

Состоялся насыщенный обмен мнениями по ключевым элементам проекта. Несомненно, согласны с многочисленными выступлени-

ями на Спецкомитете в том плане, что Проект конвенции должен соблюдать баланс в вопросах защиты государственного суверенитета, уважения прав человека и криминализационных аспектов. При этом в будущем документе необходимо учитывать активное применение современных технологий.

Наибольшую актуальность по мнению государств-участников приобрели вопросы юрисдикции, разработки универсального понятийного аппарата, усиления международного сотрудничества при раскрытии трансграничных преступлений, обмена электронными доказательствами и защиты персональных данных.

Позиции государств-участников во многом схожи в вопросах взаимной правовой помощи, экстрадиции, конфискации активов, передачи осужденных лиц, ответственности юридических лиц, необходимости обеспечения по запросу государств технического содействия и подготовки кадров.

Есть и расхождения. Прежде всего, в вопросах сферы охвата будущей конвенции, целесообразности включения положений по защите критической информационной инфраструктуры, террористической и экстремистской деятельности. Западные страны не оставляют попыток включения в проект положений аналогичных ст.32b) Будапештской конвенции по трансграничному доступу к данным.

В качестве национального вклада Российская Федерация внесла собственный проект универсальной конвенции по противодействию информационной преступности, соавторами которого стали Белоруссия, Китай, Таджикистан, Никарагуа и Бурунди. Большинство его элементов нашло широкое отражение в выступлениях различных делегаций и вошло в документы сессий Спецкомитета.

Следующий важный этап — выработка Председателем т.н. нулевого проекта конвенции работа над которым начнется в ходе следующей сессии (Вена, январь 2023 г.). Итоговый текст конвенции Спецкомитет должен представить Генассамблее ООН в ходе ее 78-й сессии (в 2024 году).



## Ю.А. Ясносокирский

Начальник отдела ООН и глобальных форматов ДМИБ МИД России

### АТРИБУЦИЯ КОМПЬЮТЕРНЫХ АТАК: ДУБИНА ИЛИ СРЕДСТВО МИРОВОЙ ПОЛИТИКИ

Хотел бы начать свое выступление, имеющее столь интригующее название с двух эпизодов.

Первый, 31 августа с.г. кавалькада машин «Яндекс такси» гурьбой направилась к метро «Кутузовская», собравшись по одному и тому же адресу. В результате образовалась огромная пробка.

Другой, за полтора месяца до вышеприведенных событий в Албании в одночасье все сайты органов государственной власти вышли из строя. В результате были прерваны албано-иранские дипломатические отношения. Как известно, следующим шагом может быть война.

Что объединяет эти два разноплановых и совсем непохожих по своим последствиям события. Это необходимость тщательной и выверенной атрибуции.

#### 1. Что собой представляет атрибуция?

В контексте использования информационно-коммуникационных технологий атрибуция является совокупностью технических и организационных мероприятий с целью определения источника вредоносных и противоправных деяний в цифровой среде и возложения за них ответственности на конкретные государства.

Существуют несколько ее видов: техническая, политическая и юридическая.

**Техническая атрибуция** предполагает использование компьютерной криминалистики для оценки технических улик и доказательств (сетевые журналы, следы вредоносного ПО) на системах, затронутых атакой. Они сравниваются с инструментами и методами прошлых инцидентов, сопоставляются друг с другом и ложатся в основу выдвигаемой гипотезы относительно источника атаки.

В настоящий момент формирование объективного деполитизированного международного механизма атрибуции компьютерных атак представляется трудноосуществимым без проведения технологической адаптации



глобальных сетей связи в целях обеспечения равных условий доступа к нему для всех государств, а также транспарентности общего цифрового пространства.

В рамках процессов **политической атрибуции** атакуемое государство ставит задачу определить непосредственного виновника атаки, его политическую принадлежность и мотивацию. Выносимые заключения, как правило, опираются на стратегию национальной безопасности той или иной страны, а также текущий геополитический контекст. Политическая атрибуция может осуществляться как на двусторонней основе по дипломатическим каналам, так и публично для разоблачения «агрессора».

К примеру, в целях сохранения своего глобального технологического лидерства и обеспечения контроля над мировым информационным пространством западные страны во главе с США продолжают наращивать усилия по продвижению выгодных им подходов к проблематике атрибуции компьютерных атак. В частности, стремятся закрепить и популяризировать практику проведения атрибуции в отношении иностранных государств на базе национального законодательства, так называемых «достоверных разведданных» и без обнародования конкретных технических доказательств. Яркий пример — приведенный мною выше пример разрыва Албанией дипломатических отношений с Ираном на основа-



нии якобы неопровержимых доказательств, совершенных на албанские государственные сетевые ресурсы атак со стороны аффилированных с иранскими властями хакерских группировок. Характерно, что в решительную поддержку Тираны выступил Вашингтон, незамедлительно подключивший к разоблачению иранской «агрессии» ФБР и компанию «Майкрософт». Последней весьма оперативно был представлен соответствующий доклад.

Попытки легитимизации произвольного установления ответственности государств за «противоправные» деяния в ИКТ-сфере и наложение соответствующих рестрикций предпринимаются западниками, в том числе на площадке ООН. Не имея поддержки большинства государств для формирования атрибутивного механизма в структуре организации, США ведут дело к созданию подконтрольного им вне ооновского многостороннего механизма, который позволит определять, назначать и наказывать «кибервиновных» по своему усмотрению.

При поддержке узких групп единомышленников западниками запускаются региональные и многосторонние инициативы, направленные на проведение коллективной публичной атрибуции. В качестве примеров — ИКТ-сегмент альянса «Пять глаз» (Австралия, Канада, Новая Зеландия, Великобритания, США); продвигаемая Вашингтоном «инициатива по киберсдерживанию».

В этих целях также активно задействуется потенциал НАТО и ОБСЕ, где под предлогом осуществления комплекса мер укрепления доверия реализуются обильно финансируемые внебюджетные проекты, направленные на навязывание собственных стандартов реагирования на кибернападения, обмен данными о способах защиты критической информационной инфраструктуры, повышение профиля НПО в определении источников информационной агрессии.

По сути, в перспективе атрибуция, совершенная по таким лекалам, может быть использована не только для дискредитации в глазах мирового сообщества конкретных «неудобных» государств, но и для поиска основания для проведения агрессивных действий, вплоть до вооруженного противостояния — к примеру, на основании субъективной трактовки статьи 51 Устава ООН о праве на индивидуальную

и коллективную самооборону или под предлогом упреждающей защиты объектов критической инфраструктуры.

## 2. Что же делать?

На межгосударственном уровне проблема атрибуции может быть решена путем выведения данного вопроса из политического поля в юридическое, т.е. речь идет об **юридической атрибуции**.

Существует два варианта (разумеется, данное деление носит условный характер):

- во-первых, можно задействовать уголовно-процессуальный механизм, когда факт кибератаки рассматривается через призму состава преступления. В случае если следы преступников ведут в иностранное государство, должны быть задействованы апробированные **механизмы взаимной правовой помощи, а также обмен необходимой технической информацией об индикаторах вредоносной активности по каналам групп реагирования на компьютерные инциденты**. Сложности в этом плане связаны с добровольным характером взаимодействия упомянутых групп, намеренным препятствованием других стран раскрытию чувствительной информации для атрибуции компьютерных атак, правовыми ограничениями и т.д.
- во-вторых, к упомянутому выше механизму можно было бы добавить международно-правовой механизм, который базируется на системе мирного разрешения споров, предусмотренный п. 1 ст. 33 Устава ООН, когда стороны должны решать споры путем переговоров, обследования, разбирательства и обращения к региональным организациям.

В перспективе можно было бы перейти к разработке и принятию под эгидой ООН глобального юридического документа, регламентирующего процедуру реализации атрибуции. Это позволило бы превратить атрибуцию из пропагандистской, ничем не основанной «дубины» обвинений в подлинно международно-правовое средство урегулирования компьютерных инцидентов, что несомненно будет способствовать укреплению международного мира и безопасности, а также пресечению противоправных деяний и преступлений в сфере ИКТ.

## Л.А. Осадчая

*Представитель Национального  
центрального бюро Интерпола,  
МВД России*

### ОБ УЧАСТИИ НЦБ ИНТЕРПОЛА МВД РОССИИ В БОРЬБЕ С МЕЖДУНАРОДНОЙ КИБЕРПРЕСТУПНОСТЬЮ

Для начала позволю себе напомнить, что Интерпол — это крупнейшая в мире международная полицейская организация, в состав которой в настоящее время входят 195 государств. Основной задачей Организации является развитие и координация сотрудничества национальных правоохранительных органов в борьбе с общеуголовной преступностью.

Наша страна вступила в Интерпол в 1990 г. За годы, прошедшие с тех пор, российское Бюро Интерпола стало неотъемлемой частью этой большой единой системы. Накоплен огромный опыт в координации усилий правоохранительных органов по борьбе с разными видами преступлений.

В последние годы в связи с появлением и стремительным развитием киберпреступности в российском национальном бюро создан новый специализированный участок. Его основные усилия направлены на информационное сопровождение уголовных дел и дел оперативного учета в отношении преступлений, совершенных в сфере компьютерных технологий и телекоммуникационной среде, находящихся в производстве органов внутренних дел и иных ведомств Российской Федерации.

Второй основной задачей нового участка является исполнение запросов правоохранительных органов иностранных государств-членов Интерпола.

Основная доля информационного обмена с правоохранительными органами стран-членов Интерпола приходится на проверку абонентов телефонных номеров и пользователей IP-адресов по таким видам преступлений, как мошенничество, вымогательство, хищение денежных средств с банковских счетов, распространение противоправного контента, в том числе, «Детской порнографии», направление ложных сообщений о минировании... Кроме того, информационный обмен осуществляется по запросам о предоставлении сведений о взло-



манных банковских счетах и установлении пользователей страниц в социальных сетях.

Из года в год объем информации, которой мы обмениваемся с партнёрами, неуклонно рос. Однако сейчас мы отмечаем обратную тенденцию. Например, общий документооборот НЦБ Интерпола МВД России с правоохранительными органами стран-членов Интерпола по линии противодействия преступлениям, совершаемых при помощи информационно-коммуникационных технологий (ИКТ) в период с января по сентябрь **2021** года составил **1291** документ. А за тот же период нынешнего года — **только 649 документов**. Налицо снижение на 50%.

Тем не менее, мы продолжаем усилия в направлении развития взаимодействия с нашими иностранными партнерами. Так как в этом видим нашу главную задачу.

В прошлом году в Москву приезжал один из руководителей Интерпола, курирующий направление борьбы с киберпреступностью, Крейг Джонс. Он представил в Москве проект «Глобальной стратегии Интерпола по противодействию киберпреступности на 2022–2025 гг.». Состоялся полезный и конструктивный разговор, в том числе, и об участии России в осуществлении этой стратегии.

В мае этого года у нас состоялась очень полезная рабочая встреча с представителями профильных подразделений МИД России, в том числе Департамента Международной

Информационной Безопасности, в рамках которой обсудили актуальные вопросы межведомственного взаимодействия по линии ИКТ-преступности. В частности, на фоне усиления давления на Россию, выработали позицию относительно учета вклада Интерпола в будущую всестороннюю универсальную конвенцию по борьбе с киберпреступностью.

Что я имею ввиду: в июне текущего года в отношении правоохранительных органов Российской Федерации по каналам Интерпола были введены ограничительные меры, что существенным образом повлияло на обработку информации в учетах Интерпола. Кроме того, ряд стран-членов Интерпола заняли неконструктивную позицию в отношении России и практически свели к нулю взаимодействие с правоохранительными органами нашей страны по ряду важных линий совместной работы (Япония — полностью, Германия, Испания, Франция и некоторые другие — частично).

Для повышения эффективности борьбы с преступностью наши сотрудники пользуются различными базами данных Интерпола. И одновременно мы сами участвуем в пополнении этих баз данных актуальной информацией.

Так, например, Российским бюро Интерпола активно используется база данных Генерального секретариата Интерпола, содержащая изображения несовершеннолетних, пострадавших от сексуального насилия. База содержит около 3 миллионов изображений, она помогла найти и изобличить тысячи и тысячи преступников. В том числе и в нашей стране.

А совместно с Роскомнадзором Бюро осуществляет работу по организации проверки и включению в Единый реестр запрещенных сайтов и Интернет-ресурсов, принадлежащих

российскому сегменту сети Интернет и содержащих материалы со сценами сексуальной эксплуатации несовершеннолетних.

Два месяца назад наша делегация посетила штаб-квартиру Генерального секретариата Интерпола в Лионе. В результате переговоров договорились активизировать работу по обучению сотрудников МВД использованию баз данных Интерпола. Обучение будет происходить на их базе и завершится выдачей специальных сертификатов.

Есть еще одно подразделение Интерпола, с которым мы стараемся активизировать взаимодействие. Это Международный Центр Интерпола по инновациям в Сингапуре. Мы информировали этот Центр о формате нашей работы, мы направили туда несколько наших запросов по ведущимся нашими оперативными подразделениями уголовным делам... Так что пока ждем ответа.

Мы никогда не забываем и напоминаем нашим коллегам в Интерполе, что большинство компьютерных преступлений, по крайней мере, значительная их часть, являются трансграничными, то есть осуществляется с использованием территории разных стран. Что значительно затрудняет или вообще делает невозможным их расследование и пресечение деятельности криминальных сообществ. Так что мы обязаны помогать друг другу, чтобы справиться с киберпреступностью.

Несмотря на очевидный период охлаждения и в ряде случаев полного замораживания контактов и взаимодействия мы надеемся, что в непростой обстановке в мире всё-таки победит здравый смысл и взаимодействие правоохранительных структур не ослабнет, так как от этого напрямую зависит безопасность наших народов.

## Т.А. Абрегов

*Старший прокурор отдела Управления  
по надзору за исполнением законов  
о федеральной безопасности,  
международных отношениях,  
противодействии экстремизму и  
терроризму Генеральной прокуратуры  
Российской Федерации*

### **ПРОТИВОДЕЙСТВИЕ ПРОЯВЛЕНИЯМ ЭКСТРЕМИЗМА И ТЕРРОРИЗМА В СЕТИ «ИНТЕРНЕТ». ЗАКОНОДАТЕЛЬНОЕ РЕГУЛИРОВАНИЕ ВОПРОСОВ ОГРАНИЧЕНИЯ ДОСТУПА К ИНФОРМАЦИИ**

Широкое использование информационно-телекоммуникационных технологий обусловило активизацию экстремистских и террористических объединений по продвижению деструктивной идеологии и антиобщественных установок.

К примеру количество зарегистрированных в 2021 году преступлений экстремистской направленности возросло на 27%. Из них больше половины (62,5%) совершены с использованием сети «Интернет». В свою очередь, треть преступлений террористической направленности также выявлена в сети «Интернет».

Существует множество способов получения доступа к противоправному контенту, для чего не требуется глубоких познаний в области информационных технологий, а способы донесения деструктивной информации до широких масс постоянно совершенствуются.

Противодействие подобным негативным проявлениям требует от государственных органов оперативной выработки эффективных решений, которые должны отвечать современным вызовам и угрозам.

С 2014 года в соответствии со статьей 15 Федерального закона «Об информации, информационных технологиях и о защите информации» Генеральная прокуратура Российской Федерации реализует полномочия по направлению в Роскомнадзор требований о внесудебной блокировке информации в сети «Интернет».

Перечень блокируемой информации установлен указанной статьей и является исчерпывающим.



Результатом многолетней совместной с Роскомнадзором работы стало удаление многочисленных материалов, содержащих призывы к экстремизму, терроризму, массовым беспорядкам и другим противозаконным действиям.

Следует также отметить, что благодаря внесенным в Федеральный закон № 149-ФЗ изменениям с 1 января 2022 года во внесудебном порядке также блокируется информация о деятельности организаций, запрещенных в связи с осуществлением экстремистской и террористической деятельности, что особенно актуально на фоне активизации деструктивных молодежных сообществ.

К примеру, по иску Генеральной прокуратуры Российской Федерации судом признано террористическим движение «Колумбайн», основанное на идеологии насилия и терроризма. Пропаганда идеологии движения привела к ряду шокирующих своей жестокостью нападений на образовательные организации и гибели детей. Для массовой пропаганды в Интернете так называемой «колумбайновской» идеологии было создано почти 700 сообществ.

Признана экстремистской и запрещена судом также по иску Генеральной прокуратуры Российской Федерации деятельность международного общественного движения «Арестантское уголовное единство» (AYE). Только в социальной сети «ВКонтакте» насчитыва-



лось более 30 тыс. групп, участники которых пропагандировали идеологию криминальной субкультуры, а также призывали к совершению преступлений как общеуголовной, так и экстремистской направленности.

На основании требований Генеральной прокуратуры Российской Федерации доступ к материалам, пропагандирующим и оправдывающим деятельность названных организаций, систематически блокируется.

14 июля текущего года в связи с непрекращающимися информационно-психологическими атаками и распространением материалов, направленных на дестабилизацию общественно-политической обстановки в России приняты следующие изменения в указанный выше закон, а именно, внесудебной блокировке также подлежит «недостоверная информация, содержащая данные об использовании Вооруженных Сил Российской Федерации в целях защиты интересов Российской Федерации и ее граждан, поддержания международного мира и безопасности, а равно содержащей данные об исполнении государственными органами Российской Федерации своих полномочий за пределами территории Российской Федерации в указанных целях, или информации, на-

правленной на дискредитацию использования Вооруженных Сил, а также содержащей призывы к введению в отношении Российской Федерации, ее граждан либо российских юридических лиц политических, экономических или иных санкций.

Ранее Генеральной прокуратурой также были приняты меры реагирования в связи с деструктивной и, явно выходящей за пределы коммерческих интересов, деятельности американской транснациональной компании Мета.

По требованию Первого заместителя Генерального прокурора ограничен доступ к социальным сетям Фейсбук и Инстаграм.

Помимо этого по иску Генпрокуратуры России деятельность компании Мета запрещена по основаниям осуществления экстремистской деятельности.

Поводом к этому послужили заявления официальных представителей Мета, а также организованная ими кампания против интересов России и ряда отечественных журналистов. Альтернативная и противоречащая интересам США информация всячески ограничивалась, а российские СМИ подвергались дискриминации.



## Н.М. Гудков

*Старший прокурор Главного управления  
по надзору за следствием, дознанием и  
оперативно-разыскной деятельностью  
Генпрокуратуры России*

### **СОВРЕМЕННЫЕ УГРОЗЫ ИСПОЛЬЗОВАНИЯ ВЫСОКИХ ТЕХНОЛОГИЙ В ПРЕСТУПНЫХ ЦЕЛЯХ И ПРИНИМАЕМЫЕ МЕРЫ ПО ПРОТИВОДЕЙСТВИЮ ПОСЯГАТЕЛЬСТВАМ В УКАЗАННОЙ СФЕРЕ**

Вынесенная сегодня на обсуждение тема остается крайне актуальной и с каждым годом продолжает требовать к себе все большего внимания со стороны как государства, так и всего мирового сообщества.

Криминальные деяния, совершенные с использованием информационно-коммуникационных технологий, являются одним из самых прогрессивно развивающихся видов преступности.

При этом регулярный анализ практики противодействия таким преступлениям свидетельствует о сохраняющихся рисках цифровизации традиционных видов противоправных посягательств, посягающих на права личности, причиняющих имущественный ущерб гражданам, коммерческим структурам и государству, а также создающих угрозу национальной безопасности.

Среди факторов, характеризующих активность преступников на данном направлении, можно выделить внедрение высоких технологий в повседневную жизнь и все сферы правоотношений, доступ все большего количества пользователей к глобальным информационным сетям, развитие электронной торговли, дистанционных услуг и форматов взаимодействия, а также проведения различных операций, не требующих непосредственного контакта.

В свою очередь, инструменты и механизмы совершения преступлений, применяемые злоумышленниками нацелены все больше на обеспечение их конспирации, анонимизацию непосредственно процессов сбора, аккумулярования, перемещения и трансформации информации и финансовых активов, трансграничность таких процессов, охват широкой аудитории, возможность массового и скоростного воздействия на цель.



Все это сопровождается опережающими темпами трансформации преступности в сфере ИКТ в противовес имеющимся системам безопасности и уровню правового регулирования, что создает предпосылки злонамеренного использования телекоммуникационных и интернет-сервисов в отсутствие каких-либо издержек.

На этом фоне можно констатировать, что общемировые тенденции увеличения числа преступных посягательств, совершенных с применением ИКТ коррелируются с процессами, происходящими в Российской Федерации. Массив посягательств указанной категории, совершаемых в нашей стране, в общей структуре преступности стабильно превышает 20%, достигая полумиллиона противоправных деяний в год.

В этой связи координация деятельности правоохранительных органов по выявлению, предупреждению и пресечению преступлений в сфере информационно-коммуникационных технологий остается одним из ключевых направлений работы органов прокуратуры Российской Федерации. Причем плоды этой деятельности с каждым годом все очевиднее.

В результате реализованных в последние годы мер наблюдается существенное снижение роста динамики преступности с 73% по итогам 2020 г. до почти 1% по итогам прошлого года (свыше 500 тыс.) и по итогам 1 полуго-

дия текущего года уже отрицательная их динамика (- 8%).

Позитивные тенденции мы наблюдали в части снижения количества случаев использования Интернета при совершении деяний указанной категории (182 тыс.) мобильной связи (-13%, 95 тыс.), банковских карт (-31%, 62 тыс.). Следовательно снизился и объем ущерба, причиненного этими посягательствами, гражданам с 3 до 2,8 млрд рублей.

Активнее работа правоохранительными органами велась по выявлению посягательств в сфере непосредственно компьютерной информации (+ 53% до 7 тыс.), которые собственно и создают предпосылки к несанкционированному воздействию на информацию, неправомерному воздействию на критическую информационную инфраструктуру, формируют основы для обеспечения анонимности злоумышленников в сети.

Определенное влияние на указанные тенденции оказала реализация в 2020–2021 гг. мероприятий, предусмотренных постановлением Координационного совещания руководителей правоохранительных органов от 2020 года и протоколами оперативных совещаний Совета Безопасности Российской Федерации, посвященных тематике противодействия киберпреступности.

В структуре преступности в сфере высоких технологий по-прежнему преобладают кражи (156 тыс.) и мошенничества (248 тыс.). Классическим методом их совершения выступает, как и прежде, социальная инженерия, которая чаще всего направлена на социально уязвимые группы людей.

Эффективнее работа строилась по выявлению незаконного оборота порнографических материалов, в т.ч. с изображениями несовершеннолетних (+10% до 2 тыс.), дистанционного сбыта наркотиков (+9% до 51 тыс.). Также в стране зарегистрировано порядка 8 тыс. (+60%) преступлений сопряженных с незаконным оборотом персональных данных и иной охраняемой законом информации, а также непосредственно в сфере посягательств на компьютерную информацию.

Подобные тенденции, в частности, обусловлены расширением деятельности темных торговых площадок, в том числе размещенных в ДаркНете. Указанные ресурсы

специализируются на предоставлении услуг по обороту запрещенных предметов и документов, баз персональных данных граждан, а также в сфере «хакинга», «кардинга», легализации преступных доходов, используются для рекрутинга, нанесения кибератак, сбора и распространения различных сведений ограниченного характера.

Используемая данными площадками модель криминального бизнеса предусматривает чрезвычайно эффективные средства по анонимизации их участников, от размещения ресурсов в защищенных сетях (TOR и др.), шифрования применяемого в мессенджерах трафика (Signal, Telegram и т.д.), до активного применения криптовалют, в т.ч. их наиболее защищенных видов (Monero, Dash и пр.).

Это обуславливает наличие в открытом доступе большого объема информации о способах совершения компьютерных атак, инструментария, автоматизирующего их проведение, сервисов для размещения вредоносной инфраструктуры, в том числе сохраняющих анонимность пользователя, приводят к все более широкому задействованию ИКТ в противоправной деятельности.

На этом фоне распространена практика создания хакерами межнациональных группировок, члены которых при подготовке и совершении преступления могут находиться на территории разных стран и континентов.

Причем указанные обстоятельства создают дополнительные сложности в расследовании преступлений и формировании доказательственной базы.

На этом фоне продолжает увеличиваться интенсивность взаимодействия как между компетентными органами предварительного расследования, так и между центрами реагирования на компьютерные инциденты.

Кроме того, особого внимания заслуживает поступательное усиление интенсивности и числа информационных атак, в частности DDoS, на госорганы, банки, предприятия, больницы, школы и коммерческие организации. В целях дезорганизации работы государственных органов и дестабилизации общественной обстановки также осуществлялась массовая рассылка ложных сообщений о террористических актах, в том числе в адрес объектов социальной инфраструктуры (более 20 тыс. преступлений).

Нередко этому способствовали и призывы представителей иностранных государств к совершению подобного рода действий, подробная информация об этом летом опубликована на официальном сайте МИДа России и звучала на площадках ООН.

Всего в 2021 г. предварительно расследовано почти 120 тыс. противоправных посягательств в сфере ИКТ (+25%). При этом развитие методов противодействия правонарушениям в цифровом пространстве все чаще позволяет выявлять серийные преступления.

Среди основных мер, способствующих повышению эффективности работы правоохранителей и закреплению позитивных тенденций по сокращению числа обозначенных групп преступлений следующие.

Продолжается совершенствование непосредственного уголовного законодательства, которое уже сейчас содержит порядка 30 уголовно-наказуемых составов преступлений рассматриваемой категории.

При этом в целях формирования единого подхода при отнесении преступных деяний к числу совершенных в сфере ИКТ утвержден перечень данных преступлений. Разработанные критерии позволяют повысить информативность статистических показателей на данном направлении для более оперативного реагирования на развивающиеся в цифровой среде угрозы.

Продолжается формирование специализированных подразделений правоохранительных органов по противодействию ИКТ преступлениям. Осуществляется внедрение в их деятельность компьютерно-криминалистических инструментов и автоматизированных поисковых систем. К примеру, подсистемы ИБД-Ф «Дистанционные мошенничества», только за один год с момента введения которой в эксплуатацию установлено свыше 600 тыс. признаков серийных преступлений, в том числе совершенных в разных регионах страны. Развивается потенциал подобных систем, упор в которых сделан на фиксацию и категорирование цифровых следов преступлений, для целей пресечения незаконного оборота наркотических средств, и в иных областях.

Особое внимание уделяется совершенствованию электронного документооборота с финансово-кредитными учреждениями, операторами связи и провайдерами Интернет ус-

луг, в том числе в рамках централизованной электронной платформы для обеспечения оперативного взаимодействия всех компетентных органов и учреждений.

В частности, осуществляется интеграция информационных ресурсов Банка России и МВД России, что позволит мгновенно реагировать на факты мошеннических действий и оперативно замораживать преступные доходы злоумышленников. Кроме того, соответствующие системы позволяют пресекать действия злоумышленников с применением средств мобильной связи. Используемые ими номера вносятся в соответствующие базы данных и тысячами блокируются операторами связи.

Совершенствуются и непосредственно механизмы взаимодействия всех заинтересованных сторон. В частности, закреплён предельный срок предоставления банками сведений по счетам по запросам оперативных подразделений (до 3 суток). Расширяются возможности использования информационных технологий в уголовном судопроизводстве.

Прокуроры, в свою очередь, ориентированы на усиление надзора.

К примеру, в Генеральной прокуратуре Российской Федерации установлен контроль за результатами проверки правоохранительными органами сообщений Банка России об операциях, совершенных без согласия клиента (по итогам за год возбуждено порядка 30 тыс. дел, потерпевшие по ним попросту не хотели тратить время на обращение в полицию), а также о выявлении в сети «Интернет» сайтов, распространяющих недостоверную информацию о предоставлении финансовых услуг населению и осуществлении нелегальной деятельности на финансовом рынке (с признаками финансовых пирамид).

Пристальное внимание уделяется процессам профилактики рассматриваемых преступлений. На регулярной основе осуществляются мероприятия по повышению правовой и финансовой грамотности граждан. Особо эффективны при этом инструменты профилактики, используемые во взаимодействии с финансово-кредитными организациями.

Большие усилия сконцентрированы в повышении квалификации всех задействованных в данной работе лиц. В профильных учеб-

ных заведениях введены соответствующие дополнительные курсы, формируются специализированные учебные программы, межведомственные и межгосударственные форматы подготовки кадров и повышении квалификации специалистов.

Отдельного внимания на этом направлении заслуживает реализация представленных органам прокуратуры полномочий по ограничению доступа к запрещенной информации, в т.ч. способной причинить вред здоровью и развитию детей.

Одновременно стоит отметить и уже формирующуюся нормативную базу по деанонимизации информационно-телекоммуникационного пространства, блокированию звонков с подменой номеров и противоправного контента в сети «Интернет», несанкционированным действиям и неправомерному использованию услуг сетей связи.

К примеру, для пресечения телефонного мошенничества соответствующие изменения предусмотрены поправками в Федеральный закон «О связи». Они детально регламентируют порядок прекращения оказания услуг связи или услуг по пропуску соответствующего трафика (подменных номеров) в сеть.

Также формируются новые инструменты, значительно повышающие безопасность банковских платежей и переводов. Особое внимание при этом акцентировано на профилактике мошеннических действий с использованием антифрод систем самими банками.

Совершенствуется законодательство в сфере персональных данных. Ужесточена ответственность их операторов в случае утечек такой информации, дополнены механизмы обеспечения безопасности их оборота.

Конечно, имеются и пробелы, которые мы стараемся преодолеть. Прежде всего, в части совершенствования порядка производства специальных процессуальных действий в электронном пространстве, применения в процессе доказывания электронных доказательств. Но и на этом направлении уже имеются существенные наработки, которые мы планируем реализовать в ближайшее время.

Подытоживая выступление, отмечу, что понимание глубины перечисленных угроз и вызовов, а также их существа позволило правоохранительной системе при координирующей роли Генеральной прокуратуры Российской Федерации своевременно реформировать порядок организации работы.

Вместе с тем, развитие технологий, их широкое распространение и повышенное влияние на все сферы жизнедеятельности определяют необходимость дальнейшего наращивания потенциала правоохранительных органов по противодействию им, включая совершенствование международного сотрудничества в целях усиления качества и эффективности такой деятельности.

Одним из важнейших направлений при этом является консолидация усилий всех государств на площадке Специального комитета для разработки всеобъемлющей Конвенции по противодействию преступлениям в сфере информационно-коммуникационных технологий.

Причем отрадно, что проводимые Генеральной прокуратурой Российской Федерации межведомственные консультации по теме борьбы с преступностью, демонстрируют единство подходов на данном направлении со многими партнерами.



## А.А. Вураско

Руководитель группы развития  
специальных сервисов  
ООО «Ростелеком-Солар»

### НОВЫЕ РЕАЛИИ: ВЛИЯНИЕ ГЕОПОЛИТИЧЕСКОЙ ОБСТАНОВКИ НА ЛАНДШАФТ КИБЕРУГРОЗ В РОССИИ В КРАТКОСРОЧНОЙ И ДОЛГОСРОЧНОЙ ПЕРСПЕКТИВАХ

2022 год лишний раз доказал, что геополитическая обстановка способна серьезно влиять на ландшафт киберугроз. В то же время он продемонстрировал и удивительную гибкость и стойкость киберкриминала, а также его возможности адаптироваться практически к любым условиям.

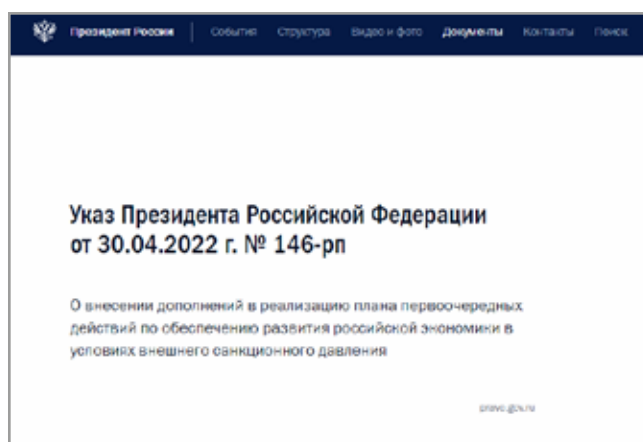
Сразу оговорюсь, что буду использовать термины «киберпреступники» и «киберкриминал» применительно не только к тем лицам, которые совершают преступления непосредственно в сфере информации и телекоммуникаций, но и к некоторым категориям мошенников, использующих ИКТ. Все дело в том, что в последние годы в связи с развитием концепции Cybercrime as a Service (киберпреступление как услуга) происходит активное сращивание некоторых направлений криминального бизнеса. Так, например, в случае с мошенничествами на торговых площадках, волна которых захлестнула Россию еще в 2020 году, успех данной схемы заключался в том, что опытные и хорошо подготовленные киберпреступники разработали изначальную схему, создали всю необходимую инфраструктуру, включая фишинговые сайты, сценарии вывода похищенных денег, разработали обучающие материалы, а после отдали все это на откуп обычным неподготовленным людям, получая свой процент с каждого перевода денег от жертвы. Казалось бы, сами по себе мошенничества на «Авито» и иных подобных платформах не являются киберпреступлением — это вполне традиционные мошенничества, в процессе осуществления которых интернет используется в первую очередь как средство коммуникации. Но в случае с концепцией Cybercrime as a Service интернет — это не только удобный способ общения с жертвами — это инфраструктурный комплекс, позволяющий реа-



лизовать преступление от и до. То же самое во многом применимо и к современным телефонным мошенничествам. В ряде сценариев задействуются и фишинговые сайты и достаточно сложные скрипты, позволяющие автоматизировать процесс совершения преступления.

Естественно, такие сайты и скрипты создаются не рядовыми исполнителями, а профессионалами криминального бизнеса, формирующими под своим крылом огромную преступную сеть.

Таким образом получается, что простые мошенники, коммуницирующие с жертвами



**Пример фейкового сайта Президента России, созданного для того, чтобы убедить жертву в правдивости слов злоумышленников.**



посредством интернета или мобильной связи, по факту являются членами распределенных транснациональных преступных групп, у руля которых стоят самые настоящие киберпреступники.

Но вернемся к нашей теме. До 24 февраля 2022 года все тенденции киберкриминального рынка в России были достаточно легко прогнозируемы. Основным мотивом киберпреступников являлось желание извлечь материальную выгоду, схемы работы были отлажены и проверены временем, а значит — никаких активных действий и революционных изменений в общем ландшафте угроз не предвиделось. Однако, начало специальной военной операции повлекло за собой целый ряд последствий, оказавших значительное влияние на ландшафт угроз.

Во-первых, резко увеличилось количество кибератак как таковых. Причем речь идет не только об объектах критической информационной инфраструктуры, атакам подверглись самые разные организации на территории Российской Федерации, даже те, которые ранее не были интересны киберпреступникам по причине того, что заработать на них было просто невозможно. Подобный всплеск стал возможен благодаря тому, что вектор мотивации атакующих сместился в сторону хактивизма. Если раньше целью атак было желание заработать, то теперь главная задача — навредить российским организациям и предприятиям. Это привело к тому, что полученные в результате атак данные стали не выстав-

ляться на продажу, а раздаваться бесплатно, а перечень атакуемых объектов существенно расширился: атакам подверглись абсолютно все уязвимые ресурсы вплоть до сайтов детских садов.

И в этом отношении текущая ситуация как никогда хорошо продемонстрировала, что информационная безопасность в современном мире должна находиться на первом месте. Концепция «да кому мы нужны, кто нас будет атаковать» давно не работает. Любая организация, использующая информационно-телекоммуникационные технологии, может и будет подвергнута атакам.

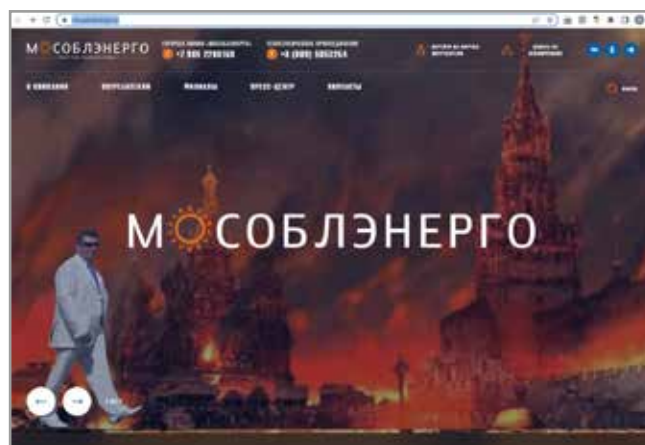
Во-вторых, западные санкции и уход из России платежных систем Visa и Mastercard ударили в том числе и по киберпреступникам, ведь привычные им пути вывода денег и способы оплаты зарубежных сервисов оказались нарушены. В марте 2022 года количество фишинговых атак и кибермошенничеств сократилось на 85 процентов по сравнению с показателями января-февраля.

Казалось бы, можно радоваться, но нет, уже к концу мая количество сетевых мошенничеств вернулось к предыдущему уровню, а по ряду направлений даже превысило показатели 2021 года. Все дело в том, что злоумышленники перестроили свои алгоритмы работы и успешно адаптировались к новым условиям.

А вот число кибератак на российские объекты стало напротив снижаться, только вот причина этого явления кроется не в том, что



**Пример фишингового сайта, созданного телефонными мошенниками под конкретную жертву.**



**Пример совершенного хактивистами дефейса сайта «Мособлэнерго».**

хакеры потеряли интерес к отечественной инфраструктуре, а в том, что все наиболее доступные объекты уже подверглись компрометации и остались только те ресурсы, атака на которые требует серьезной подготовки, хороших навыков и финансовых вложений.

Впрочем, за период с марта по июнь в сети оказалось такое количество полученных в результате взломов конфиденциальных данных, что люди просто перестали удивляться новым утечкам. Только крупные инциденты, затронувшие популярные курьерские службы, стали причиной попадания в свободный доступ персональных данных миллионов россиян. Появились сайты-агрегаторы, на которых любой человек может абсолютно бесплатно получить данные о практически любом гражданине нашей страны, просто введя его имя или номер телефона.

На протяжении последнего года злоумышленники очень умело использовали в своих целях актуальную новостную повестку и инфоповоды. Стоило произойти какому-либо событию, будоражащему умы наших соотечественников, как тут же это событие становилось информационным прикрытием для новой волны сетевых мошенничеств. При этом в ряде случаев очень хорошо прослеживалась территориальная привязка, нацеленность фейковых сайтов именно на россиян, а не на граждан сопредельных государств, например Украины. В ряде случаев имелась даже приписка о том, что для граждан этой страны недоступны якобы полагающиеся социальные выплаты — все для того, чтобы украинцы случайно не дополнили копилку жертв мошеннической схемы.

И вот тут мы подходим к самому главному тезису, который я не перестаю повторять последние 10 лет. Современная киберпреступность трансгранична. Злоумышленники прекрасно понимают, что совершать преступления в отношении граждан другого государства в условиях, когда информационный обмен между правоохранительными органами разных стран серьезно ограничен, предельно выгодно. Они используют любые международные противоречия в своих целях, что позволяет им наполнять кошельки, оставаясь при этом совершенно безнаказанными. Я думаю, ни для кого не будет секретом, что значительная часть киберпреступлений, а также



## Пример мошеннического сайта.

телефонных и сетевых мошенничеств в отношении россиян в последние годы осуществляется с территории Украины. Причем было бы неправильно говорить о том, что такие преступления совершаются исключительно украинцами — многие российские киберпреступники эмигрировали в сопредельное государство для того, чтобы скрыться от правосудия. Причина проста: взаимоотношения правоохранительных органов России и Украины после 2014 года находится на около нулевом уровне. Контакты носят эпизодический и далеко не всегда продуктивный характер.

Или другой пример. В последний год наблюдается активная миграция мошеннических схем, затрагивающих популярные торговые площадки, на запад. С чем это связано? С одной стороны, с тем, что российский рынок подобных мошенничеств уже банально перенасыщен, пик их популярности прошел и находить жертв становится все сложнее. А с другой — работать по Европе банально безопаснее. Даже в том случае, если правоохранительные органы другой страны смогут выйти на след злоумышленника из России, процесс коммуникации в лучшем случае займет месяцы, в худшем — годы, поэтому надеяться на счастливый финал с наказанием злоумышленника особенно не приходится.

Какой вывод можно сделать из всего сказанного? Киберпреступность — это глобальная проблема и эффективность противодействий ей напрямую зависит от того, насколько быстро и качественно будут осуществляться контакты между правоохранительными органами разных государств.

Несколько лет назад на одной международной конференции кто-то из представите-

лей киберполиции одной из западноевропейских стран сказал, что мы должны совершенствовать наше взаимодействие вне зависимости от внешнеполитической ситуации. Пока политики играют в свои глобальные игры, мы работаем и наша общая цель бороться с преступностью. Достаточно одному государству выпасть из этой системы, как вся наша борьба теряет эффективность. И я полностью придерживаю эти слова.

В современном информационном мире мы уже не сможем оградить себя неприступной стеной, а значит нам надо не опускать руки и искать новые пути взаимодействия, вырабатывать механизмы обмена информацией и лавировать между появляющимися внешними негативными факторами. Пока у киберпреступников это получается делать намного эффективнее. Но в наших силах все изменить.

## М.Л. Немсадзе

*Заместитель начальника отдела  
международного сотрудничества в  
области безопасности Департамента  
международного права и сотрудничества  
Минюста России*

### **МЕЖДУНАРОДНО-ПРАВОВЫЕ МЕХАНИЗМЫ СОТРУДНИЧЕСТВА В ОБЛАСТИ БОРЬБЫ С ИНФОРМАЦИОННОЙ ПРЕСТУПНОСТЬЮ И ПЕРСПЕКТИВЫ ИХ СОВЕРШЕНСТВОВАНИЯ**

В условиях отсутствия универсального международного договора, регулирующего вопросы борьбы с информационной преступностью, международные договоры о взаимной правовой помощи по уголовным делам составляют основу сотрудничества в области расследования информационных преступлений.

На национальном уровне в России вопросами разработки и заключения двусторонних договоров о правовой помощи, а также присоединения к многосторонним форматам в этой сфере занимается Министерство юстиции Российской Федерации, которое является одним из центральных органов по вопросам, связанным с деятельностью судов.

Следует отметить, что у Российской Федерации на настоящий момент имеется 47 действующих двусторонних международных договоров о взаимной правовой помощи по уголовным делам.

Одновременно необходимо обозначить высокую значимость и эффективность таких региональных многосторонних международных договоров о взаимной правовой помощи как Конвенция о правовой помощи и правовых отношениях по гражданским, семейным и уголовным делам 1993 г. (*Азербайджан, Армения, Белоруссия, Грузия, Казахстан, Киргизия, Молдавия, Российская Федерация, Туркменистан, Таджикистан, Узбекистан, Украина*), заключенная в рамках СНГ, и имеющая для России и региона огромное значение ввиду особых исторических связей ее участников.

Конвенция о правовой помощи и правовых отношениях по гражданским, семейным и уголовным делам 2002 г., в настоящее время участниками Кишиневской конвенции являются 6 стран (*Азербайджан, Армения, Беларусь, Казахстан, Киргизия и Таджикистан*). Россий-



ская Федерация ратифицировала данную Конвенцию 30 декабря 2021 г. № 452-ФЗ, а также Европейская конвенция о взаимной правовой помощи по уголовным делам 1959 г. и протоколы к ней, на основании которой оказываются существенные объемы правовой помощи по уголовным делам.

С учетом указанных многосторонних инструментов общий территориальный охват действующих для России международных договоров о взаимной правовой помощи по уголовным делам составляет 97 государств.

К сожалению, следует отметить, что указанные договоры не в полной мере учитывают специфику информационных преступлений.

В связи с этим в ходе переговорного процесса с иностранными партнерами Минюстом России предпринимаются отдельные шаги, направленные на совершенствование определенных положений заключаемых договоров. Среди данных положений хотелось бы особенно выделить те положения, которые касаются вопросов закрепления сроков исполнения запросов о правовой помощи, повышения оперативности и применения современных механизмов взаимодействия, в том числе использование специальных защищенных каналов связи.

Как представляется, главной проблемой в области борьбы с информационной преступностью в правовом плане на данном этапе является отсутствие универсального догово-



ра в сфере противодействия информационной преступности.

В этой связи важно отметить, что в настоящее время Российская Федерация ведет активную работу в рамках Специального межправительственного комитета по разработке всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях, утвержденного резолюцией Генеральной ассамблеи ООН. Так, 27 июля 2021 года Россия внесла в специальный комитет ООН свой проект универсальной конвенции.

*Проект конвенции имеет ряд преимуществ:*

- *учитывает современные вызовы и угрозы в сфере международной информационной безопасности (в том числе криминальное использование криптовалют);*
- *вводит новые составы преступлений, совершаемых с использованием информационно-коммуникационных технологий: распространение фальсифицированной медицинской продукции, оборот наркотиков, вовлечение несовершеннолетних в совершение противоправных деяний, опасных для их жизни и здоровья, и другие;*
- *расширяет сферу международного сотрудничества в вопросах выдачи и оказания правовой помощи по уголовным делам, включая выявление, арест, конфискацию и возврат активов.*

Но, тем не менее, в условиях отсутствия универсального международного договора, регулирующего вопросы борьбы с информационной преступностью, отдельного внимания заслуживают специализированные международно-правовые механизмы сотрудничества в области борьбы с информационной преступностью, одним из которых, например, является Соглашение о сотрудничестве государств — участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий 2018 г., вступившее в силу 12 марта 2020 года. Соглашение предусматривает обязательную криминализацию широкого ряда деяний:

- а) уничтожение, блокирование, модификация либо копирование информации, нарушение работы информационной

(компьютерной) системы путем несанкционированного доступа к охраняемой законом компьютерной информации;

- б) создание, использование или распространение вредоносных программ;
- в) нарушение правил эксплуатации компьютерной системы лицом, имеющим к ней доступ, повлекшее уничтожение, блокирование или модификацию охраняемой законом компьютерной информации, если это деяние причинило существенный вред или тяжкие последствия;
- г) хищение имущества путем изменения информации, обрабатываемой в компьютерной системе, хранящейся на машинных носителях или передаваемой по сетям передачи данных, либо путем введения в компьютерную систему ложной информации, либо сопряженное с несанкционированным доступом к охраняемой законом компьютерной информации (и другие), а также устанавливает различные эффективные формы сотрудничества государств-участников.

В заключение в целях успешной борьбы с информационной преступностью в контексте развития правовых механизмов в данной сфере видятся следующие **рекомендации**:

- своевременное совершенствование национального законодательства;
- повышение уровня подготовки сотрудников правоохранительных органов по вопросам законодательства об информационной преступности, сбора доказательств и их информационно-технических навыков;
- развитие сотрудничества между государствами путем заключения новых и совершенствования действующих двусторонних договоров о взаимной правовой помощи по уголовным делам (одним из прорабатываемых способов совершенствования является подписание дополнительных протоколов);
- увеличение числа участников многосторонних договоров о взаимной правовой помощи по уголовным делам;
- осуществление совместной работы государств, направленной на принятие универсального международного договора в сфере борьбы с информационной преступностью на площадке ООН.





**КРУГЛЫЙ СТОЛ № 5**  
**РАЗВИТИЕ РЕГИОНАЛЬНОГО СОТРУДНИЧЕСТВА**  
**В СИСТЕМЕ МЕЖДУНАРОДНОЙ**  
**ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

**Модератор:**

*Смирнов А.И.*, генеральный директор НАМИБ

**О.С. Лобанова**

*Атташе ДМИБ МИД России*

## **О ПРОДВИЖЕНИИ РОССИЙСКИХ ПОДХОДОВ ПО МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ПРОФИЛЬНЫХ РЕГИОНАЛЬНЫХ ПЛОЩАДКАХ**

Позвольте поблагодарить организаторов за возможность принять участие в столь масштабном и значимом мероприятии.

В настоящее время система международных отношений в области информационной безопасности претерпевает существенные изменения. ИКТ трансформируются из средства мирного развития общества в инструмент достижения геополитических задач. Западные страны продолжают раскалывать международное информационное пространство и провоцировать опасные конфликты. Возрастают угрозы в информационном пространстве. В силу своей специфики ИКТ становятся орудием в политическом противоборстве, которое может спровоцировать реальную конфронтацию.

В этих условиях как никогда важно сплотиться и вести скоординированную политику для поощрения ответственного использования ИКТ, развития мер доверия в информационном пространстве и противодействия применению ИКТ в преступных целях. Важно, чтобы коллективные усилия в этой области носили деполитизированный, прагматичный характер.

Россия проводит последовательную работу на этом направлении. Задействованы уже устоявшиеся площадки, активизируются новые форматы.

В частности, огромный потенциал видим в Шанхайской организации сотрудничества. Шестнадцать лет назад именно ШОС стала первой региональной организацией, выработавшей правила ответственного поведения государств в информационном пространстве.

Ключевой структурой ШОС в данной области на протяжении многих лет остается Группа экспертов ШОС по МИБ. Под ее эгидой был принят целый ряд фундаментальных решений.

Группа не стоит на месте и адаптируется под новые реалии. В рамках ее последне-



го заседания (Ташкент, 13 июля 2022 г.) был представлен ряд политических и практических инициатив. В частности, речь шла о возможном подключении к формату Группы государств-наблюдателей при Организации — Афганистана, Белоруссии, Ирана, Монголии, а также Туркменистана.

Среди практических предложений можно отметить: создание реестра контактных пунктов в рамках ШОС по обмену сведениями о компьютерных инцидентах; налаживание специализированного диалога по линии национальных центров реагирования на компьютерные инциденты; формирование списка подразделений и контактных лиц, ответственных за взаимодействие в правоохранительной сфере.

Важным направлением считаем возможность подготовки квалифицированных специалистов государств-членов ШОС в сфере компьютерной и информационной безопасности на базе реализуемых профильных программ высшего и дополнительного профессионального образования.

Высоко оцениваем уровень практического межведомственного взаимодействия в рамках ОДКБ. Считаем необходимым сосредоточиться на активизации его политической составляющей. С этой целью выдвигаем конкретные инициативы по развитию нашего сотрудничества в области МИБ, что идет в развитие вступившего в силу Соглашения о сотрудничестве

в области обеспечения информационной безопасности 2017 г.

Еще одной крупной площадкой является Региональный форум АСЕАН по безопасности (АРФ). К настоящему времени Форумом накоплен значительный опыт в укреплении мер доверия в области МИБ. Во многом этому способствовала разработка Россией, Австралией и Малайзией и принятие в 2015 г. Рабочего плана АРФ по безопасности в сфере использования ИКТ и самих ИКТ. Утверждение этого документа стало важным шагом на пути к формированию общих ориентиров стран-участниц АРФ в области развития мирной и безопасной ИКТ-среды, а также предотвращению конфликтов в информационном пространстве.

Непосредственно переговоры по мерам доверия в области МИБ начались в 2018 г. в рамках специализированного механизма межсессионных встреч по безопасности в сфере использования ИКТ (МВ-ИКТ). Эксперты вырабатывают конкретные инициативы в соответствии с мандатом, заложенным в Рабочем плане.

Россия является одним из наиболее активных участников данного процесса. С 2020 года последовательно продвигаем две наши ключевые инициативы — по профильной терминологии и противодействию использованию ИКТ в преступных целях.

Предпосылкой для запуска дискуссии по терминологии стала негативная тенденция, которую мы фиксируем на протяжении многих лет как на региональных — это АРФ, ОБСЕ, ШОС и СНГ, так и на глобальных площадках — ООН — принципиальные разногласия государств в понимании специализированных терминов создают препятствия для развития сотрудничества.

В целях нахождения в АРФ общего понимания данной проблематики Россия и Камбоджа запустили профильную дискуссию. В 2021 г. проведен опрос среди стран-участниц АРФ. Результаты такого исследования наглядно продемонстрировали актуальность данной темы для подавляющего большинства арфовских стран. Многие государства-респонденты отметили нехватку опыта и компетенции в этой сфере, что тормозит процесс выработки терминологии на национальном уровне. Многие высказались в пользу проведения специали-

зированной дискуссии на площадке АРФ в целях обмена опытом и лучшими практиками.

Понимая актуальность данной темы, Россия и Камбоджа решили организовать серию семинаров по данной проблематике. Первый такой семинар состоялся 7 апреля с.г. в онлайн-режиме. В нем приняли участие представители государственного и частного секторов из 17 стран-участниц АРФ, а итоги продемонстрировали большой интерес к этой теме. Эксперты обсудили национальный опыт и наработки международных площадок в этой сфере. Более того, некоторые страны выступали за необходимость создания единого глобального глоссария по международной информационной безопасности. Очередной семинар запланирован на следующий год.

Что касается российской инициативы о противодействии использованию ИКТ в преступных целях, ее актуальность трудно переоценить. Количество преступлений в информационном пространстве неуклонно растет. Разнообразие и масштаб преступных деяний только возросли в связи с пандемией, что не может не вызывать озабоченность международного сообщества. Очевидно, что только сплоченные действия государств смогут помочь справиться с этой угрозой. В этих целях учрежден спецкомитет ООН, который занимается разработкой конвенции о противодействии использованию ИКТ в преступных целях.

В поддержку глобального процесса Россия совместно с другими странами-участницами АРФ на протяжении двух лет проводит двухдневный семинар. В нем традиционно принимают участие представители государственных органов, бизнеса, академического сообщества, непосредственно вовлеченные в процесс противодействия информационной преступности. Участники обсуждают не только политические вопросы, но и технические аспекты, обмениваются лучшими практиками правоохранительных органов. Отличительной особенностью подобных мероприятий является их практическая направленность. Интерес со стороны арфовцев к подобной инициативе с каждым годом только возрастает.

В прошлом году на министерской встрече АРФ Россия (совместно с Индонезией, Республикой Корея и Австралией) утверждена сопредседателем МВ-ИКТ на 2022–2024 гг. Нацелены на то, чтобы приложить максимум

усилий для обеспечения предметной неполитизированной дискуссии в интересах всех участников Форума.

Придаем большое значение и укреплению диалогового партнерства по МИБ с АСЕАН. Данный формат был учрежден в прошлом году во исполнение соответствующего решения руководства наших стран. Диалог Россия-АСЕАН по вопросам, связанным с безопасностью ИКТ, призван стать основной площадкой по рассмотрению данной проблематики и способствовать расширению прямого межведомственного взаимодействия между нашими странами. Первая встреча в таком формате состоялась осенью прошлого года в онлайн-режиме.

В 2021 году Россия инициировала обсуждение тематики МИБ и в рамках нового формата — Совещания по взаимодействию и мерам доверия в Азии (СВМДА). По нашему предложению впервые в каталог мер доверия включен раздел «Безопасность в сфере использования ИКТ и самих ИКТ». Россия утверждена

координатором, а Китай — сокоординатором данного направления на период 2022–2023 гг. Предстоит насыщенная содержательная работа по развитию данной меры доверия. В этом году провели первое мероприятие — семинар по теме «Устойчивое и безопасное развитие сети Интернет» (онлайн, 24 августа с.г.). Во встрече приняли участие эксперты заинтересованных органов государственной власти, деловых кругов и научного сообщества 17 государств-членов СВМДА. Проведен развернутый обмен мнениями по вопросам укрепления международного сотрудничества, регулирования национальных сегментов мировой сети и обеспечения цифрового суверенитета.

Подводя итог, хотелось бы отметить высокий потенциал таких форумов в разработке мер доверия. Более того, их конструктивные наработки в дальнейшем могут использоваться в качестве вклада в работу профильных органов.

Благодарю за внимание.



## Д.Б. Фролов

Советник генерального директора  
ФГУП «Российская телевизионная и  
радиовещательная сеть» (РТРС), зав.  
базовой кафедрой РТРС «Цифровое  
телерадиовещание и информационная  
безопасность» ИПК МТУСИ

### ДИПФЕЙКИ И ВОПРОСЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В МЕЖДУНАРОДНОМ И РЕГИОНАЛЬНОМ АСПЕКТАХ

Информационное противоборство в условиях жестких санкций со стороны западных государств и в условиях проведения специальной военной операции на Украине сопровождается усилением дезинформационной составляющей и информационного воздействия на мировое сообщество. Цель — создать видимость и особую виртуальную реальность, где Россия выглядит агрессором, попирающим общечеловеческий ценности. Об этом свидетельствует большое количество провокаций, сопровождаемых бесчисленным множеством фейков. Учитывая современную возможность использования новых цифровых технологий, в качестве элементов информационного оружия, по нашему мнению, особую опасность в этой связи представляет технология дипфейков.

Термин «дипфейк» пришел в нашу жизнь сравнительно недавно и состоит из двух англоязычных терминов «deep learning» («глубокое обучение») и «fake» («подделка»). В совокупности это означает, что дипфейк — искусственный контент, созданный с помощью компьютера (искусственного интеллекта), в котором человек в существующем фото и видеоряде или аудиоряде подменяется на другого, либо совершает смоделированные искусственным интеллектом действия, которые он не совершал.

Начавшись как некая забава (программы для создания забавных аватарок и шуток над друзьями), дипфейки стали рассматриваться как элемент информационного воздействия, который позволяет эффективно транслировать «нужное» мнение или высказывания, якобы от имени лиц, имеющих влияние на аудиторию. В зависимости от аудитории, это могут быть политики, блогеры, известные медиа-личности.



Примером дипфейка, созданном для развлечения, может служить стихотворение «Пожалейте бедного пародиста» актера Джима Мескимена (<https://www.youtube.com/watch?v=5rPKeUXjEvE>) — в этом видеоролике актер читает стихотворение в 20 лицах сразу. Также данная технология нашла применение в кинематографе и в других отраслях медиаиндустрии, в том числе — в информационных войнах, в качестве дезинформации или фейков.

Как элемент информационного оружия, если рассматривать этот термин кратко и не углубляться в детали — это манипулирование информацией (либо источниками информации), в данном случае — целевой аудитории, что позволяет сформировать определенное мнение, не давая ей (аудитории) понять, что производится манипуляция. Соответственно, дипфейк — это технология мощного информационного воздействия, которая имитирует доверенный для целевой аудитории источник, что позволяет отключить (или значительно снизить) порог критического восприятия информации.

В случае, если дипфейк распространяется (осознанно или неосознанно) различными СМИ либо блогерами, имеющими массовую аудиторию (т.н. «инфлюенсеры»), то данная информация распространяется подобно кругам на воде: могут иметь место массовые перепечатки (репосты), их будет тем боль-

ше, чем авторитетней для целевой аудитории источник и те, кто его репостят.

Следует отметить, что несмотря на то, что первичная информация, распространяемая в СМИ и телекоммуникационных сетях (в данном случае дипфейк) обладает, как правило, высокими показателями цитируемости, то опровержения, как правило, имеют противоположный вектор.

Дипфейки обычно создаются с помощью специализированных программ, в последнее время набрала популярность библиотека DeepFaceLab (<https://github.com/iperov/DeepFaceLab>), в отношении которой автор прямо указывает, что с помощью этой библиотеки можно делать дипфейки политиков, а также приводит примеры таких дипфейков. К подобным программам можно отнести различное ПО для смартфонов, наподобие Reface, но они дают значительно худший результат с точки зрения информационного восприятия, поскольку выполняются на сравнительно маломощных устройствах и не обладают достаточным временем на проведение качественного обучения модели. Такие дипфейки зачастую легко вычисляются даже неподготовленным человеком.

Пока что ни одна специализированная программа на текущий момент не в состоянии выдать сразу же готовую модель качественного дипфейка, везде требуется затратить какое-то количество человеко-часов, чтобы привести в порядок полученную модель.

В целом, хочу подчеркнуть, все необходимые инструменты для создания лежат в открытом доступе и качество дипфейка будет напрямую зависеть от профессионализма его создателя.

После создания дипфейка необходимо его распространить. Это может достигаться разными путями.

Первый, и самый очевидный путь: распространить его через различные протестные группы в соцсетях и мессенджерах, используя блогеров.

Второй вариант — использовать блогера или СМИ «втемную», воспользовавшись тем, что в погоне за «горячей новостью» должный фактчекинг (проверка изложенных фактов) проведен не будет.

Третий вариант, наиболее сложный: это непосредственно компьютерная атака на

стриминговую платформу вещания или студию, которая производит контент.

Это становится возможным в силу того факта, что кибербезопасность таких платформ зачастую обеспечивается ненадлежащим образом, что создает предпосылки для мотивированных атакующих попыток получить несанкционированный доступ к ней. Пример — атака неустановленных лиц на стриминговые платформы и запуска на них проукраинского контента во время проведения специальной операции в феврале-марте 2022 г. Указанная атака была малоуспешной, поскольку ответственные лица быстро вычислили подмену контента, но в случае, если бы там был дипфейк — подмену сразу могли бы и не заметить. Аналогичным образом может быть атакована и студия вещания: получен несанкционированный доступ и подменен видеофайл, который транслируется в сторону операторов.

В этом случае эффект может быть наиболее максимальный, поскольку сообщение получит по официальным каналам большое число пользователей, а дальнейшее опровержение может не возыметь должного эффекта.

В наш век происходит быстрое развитие «интернета вещей», к которым относятся, в частности, умные телевизоры (смарт-тв). Поэтому не обязательно для генерации фейк-ньюс и дипфейков взламывать вещателя или телеком-оператора: достаточно взломать смарт-тв, вопросам обеспечения информационной безопасности которого не всегда уделяется должное внимание, после чего транслировать подмененный контент конкретному абоненту, например, в качестве шутки, или целенаправленно, как дискредитацию конкретной личности.

В настоящее время данные технологии находятся на начальной стадии развития и поэтому разрабатывать методики выявления и противодействия возможным дипфейкам в СМИ нужно уже сейчас, не дожидаясь, пока технологии будут настолько совершенны и выйдут в массы, что придется долго находиться в позиции догоняющих.

По нашему мнению, сейчас легко можно выявить дипфейк только в случае распространения через протестные группы в социальных сетях и мессенджерах. Во всех остальных случаях зафиксировать и остановить дипфейк

так сказать «на лету» технической возможности нет. Можно только провести анализ инцидента и доказать, что это дипфейк, в частности, опираясь на:

- Погрешности монтажа видео
- Отсутствие отражений / несовпадение отражений на зеркальных предметах
- Явные наложения изображений, пропадание изображений
- Несоответствие освещения объекта и основной сцены

В более сложных случаях требуется уже проведение экспертизы, которая способна установить подделку видео на основе иных технических методик.

Каковы же перспективы? Мы будем видеть дальнейшее увеличение и разнообразие числа дипфейков. Это — элементы новых информационных вызовов и воздействий, которые активно и целенаправленно могут использоваться и в технологиях информационных войн. Как следствие, в дальнейшем будут упрощаться инструменты по генерации дипфейков, но одновременно и разовьются методы выявления дипфейков и их нейтрализации. Разумеется, наберут популярность и инструменты

раннего выявления дипфейков. Не за горами и создание национальных систем мониторинга, возможно, это будет реализовано на базе крупных государственных вещательных корпораций.

Однако, стоит отметить, что для эффективной борьбы со стремительно развивающейся индустрией подделок, кроме отдельных усилий уважаемых, проверенных изданий, кроме отдельных интересных специализированных разработок, применимых на практике, требуются объединенные усилия всего научно-технического сообщества: вещателей, ученых, инженеров, разработчиков современных методов обработки контента, создающих стандарты для таких методов. Иными словами, должна быть привлечена не только широкая научно-техническая аудитория, но и специалисты гуманитарного профиля в сфере информационного противоборства. Возможно появление специализированных стандартов, регламентирующих методы и механизмы проверки контента на наличие подделок. Время для подготовки подобных мероприятий уже пришло.

## В.А. Педанов

Генеральный директор ООО «Технологии безопасности транспорта»,  
представитель Группы компаний  
«Инжиниринговые Технологии» в АСЕАН

### АКТУАЛЬНЫЕ ПРОБЛЕМЫ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В АСЕАН

Новым историческим этапом стало для международного сообщества развитие сотрудничества в сфере МИБ. Появление новых угроз в информационном пространстве способствует развитию международного сотрудничества в сфере обеспечения МИБ, которое является закономерным следствием роста числа угроз в сфере информационно-коммуникационных технологий (далее — ИКТ) и желанием международного сообщества противостоять им. С развитием электронных вычислительных технологий появились риски их злонамеренного использования. В эпоху развития интернета эти риски кратно возросли. Новым глобальным вызовом международному сообществу стало внедрение ИКТ в критическую инфраструктуру и растущая роль кибер-физических процессов. Занимая значительное место в структуре компонентов национальной безопасности, информационная безопасность становится предметом внимания и международного сообщества.

Эффективность групповых систем обеспечения безопасности привлекает внимание государств к решению проблем МИБ в рамках коалиционных инструментов<sup>1</sup>. В виду растущего экономического и политического значения в мире, а также ввиду личных профессиональных интересов авторов, представляется интересным анализ международного сотрудничества в сфере МИБ в рамках региона АСЕАН и его соотношения с российской позицией в международных сообществах. Целью настоящего исследования является анализ опыта сотрудничества стран АСЕАН в сфере МИБ, как ответ на объектив-



но существующую проблематику, а также определение позитивных практик, возможных к рецептированию всем международным сообществом.

Для России особенно значимо развитие взаимодействия со странами АСЕАН по вопросам МИБ. Следует отметить, что отношения России и стран АСЕАН выходят на новый качественный уровень с ноября 2018 года, когда в ежегодном Восточноазиатском саммите впервые принял участие не глава правительства, а Президент России. В ходе визита Президента России был также проведён третий саммит Россия — АСЕАН, результатом которого стало совместное заявление сторон о стратегическом партнёрстве<sup>2</sup>. Интерес представляет то, какое значение было уделено именно вопросам совместной работы над обеспечением международной информационной безопасности. Помимо координации действий в привычных для сторон отраслей сотрудничество (экономическое, военно-промышленные вопросы), стороны достигли ряда договорённостей в сфере ИКТ, а именно:

- 1) укреплять сотрудничество на глобальных и региональных площадках в ре-

1 Бордюжа Н.Н. Эффективность системы коллективной безопасности на евразийском пространстве: реалии и перспективы // Национальные интересы: приоритеты и безопасность. 2006. №6. URL: <https://cyberleninka.ru/article/n/effektivnost-sistemy-kollektivnoy-bezopasnosti-na-evraziyskom-prostranstve-realii-i-perspektivy> [дата обращения: 10.09.2022].

2 Совместное заявление 3-го саммита Российская Федерация-АСЕАН о стратегическом партнёрстве, 14 ноября 2018 года [Электронный ресурс] // Президент России: официальный сайт. URL: <http://kremlin.ru/supplement/5360>. – [дата обращения 10.09.2022]



агировании на традиционные и новые вызовы в сфере безопасности (международный терроризм, транснациональная преступность, угрозы в сфере использования информационно-коммуникационных технологий, незаконное производство и контрабанда наркотиков) (п. 15);

- 2) способствовать реализации Заявления Российской Федерации и АСЕАН о сотрудничестве в области обеспечения безопасности в сфере использования информационно-коммуникационных технологий (ИКТ) и самих ИКТ (п. 16).

Помимо общих договорённостей о стратегическом партнёрстве, отдельно было озвучено Заявление Российской Федерации и АСЕАН о сотрудничестве в области обеспечения безопасности использования ИКТ и самих информационно-коммуникационных технологий. Стороны договорились о ряде конкретных направлений совместной деятельности в сфере ИКТ, а именно:

- 1) активизация совместных усилий по сокращению цифрового разрыва (п. 10);
- 2) наращивание национальных потенциалов и запуск образовательных программ и тренингов по различным вопросам безопасности в сфере использования ИКТ и самих ИКТ (п. 11);
- 3) укрепление практического сотрудничества по безопасности в сфере использования ИКТ и самих ИКТ на таких направлениях, как борьба с использованием ИКТ в террористических целях и для иной преступной деятельности;
- 4) содействие укреплению и оптимизации существующих региональных механизмов по безопасности в сфере использования ИКТ и самих ИКТ (п. 13);
- 5) рассмотрение Ассоциацией государств Юго-Восточной Азии инициативы Российской Федерации об учреждении Ди-

алога Россия – АСЕАН по вопросам, относящимся к безопасности ИКТ (п. 14)<sup>3</sup>.

Государства АСЕАН и Россия достижениям этих договорённостей подтвердили свою заинтересованность в поддержании стабильности и безопасности в сфере МИБ. Однако, реализация практических мер в сфере обеспечения МИБ, несмотря на достигнутые договорённости, не всегда соответствует поставленным целям. Так, в ходе выступления директора Департамента МИБ МИД России А.В. Крутских на специальной сессии Министерской конференции АСЕАН по кибербезопасности V Сингапурской международной кибер-недели 7 октября 2020 года, остро поставил актуальный для развития международного сотрудничества в сфере МИБ вопрос: «почему при наличии значительного числа авторитетных и работающих переговорных форматов мы все никак не можем договориться о создании так называемой вакцины от кибер-пандемии? Затягивается процесс внести хотя бы базовый порядок в набирающий в силу кибер-хаос?»<sup>4</sup>. В ходе выступления А.В. Крутских призывает также «не обольщаться» в связи с достигнутым прогрессом в рамках международного переговорного процесса по вопросу об обеспечении МИБ. В качестве основной проблемы указывается, что сам переговорный процесс заменяется обще концептуальной дискуссией, которая не приводит к существенному прогрессу.

При этом для государств АСЕАН обеспечение международной информационной безопасности представляет высокую значимость прежде всего в связи с активным развитием цифровой экономики в регионе, что стимулирует наращивание регионального сотрудничества между странами в сфере МИБ. Так исследование AT&Kearney ВВП региона может быть увеличено на 35% (1 трлн долларов США) благодаря развитию цифровой экономике в период с 2018 по 2023 год<sup>5</sup>. Ввиду активного развития цифровой экономики и её активного проникновения во

3 Заявление Российской Федерации и АСЕАН о сотрудничестве в области обеспечения безопасности использования информационно-коммуникационных технологий и самих информационно-коммуникационных технологий [Электронный ресурс] // Президент России: официальный сайт. – Режим доступа: <http://kremlin.ru/supplement/5361>. – [дата обращения 10.09.2022].

4 Министерство иностранных дел Российской Федерации. – Выступление специального представителя Президента Российской Федерации по вопросам международного сотрудничества в области информационной безопасности, директора Департамента международной информационной безопасности А.В. Крутских на специальной сессии Министерской конференции АСЕАН по кибербезопасности с диалоговыми партнерами V Сингапурской международной кибер-недели в формате видеоконференции, 7 октября 2020 года. // URL.: [https://www.mid.ru/ru/maps/sg/-/asset\\_publisher/5SAHbSOAdwNc/content/id/4372514](https://www.mid.ru/ru/maps/sg/-/asset_publisher/5SAHbSOAdwNc/content/id/4372514) [дата обращения 12.09.2022].

5 AT&Kearney. Cybersecurity in ASEAN- AN Urgent Call to Action. – 2018 // URL.: [https://www.cisco.com/c/dam/m/en\\_sg/cybersecurity/cybersecurity-inasean/files/assets/common/downloads/publication.pdf](https://www.cisco.com/c/dam/m/en_sg/cybersecurity/cybersecurity-inasean/files/assets/common/downloads/publication.pdf) [дата обращения 15.09.2022].



все сферы жизни общества в странах АСЕАН, эти государства становятся одной из главных мишеней для информационных атак.

В соответствии с отчётом CheckPoint Азиатско-Тихоокеанский регион находится на втором месте в мире по числу кибератак (после Африки): в среднем 1299 атак в неделю на организацию — в 2021 г на 20% выше, чем в 2020 г<sup>6</sup>. В указанном отчёте также отмечается, что в регионе АСЕАН наблюдается наибольшее количество попыток атак программ-вымогателей: в 2021 году каждую неделю им подвергается одна из 34 организаций. Это сочетается также и с тем, что растёт число атак на критическую информационную инфраструктуру и инфраструктуру умных городов.

Причиной этому служит недостаточно развитая система политических институтов в большей части стран, которые не способны, ввиду экономических, технологических и иных факторов, обеспечить должный уровень обеспечения безопасности информационных ресурсов. Сказывается нехватка специалистов в сфере обеспечения кибер-безопасности и отсутствие сильных технологических школ с преемственностью знаний в значительной части региона. Определяющее значение имеет низкий уровень подготовки кадров на местах. Следствием этого является низкий уровень локальных технологий в сфере ИБ. В связи с низким уровнем развития собственных технологий в сфере обеспечения информационной и кибербезопасности, страны АСЕАН имеют высокую зависимость от зарубежных (Китай, Запад) технологических продуктов и средств киберзащиты. Следствием этого является низкая способность реагировать на киберугрозы и инциденты. Так исследование Ponemon Institute, проведённое при поддерж-

ке IBM в 2017 году, показывает, что в среднем для проведения кибер-атаки на критическую инфраструктуру в странах мира требуется порядка 180 дней, а для атак на инфраструктуру компаний в АСЕАН-около 65 дней<sup>7</sup>.

Лидерство в части развития экосистемы обеспечения информационной безопасности, как в вопросах институционального управления, так и в вопросах подготовки кадров, занимает Сингапур<sup>8</sup>. Исторически тесные связи с Израилем — одним из ведущих государств в сфере развития технологий безопасности ИКТ, а также высокий уровень экономического развития и организации политических институтов, дают высокие возможности для развития суверенной программы информационной безопасности. Так Сингапур был первым государством в АСЕАН, кто поднял тему кибер-безопасности на законодательном уровне, опубликовав в 1993 году Акт о компьютерных злоупотреблениях и кибербезопасности (Computer Misuse and Cybersecurity Act 1993)<sup>9</sup>. Помимо этого, Сингапур совместно с Японией и Великобританией создал и поддерживает некоммерческую международную организацию The CyberGreen Institute, одной из ключевых задач которого является улучшение глобального кибер-здоровья (improving global cyber health)<sup>10</sup>.

Стоит отметить, что страны АСЕАН в целом предпринимают последовательные попытки укрепления цифровой экономики, в том числе с развитием международного сотрудничества в сфере МИБ. Целью такого сотрудничества является в том числе и дополнительная стимуляция развития цифровой экономики. Так страны АСЕАН, по инициативе Сингапура приняли и следуют Программе повышения кибер-потенциала АСЕАН<sup>11</sup>. В рамках программы предполагается:

6 Число кибератак в России и в мире . – 11.05.2022 // URL.: [https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%A7%D0%B8%D1%81%D0%BB%D0%BE\\_%D0%BA%D0%B8%D0%B1%D0%B5%D1%80%D0%B0%D1%82%D0%B0%D0%BA\\_%D0%B2\\_%D0%A0%D0%BE%D1%81%D1%81%D0%B8%D0%B8\\_%D0%B8\\_%D0%B2\\_%D0%BC%D0%B8%D1%80%D0%B5#.D0.A0.D0.BE.D1.81.D1.82\\_.D0.BA.D0.B8.D0.B1.D0.B5.D1.80.D0.B0.D1.82.D0.B0.D0.BA\\_.D0.BD.D0.B0.40.25\\_-\\_Check-Point](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%A7%D0%B8%D1%81%D0%BB%D0%BE_%D0%BA%D0%B8%D0%B1%D0%B5%D1%80%D0%B0%D1%82%D0%B0%D0%BA_%D0%B2_%D0%A0%D0%BE%D1%81%D1%81%D0%B8%D0%B8_%D0%B8_%D0%B2_%D0%BC%D0%B8%D1%80%D0%B5#.D0.A0.D0.BE.D1.81.D1.82_.D0.BA.D0.B8.D0.B1.D0.B5.D1.80.D0.B0.D1.82.D0.B0.D0.BA_.D0.BD.D0.B0.40.25_-_Check-Point) [дата обращения 15.09.2022].

7 Ponemon Institute. Cost of Data Breach Study: Global Overview. – Benchmark research sponsored by IBM Security Independently conducted by Ponemon Institute LLC. – 2017 // URL.: <http://universe.byu.edu/wpcontent/uploads/2017/10/Ponemon-2017-Study.pdf> [дата обращения 15.09.2022].

8 Горян Э.В. Ведущая роль Сингапура в обеспечении кибербезопасности в АСЕАН: промежуточные результаты и перспективы дальнейшего расширения // Территория новых возможностей. Вестник Владивостокского государственного университета экономики и сервиса. 2018. Т. 10. № 3. С. 103–117.

9 Singapore status online. – Computer Misuse and Cybersecurity Act // URL.: <https://sso.agc.gov.sg/Act/CMA1993> [дата обращения 15.09.2022].

10 CyberGreen Institute. – // URL.: <https://www.cybergreen.net> [дата обращения 15.09.2022].

11 Interpol – ASEAN Cyber Capacity Development Project // URL.: <https://www.interpol.int/en/Crimes/Cybercrime/Cyber-capabilities-development/ASEAN-Cyber-Capacity-Development-Project> [дата обращения 15.09.2022].

- Разработка Руководства по Стратегии борьбы с киберпреступностью, которое призвано помочь странам АСЕАН разработать или усовершенствовать свои национальные стратегии борьбы с киберпреступностью, что в свою очередь должно привести к более эффективному противодействию киберпреступности;
- Проведение специализированных семинаров и тренингов, основанных на тенденциях в сфере киберпреступности для устранения пробелов в знаниях сотрудников уполномоченных органов, выявленных на предыдущем этапе;
- Создание модулей онлайн-обучения для сотрудников национальных CERT стран АСЕАН по сбору и сохранению цифровых улик.

Таким образом, мы можем видеть, как документы политического характера находят своё практическое применение в рамках реализации договорённостей и развития международного сотрудничества в сфере МИБ<sup>12</sup>.

Существенным шагом вперёд стало принятие странами АСЕАН совместной программы действий в сфере МИБ — ASEAN Cybersecurity Cooperation Strategy 2021–2025<sup>13</sup>, которая была опубликована 17-го февраля 2022 года. Этот документ является дополнением к опубликованному ранее документу по цифровизации региона в целом — ASEAN Digital Masterplan 2025. В документе отмечается изменение ландшафта информационной безопасности в целом:

- Несмотря на COVID продолжается цифровизация — в регионе отмечается 125,000 новых интернет-пользователей каждый день;
- Инфраструктура «Умных городов» стран АСЕАН сталкивается с вызовами в киберпространстве, как и вся КИИ в целом;
- Киберпреступность и государственные хакеры третьих стран — могут являться вызовом для концепции «Умных наций»;
- Отмечается, что усложняющиеся кибер-атаки оказывают негативное влия-

ние на региональную и международную стабильности, а также неизбежно несут вред мирным гражданам.

В качестве ответов на обозначенную проблематику Стратегия Кооперации предлагает следующие практические шаги, призванные укрепить МИБ в регионе:

- Создание ASEAN Cybersecurity Committee;
- Подготовка к запуску ASEAN CERT;
- Отмечаются ограниченные возможности государства в обеспечении безопасности информационного пространства и указывается на необходимость стимуляции развития частного бизнеса и промышленности для повышения их кибер устойчивости;
- Указывается необходимость наращивания и развития международного сотрудничества в рамках Партнёрских Диалогов (как например существующий формат двухстороннего партнёрского диалога с Российской Федерацией).

В целом, по итогам обзора данного документа формируется устойчивое ощущение того, что странами АСЕАН, сформировано видение существующей проблематики и изложена концепция кооперации, которая может позволить найти оптимальные ответы на существующие угрозы.

Помимо сотрудничества на региональном уровне, страны АСЕАН выступают активным участником международного сотрудничества. Так страны АСЕАН, ведут активную работу по совершенствованию своих взаимоотношений в сфере МИБ с ключевыми акторами в сфере международной информационной безопасности.

Так сотрудничество в сфере обеспечения информационной безопасности с одним из наиболее значимых для АСЕАН партнёром — Китаем, было начато ещё в 2005 году, с принятием Пекинской декларации о сотрудничестве АСЕАН и Китая в области ИКТ в интересах общего развития<sup>14</sup>. В рамках этой декларации признавалось, что сетевая и информационная

12 Interpol – ASEAN Cyber Capacity Development Project. – Interpol's web page // URL.: <https://www.interpol.int/en/Crimes/Cybercrime/Cyber-capabilities-development/ASEAN-Cyber-Capacity-Development-Project> [дата обращения 15.09.2022].

13 ASEAN CYBERSECURITY COOPERATION STRATEGY (2021 – 2025): // URL.: [https://asean.org/wp-content/uploads/2022/02/01-ASEAN-Cybersecurity-Cooperation-Paper-2021-2025\\_final-23-0122.pdf](https://asean.org/wp-content/uploads/2022/02/01-ASEAN-Cybersecurity-Cooperation-Paper-2021-2025_final-23-0122.pdf) [дата обращения 16.09.2022].

14 Beijing Declaration on ASEAN-China ICT Cooperative Partnership for Common Development Beijing. – ASEAN web page // URL.: <https://asean.org/beijing-declaration-on-asean-china-ict-cooperative-partnership-for-common-development-beijing/> [дата обращения 16.09.2022].

безопасность является важным компонентом информационного общества и при этом регион сталкивается с серьезной проблемой обеспечения такой безопасности. Стороны соглашаются на том, что они должны укреплять связь и сотрудничество в области сетевой и информационной безопасности, а также стремиться к созданию Координационных организаций АСЕАН–Китай для реагирования на чрезвычайные ситуации в области сетевой и информационной безопасности. Интерес вызывает, что в этом документе не поднимаются вопросы кибербезопасности, а подчеркивается важность работы над обеспечением именно информационной безопасности.

Рассматривая более поздние документы по вопросам сотрудничества в части обеспечения безопасности в сфере ИКТ, необходимо обратить внимание на План действий по имплементации Совместной Декларации АСЕАН–Китай — Стратегическое Партнёрство для Мира и Процветания 2016–2020<sup>15</sup>, утверждённого по итогам Саммита АСЕАН–Китай 2016 года. В этом документе действия по имплементации договорённостей рассматриваются в контексте широкого ряда соглашений на уровне АСЕАН–Китай, включая такие сферы как: торговля, финансы, управление природными ресурсами, транспорт, сотрудничество в сфере науки и космоса, туризм и ИКТ и так далее. Применительно к сфере ИКТ Китай и АСЕАН договорились:

- Продолжать укреплять политический диалог через Совецание министров ИКТ АСЕАН и Китая;
- Продолжать осуществление Меморандума о взаимопонимании между АСЕАН и Китаем о сотрудничестве в области информационно-коммуникационных технологий и Плана действий по осуществлению Пекинской декларации о сотрудничестве АСЕАН и Китая в области ИКТ в интересах общего развития.
- Реализовать Механизм сотрудничества групп реагирования на компьютерные

чрезвычайные инциденты (CERT) между АСЕАН и Китаем, оптимизировать меры реагирования и процедуры в области сетевой безопасности, содействовать обмену информацией и данными, а также осуществлять наращивание потенциала и проектное сотрудничество.

- Продолжать совместную работу по улучшению взаимодействия информационно-коммуникационной инфраструктуры АСЕАН и Китая.
- Укреплять сотрудничество в области развития сельских телекоммуникаций, расширения сетевых приложений и развития приложений электронной торговли.
- Поддерживать реализации Генерального плана АСЕАН в области ИКТ на 2020 год<sup>16</sup>.

На основе перечисленных в Плате задач можно сделать вывод, что сотрудничество в сфере МИБ между Китаем и АСЕАН уже имеет продолжительную историю и находит своё практическое применение в рамках реализации совместных CERT команд и обмена данными об инцидентах информационной безопасности.

Помимо сотрудничества с Китаем, АСЕАН также развивает сотрудничество с США в сфере МИБ. Так в рамках 6-го саммита АСЕАН–США 2018 году, лидеры АСЕАН и США приняли совместное Заявление о сотрудничестве в сфере кибербезопасности<sup>17</sup>. Стороны подтвердили, что, по их мнению, международное право, и, в частности, Устав ООН, применимо и имеет важное значение для поддержания мира, стабильности и содействия созданию открытой, безопасной, стабильной, доступной и мирной среды ИКТ, и признают необходимость дальнейшего изучения того, как международное право применяется к использованию ИКТ государствами. Стороны также договорились наращивать кибернетический потенциал в борьбе с киберпреступностью, защитой критической информационной инфраструктуры, также, отдельно были

15 Plan of Action to Implement the Joint Declaration on ASEAN-China Strategic Partnership for Peace and Prosperity. – ASEAN web page // URL.: <https://www.asean.org/storage/images/2015/November/27th-summit/ASEAN-China%20POA%20%202016-2020.pdf> [дата обращения 16.09.2022]

16 Plan of Action to Implement the Joint Declaration on ASEAN-China Strategic Partnership for Peace and Prosperity. – ASEAN web page // URL.: <https://www.asean.org/storage/images/2015/November/27th-summit/ASEAN-China%20POA%20%202016-2020.pdf> [дата обращения 16.09.2022].

17 ASEAN – United States leaders' statement on cybersecurity cooperation. – ASEAN web page // URL.: <https://asean.org/storage/2018/11/ASEAN-US-Leaders-Statement-on-Cybersecurity-Cooperation-Final.pdf> [дата обращения 21.09.2022].

выделены тезисы о необходимости совместного противодействия использованию ИКТ в террористических целях. Высокую значимость также имеет пункт, в котором стороны договариваются совместно принимать меры по экономическому развитию цифровой инфраструктуры, с задействованием рыночных механизмов. Реализация договорённостей политического характера на посредством инструментов рыночной экономики, должна способствовать их эффективной имплементации и повышению взаимозависимости договаривающихся сторон друг от друга.

Всё более значимым становится сотрудничество АСЕАН и с другим региональным лидером — Японией. Сотрудничество между АСЕАН и Японией наименее конфликтно и высоко институализировано, что обуславливает потенциал дальнейшего политико-экономического развития, в том числе с внешними игроками<sup>18</sup>. Сотрудничество Японии и АСЕАН в сфере МИБ с 2009 года находит своё выражение в проведении ежегодных конференций по вопросам политики в области кибербезопасности. Так 20 октября 2020 г. была проведена 13-я Конференция Японии/стран АСЕАН по вопросам политики в области кибербезопасности<sup>19</sup>. В ходе прошедшей встречи стороны подтвердили намерения о проведении таких совместных мероприятий, как кибер-учения, взаимное повышение осведомленности, наращивание кибер-потенциала и взаимное уведомление об инцидентах информационной безопасности. Также, отмечается запуск в 2020-м году совместного центра между АСЕАН и Японией для развития сотрудничества в сфере кибербезопасности — The ASEAN-Japan Cybersecurity Capacity Building Centre (AJCC BC)<sup>20</sup>. Сотрудничество для развития взаимного потенциала в сфере обеспечения кибербезопасности и обеспечения МИБ ведётся на различных уровнях, включая взаимодействие на правительственном уровне, взаимодействие в академических кругах, а также на уровне частных корпораций и промышленности.

Анализируя актуальную проблематику в сфере МИБ, стоящую перед странами АСЕАН, следует отметить взвешенный подход, основанный на рациональной оценке существующих вызовов и путей их решения. Отмечая в качестве одной из ключевых проблем дефицит кадров и нехватку компетенций и технологий, страны АСЕАН открыты к сотрудничеству со всеми участниками международных отношений и трезво оценивают перспективы сотрудничества с каждым из них. В этой связи, оценивая развитие международного сотрудничества АСЕАН с другими региональными лидерами, складывается впечатление о недостаточности мер, предпринимаемых Россией в вопросах практической реализации договорённостей в сфере МИБ. Отсутствием совместных центров реагирования на инциденты информационной безопасности, низкий уровень взаимного проникновения на рынки частных компаний, работающих в сфере обеспечения информационной безопасности, а также, отсутствие непрерывного институционализированного диалога между Россией и АСЕАН именно по вопросам МИБ, на текущий момент, негативно сказывается на практической реализации договорённостей политического характера.

Безусловно, сотрудничество в сфере МИБ между Россией и странами АСЕАН поступательно развивается. Подтверждением этому служат перечисленные в начале работы договорённости и участие России в специальных сессиях Министерской конференции АСЕАН по кибербезопасности. Вопросы сотрудничества в сфере безопасности ИКТ поднимаются и в рамках других форматов. К примеру, 30 марта 2021 года состоялась 19-е Заседание Совместного Комитета Сотрудничества Россия-АСЕАН, по вопросам развития Стратегического партнерства Россия-АСЕАН. В ходе встречи обсуждался широкий перечень вопросов, в том числе развитие сотрудничества по политическим вопросам и вопросам безопасности, в области борьбы со стихийными бедствиями, технологий и инноваций, безо-

18 Н. Мурашкин. — Япония — АСЕАН: неизбежное партнерство для нового азиатского порядка? // РСДМ Электронный ресурс. // URL: <https://russiancouncil.ru/analytics-and-comments/analytics/yaponiya-asean-neizbezhnoe-partnerstvo-dlya-novogo-aziatkog/> [дата обращения 12.09.2022].

19 Министерство по внутренним вопросам и связям, Япония. — Итоги 13-й конференции АСЕАН по политике в области кибербезопасности. — Пресс-релиз 6 ноября 2020 г. // URL: [https://www.soumu.go.jp/main\\_sosiki/joho\\_tsusin/rus/pressrelease/2020/11/06\\_01.html](https://www.soumu.go.jp/main_sosiki/joho_tsusin/rus/pressrelease/2020/11/06_01.html) [дата обращения 12.09.2022].

20 The ASEAN-Japan Cybersecurity Capacity Building Centre (AJCC BC) // URL: <https://www.ajccbc.org/> [дата обращения 12.09.2022].



пасности ИКТ, борьбы с инфекционными заболеваниями, туризма и во многих других областях<sup>21</sup>. Однако, в сравнении с тем уровнем сотрудничества в сфере безопасности ИКТ, который существует по осям АСЕАН-Китай или АСЕАН-Япония, Россия несколько уступает. Во многом это связано с относительно низкой степенью развитости торгово-экономических взаимоотношений между странами АСЕАН и Россией.

Представляется, что для дальнейшего развития сотрудничества по вопросам безопасности ИКТ, Россия должна проводить скоординированную политику поддержки диалога Россия-АСЕАН по вопросам международной информационной безопасности, с привлечением представителей частного бизнеса и академической среды. Среди практических шагов, для развития и реализации договорённостей в сфере МИБ видится необходимым создание механизмов сотрудничества групп реагирования на компьютерные чрезвычайные инциденты (CERT) между АСЕАН и России, взаимное информирование об инцидентах информационной безопасности, а также взаимное повышение осведомлённости об инцидентах.

Стоит отметить вызывающее одобрение стремление стран АСЕАН к обеспечению международной информационной безопасности, которое находит практическое выражение в активном развитии международного сотрудничества по этому вопросу. Среди стран, с которыми АСЕАН активно наращивает сотрудничество в этой сфере можно выделить Китай, Россию, Японию, страны Коллективного Запада и Ближнего Востока. Развитием двухсторонних отношений, а также отношений на региональном уровне имеет высокое значение для формирования атмосферы взаимного доверия между государствами в сфере ИКТ, что в свою очередь способствует позитивному развитию международного сотрудничества в сфере МИБ.

Роль АСЕАН в этом процессе становится всё заметнее и для России особенно важно обеспечить надёжное и эффективное сотрудничество с государствами АСЕАН по вопросам МИБ.

В качестве актуальных направлений для развития сотрудничества в сфере МИБ между Россией и АСЕАН стоит выделить наращивание торгово-экономических связей в сфере ИКТ, обмена информацией по актуальным инцидентам информационной безопасности, которое может выражаться в обмене данными между ГосСОПКА<sup>22</sup> и CERT-командами стран АСЕАН. Актуальным примером является существующий на сегодняшний день The CyberGreen Institute, к работе которого Россия могла бы присоединиться или же создать аналогичную организацию вместе с государствами АСЕАН. На наш взгляд, именно увеличение экономической взаимосвязи и обмен актуальными данными между государственными организациями, нацеленными на обеспечение информационной безопасности, поможет реализовывать сотрудничество на практическом уровне.

## Библиография

1. ASEAN CYBERSECURITY COOPERATION STRATEGY (2021–2025): [Электронный ресурс] // URL.: [https://asean.org/wp-content/uploads/2022/02/01-ASEAN-Cybersecurity-Cooperation-Paper-2021-2025\\_final-23-0122.pdf](https://asean.org/wp-content/uploads/2022/02/01-ASEAN-Cybersecurity-Cooperation-Paper-2021-2025_final-23-0122.pdf)
2. ASEAN—United States leaders' statement on cybersecurity cooperation. — ASEAN [Электронный ресурс] // URL.: <https://asean.org/storage/2018/11/ASEAN-US-Leaders-Statement-on-Cybersecurity-Cooperation-Final.pdf/>;
3. ASEAN-Japan Cybersecurity Capacity Building Centre (AJCC BC) [Электронный ресурс] // URL. <https://www.ajccbc.org/>
4. AT&T. Cybersecurity in ASEAN- AN Urgent Call to Action. — 2018 [Электронный ресурс] // URL.: [https://www.cisco.com/c/dam/m/en\\_sg/cybersecurity/cybersecurity-inasean/files/assets/common/downloads/publication.pdf/](https://www.cisco.com/c/dam/m/en_sg/cybersecurity/cybersecurity-inasean/files/assets/common/downloads/publication.pdf/);
5. Beijing Declaration on ASEAN-China ICT Cooperative Partnership for Common Development Beijing. — ASEAN [Электронный ресурс] // URL.: <https://asean.org/>

21 On The 19th ASEAN-Russia Joint Cooperation Committee Meeting Press-Release. – March 30th, 2021, ASEAN Secretariat News // URL.: <https://asean.org/19th-asean-russia-joint-cooperation-committee-meeting-press-release/> [дата обращения 01.09.2022]

22 Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак – [www.gov-cert.ru/](http://www.gov-cert.ru/) [дата обращения 20.09.2022]



- org/beijing-declaration-on-asean-china-ict-cooperative-partnership-for-common-development-beijing/;
6. <https://www.tadviser.ru> ;
  7. Interpol — ASEAN Cyber Capacity Development Project [Электронный ресурс] // URL.: <https://www.interpol.int/en/Crimes/Cybercrime/Cyber-capabilities-development/ASEAN-Cyber-Capacity-Development-Project/>;
  8. On The 19th ASEAN-Russia Joint Cooperation Committee Meeting Press-Release. — March 30th, 2021, ASEAN Secretariat News [Электронный ресурс] // URL.: <https://asean.org/19th-asean-russia-joint-cooperation-committee-meeting-press-release/>;
  9. Plan of Action to Implement the Joint Declaration on ASEAN-China Strategic Partnership for Peace and Prosperity. — ASEAN [Электронный ресурс] // URL.: <https://www.asean.org/storage/images/2015/November/27th-summit/ASEAN-China%20POA%20%202016-2020.pdf/>;
  10. Plan of Action to Implement the Joint Declaration on ASEAN-China Strategic Partnership for Peace and Prosperity. — ASEAN [Электронный ресурс] // URL.: <https://www.asean.org/storage/images/2015/November/27th-summit/ASEAN-China%20POA%20%202016-2020.pdf/>;
  11. Ponemon Institute. Cost of Data Breach Study: Global Overview. — Benchmark research sponsored by IBM Security Independently conducted by Ponemon Institute LLC. — 2017 [Электронный ресурс] // URL.: <http://universe.byu.edu/wpcontent/uploads/2017/10/Ponemon-2017-Study.pdf/>;
  12. Singapore status online. — Computer Misuse and Cybersecurity Act [Электронный ресурс] // URL.: <https://sso.agc.gov.sg/Act/CMA1993/>;
  13. Бордюжа Н.Н. Эффективность системы коллективной безопасности на евразийском пространстве: реалии и перспективы. — Национальные интересы: приоритеты и безопасность. 2006. №6. [Электронный ресурс] // URL: <https://cyberleninka.ru/article/n/effektivnost-sistemy-kollektivnoy-bezopasnosti-na-evraziyskom-prostranstve-realii-i-perspektivy/>;
  14. Горян Э.В. Ведущая роль Сингапура в обеспечении кибербезопасности в АСЕАН: промежуточные результаты и перспективы дальнейшего расширения // Территория новых возможностей. Вестник Владивостокского государственного университета экономики и сервиса. 2018. Т. 10. № 3. С. 103–117;
  15. Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак [Электронный ресурс] // URL.: [www.gov-cert.ru/](http://www.gov-cert.ru/);
  16. Заявление Российской Федерации и АСЕАН о сотрудничестве в области обеспечения безопасности использования информационно-коммуникационных технологий и самих информационно-коммуникационных технологий [Электронный ресурс] // Президент России: официальный сайт. — URL.: <http://kremlin.ru/supplement/5361/>;
  17. Министерство иностранных дел Российской Федерации. — Выступление специального представителя Президента Российской Федерации по вопросам международного сотрудничества в области информационной безопасности, директора Департамента международной информационной безопасности А.В.Крутских на специальной сессии Министерской конференции АСЕАН по кибербезопасности с диалоговыми партнерами V Сингапурской международной кибер-недели в формате видеоконференции, 7 октября 2020 года. [Электронный ресурс] // URL.: [https://www.mid.ru/ru/maps/sg/-/asset\\_publisher/5SAHbSOAdwNc/content/id/4372514/](https://www.mid.ru/ru/maps/sg/-/asset_publisher/5SAHbSOAdwNc/content/id/4372514/);
  18. Министерство по внутренним вопросам и связям, Япония. — Итоги 13-й конференции АСЕАН по политике в области кибербезопасности. — Пресс-релиз 6 ноября 2020 г. [Электронный ресурс] // URL.: [https://www.soumu.go.jp/main\\_sosiki/joho\\_tsusin/rus/pressrelease/2020/11/06\\_01.html](https://www.soumu.go.jp/main_sosiki/joho_tsusin/rus/pressrelease/2020/11/06_01.html);
  19. Мурашкин Н.А. — Япония — АСЕАН: неизбежное партнерство для но-

вого азиатского порядка? // РСДМ [Электронный ресурс] // URL: <https://russiancouncil.ru/analytics-and-comments/analytics/yaponiya-asean-neizbezhnoe-partnerstvo-dlya-novogo-aziatskog/>;

20. См.: Interpol – ASEAN Cyber Capacity Development Project.–Interpol’s webpage [Электронный ресурс] // URL.: <https://www.interpol.int/en/Crimes/Cybercrime/Cyber-capabilities-development/ASEAN-Cyber-Capacity-Development-Project/>;

21. Совместное заявление 3-го саммита Российская Федерация-АСЕАН о стратегическом партнёрстве, 14 ноября 2018 года [Электронный ресурс] // Президент России: официальный сайт. URL: <http://kremlin.ru/supplement/5360/>.

## А.Ж. Мартиросян

Научный сотрудник Института актуальных международных проблем, аспирант Дипломатической академии МИД России, руководитель Школы международной информационной безопасности Дипломатической академии

### РЕГИОНАЛИЗАЦИЯ КАК ТЕНДЕНЦИЯ ФОРМИРУЮЩЕЙСЯ СИСТЕМЫ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Добрый день, уважаемые коллеги! Прежде, чем начать свое выступление хотелось бы поблагодарить НАМИБ за предоставленную возможность выступать сегодня, а также за сотрудничество со Школой международной информационной безопасности и доверие к нашей команде.

Актуальность тематики моего выступления обусловлена множеством факторов, о которых говорили мои коллеги на протяжении 3-х дней, один из которых заключается в том, что обеспечение и достижение информационной безопасности в ее широком понимании с учетом особенностей ИКТ-среды — это глобальная проблема и задача безопасности для государств в условиях цифровой эпохи. На мой взгляд, процесс формирования глобальной системы международной информационной безопасности проходит сейчас этап разработки региональных подходов, так примером может стать регулирование глобальной сети Интернет, которая сейчас превращается во множество локальных сетей.

Примечательно, что усилия российско-китайского «киберальянса» существенно меняют парадигму государственного контроля над информационным пространством, поскольку растет число сторонников данной идеи. Их усилия, наряду с внешними факторами, к которым можно отнести также пандемию коронавирусной инфекции (COVID-19), которая актуализировала необходимость технологического суверенитета, и неконтролируемое поведение растущих крупных Интернет-компаний, особенно GAFAM<sup>1</sup>, побудили Европейский Союз задуматься о своей цифровой экосистеме с целью укрепления стратегической



автономии Европы в ИКТ-среде, последние законодательные инициативы тому доказательство.

Обращаясь к глобальному взаимодействию, важно отметить, что несмотря на наличие некоторых успехов в 2021 г. в области международной информационной безопасности, события конца 2021 г. и первой половины 2022 г. значительно повлияли на эволюцию переговорного процесса, внося деструктивные изменения. Основополагающим негативным последствием этого стал тот факт, что актуализировалась фундаментальная проблема для формирования единой системы обеспечения международной информационной безопасности — отсутствие четко выстроенной институциональной системы. Это, в свою очередь, обуславливает появление различных механизмов, которые в перспективе могут иметь негативные последствия. Так, например, активизировались инициативы, направленные на препятствование формированию единой системы обеспечения международной информационной безопасности, доказательством чему опять же служат события вокруг Интернет-новости. В ходе «Саммита за демократию»<sup>2</sup> США выступили с предложением о создании Альянса за будущее Интернета, пусть пока не реализованного, однако он рассматривается

<sup>1</sup> Meta Platforms признана в России экстремистской организацией и запрещена.

<sup>2</sup> 28 апреля 2022 г. была подписана Декларация о будущем Интернета, в которой также прослеживается антироссийская и антикитайская риторика.

в качестве противодействия появлению «альтернативного видения глобальной сети в качестве инструмента государственного контроля»<sup>3</sup>. В данном контексте важно подчеркнуть, что возможное создание объединения с антироссийским и антикитайским уклоном может повлечь дальнейшее приостановление переговорного процесса в части регулирования, которое будет касаться Интернета<sup>4</sup>. Мы станем свидетелями того, что «фактически закладываются основы для создания цифрового альянса наподобие НАТО»<sup>5</sup>, открыто направленного на противодействие России и Китаю, что подрывает основополагающий принцип международного права обеспечение мирного и плодотворного сотрудничества государств при соблюдении баланса их интересов<sup>6</sup>. Его создание также рассматривается в контексте фрагментации Интернета.

На фоне этого ожидается дальнейшая активизация регионального формата взаимодействия государств по информационной проблематике и выработка норм именно на этом уровне.

Итак, регионализация системы обеспечения международной информационной безопасности и фрагментация норм междуна-

родного права, с одной стороны, отражают центристские силы по отношению к выработке международно-правовых норм, а с другой, и центробежные силы в части отдаления от системы выработки норм на глобальном уровне.

Иерархия системы обеспечения международной информационной безопасности должна быть выстроена по оси двустороннее региональное многостороннее глобальное сотрудничество. Региональный уровень сотрудничества может в перспективе трансформироваться как в фактор прогрессивного развития, так и в вызов для международного права и международных отношений, поскольку может повлечь их фрагментацию. Так увеличится число не универсальных норм, а применимых только на региональном уровне, с одной стороны. Однако, с другой стороны, могут быть сформированы специализированные правовые режимы, способствующие прогрессивному развитию международного права. В связи с чем, на мой взгляд, региональный уровень сотрудничества также может стать фундаментом для нахождения точек соприкосновения на глобальном уровне.

Спасибо за внимание!

3 Handelsblatt (Германия): «саммитом за демократию» Байден расколол мир. 10 декабря 2021 г. URL: [inosmi.ru/20211210/251102728.html/](https://inosmi.ru/20211210/251102728.html/) (Дата обращения: 05.09.2022).

4 Мартиросян А.Ж. Международная информационная безопасность: некоторые итоги 2021 г. и политический контекст 2022 г./ Интернет сегодня и завтра. Сборник авторских статей к Двенадцатому российскому форуму по управлению Интернетом (RIGF 2022), 28-29 сентября 2022 г..АНО Центр глобальной ИТ-кооперации.

5 Егоров И. Совбез РФ: США закладывают основы для создания цифрового альянса наподобие НАТО. 12 декабря 2021 г. URL: [rg.ru/2021/12/12/sovbez-rf-ssha-zakladyvaiut-osnovy-dlia-sozdaniia-cifrovogo-aliansa-napodobie-nato.html/](https://rg.ru/2021/12/12/sovbez-rf-ssha-zakladyvaiut-osnovy-dlia-sozdaniia-cifrovogo-aliansa-napodobie-nato.html/) (Дата обращения: 05.09.2022).

6 Мартиросян А.Ж. Международная информационная безопасность: некоторые итоги 2021 г. и политический контекст 2022 г./ Интернет сегодня и завтра. Сборник авторских статей к Двенадцатому российскому форуму по управлению Интернетом (RIGF 2022), 28-29 сентября 2022 г..АНО Центр глобальной ИТ-кооперации.

## И.В. Сурма

*к.э.н., заведующий кафедрой  
государственного управления во  
внешнеполитической деятельности  
Дипломатической академии МИД России,  
член-корреспондент РАН,  
член экспертно-консультационного  
совета СФ РФ*

### **«ЦИФРОВОЙ РЕАЛИЗМ» И ПОСТНЕОКОЛОНИАЛИЗМ: ПЕРСПЕКТИВЫ И ВЫЗОВЫ СУВЕРЕНИТЕТУ ГОСУДАРСТВА**

Подводя итоги последнего саммита НАТО в Мадриде в июне этого года и рассматривая новую Стратегическую концепцию блока, следует констатировать тот факт, что она кардинально отличается от седьмой версии 2010 г, когда в условиях мира и стабильности в Евроатлантическом регионе НАТО могла позволить себе роскошь формулировать вызовы и угрозы общими широкими мазками. Новый документ более откровенно и чётко фиксирует действия России разрушающими стабильный и предсказуемый порядок, а авторитарные государства по всему миру (речь видимо идёт о России и Китае) использующими демократические принципы устройства стран членов НАТО (в том числе — цифровую открытость) для подрыва их безопасности. Здесь Российская Федерация предстаёт в качестве основной прямой угрозы безопасности альянса, что исключает возможность партнерства и ведения диалога с ней в обозримой перспективе. На втором месте в иерархии угроз выделяется терроризм во всех его формах и проявлениях, что в векторе призывов признать Россию спонсором международного терроризма потенциально приобретает новое толкование. А на третьем месте стоит проблема обеспечения кибербезопасности. Отметим, что «системное соперничество» с Китаем является стратегическим вектором НАТО на среднесрочную перспективу и это подкрепляется положением о принципиальности развития ситуации в Индо-Тихоокеанском регионе для безопасности Евроатлантики. Саммит НАТО также впервые посетили представители региональных партнеров альянса — Австралии, Японии, Новой Зеландии, Республики Корея, а итоговое заявление заседания с их участием было



явно антикитайским. Это можно считать опасным сигналом для европейских стран членов НАТО и почти необратимым для них курсом на свертывание общих проектов с Китаем, что существенно сокращает организационный ресурс ЕС. Концепция НАТО-2022 сохранила в качестве основных задач блока сдерживание и оборону (это считается приоритетной задачей), кризисное урегулирование и обеспечение кооперативной безопасности. Средством же реализации задачи сдерживания и обороны является комплексное повышение стрессоустойчивости, а это включает в себя и развитие технологических возможностей, и наращивание материальной базы, и еще более тесная координация военных комплексов государств-членов альянса в том числе и в киберпространстве [2,3].

Научным экспертным сообществом рассматривались различные модели возможного развития Североатлантического альянса с позиции самых различных подходов (через неореализм, теорию альянсов, неоинституционализм, конструктивизм и др.), а для анализа перспектив развития ЕС, как правило, применялись неолиберальные концепции, при этом внешнеполитическая деятельность Евросоюза толковалась через нормативно-трансформационный формат [6].

Следует подчеркнуть, что основной аналитический недостаток неореализма при оценке внешнеполитической активности блока



НАТО — это исключение его внутренней динамики и склонность объяснять центробежные тенденции отсутствием общей угрозы. Также следует отметить, что особенность современного противостояния на мировой арене проявляется в его гибридном характере, то есть совмещении силовых и мирных средств, сочетании традиционного ведения войны с масштабным информационным и психологическим воздействием, специальными операциями и использованием прокси-формирований. В новых геополитических реалиях можно будет прогнозировать агрессивность коллективного Запада, а его смелость и активность будет определяться тем, что война имеет прокси-характер, то есть ведётся на чужой территории и чужими руками. В этой связи следует обратить внимание на актуальный доклад президента и главного юриста компании Microsoft г-на Брэда Смиса (Brad Smith) «Защищая Украину: Первые уроки кибервойны», где в том числе он делает акцент на четырёх принципах противодействия российским киберугрозам, включая цифровую тактику, сотрудничество между государственным и частным секторами, мультилатерализм (многосторонний подход), свободное выражение мнений и защиту открытых и демократических обществ. Кроме того, подчеркнём роль мировых ИТ-гигантов в подготовке специалистов по кибербезопасности и киберразведке для министерства обороны Соединенных Штатов (программа действует с 2012 года) и стран-членов НАТО (параллельно был запущен процесс подготовки кадров на базе учебных центров и центров передового опыта НАТО). Содержание, специфика и универсальность образования в области кибербезопасности и киберразведки наглядно свидетельствуют о масштабах и целенаправленности, с которыми США и блок НАТО осваивают новую сферу боевых действий, а именно киберпространство.

Также отметим, что ограниченная война может выступить инструментом политики, но в этом случае ее задача не тотальная победа, а установление стабильного мира на выгодных игроку условиях. Подчеркнём, что в современных условиях окончание войны, в том числе и информационной, не будет означать окончания противостояния между рядом стран, оно лишь обозначит новые геополитические контуры мировой политики.

Методологические принципы анализа больших и сложных систем в международных отношениях и особенности управления во внешнеполитической деятельности на современном этапе опираясь на закон о сходимости самоорганизующихся систем к оптимуму, предложенный и принятый научной общественностью как всеобщий закон диалектики и поддержанный известными учеными различных специальностей из многих стран мира [1] позволили разработать 10 сценариев дальнейшего устойчивого развития миропорядка с определенными плюсами и минусами для отдельных акторов мировой политики. Но, как говорится, была бы только политическая воля, а достичь геополитической стабильности, это дело техники. Но пока можно только констатировать, что происходит трансформация внешней политики США, ЕС и Североатлантического альянса, с изменением парадигмы их действий [4,5] и переходом к наступательной внешней политике, включая кибервозможности. А в условиях финансовой, технологической и цифровой неокolonизации значительного числа стран мира, на более технологически-ориентированных международных площадках разворачивается борьба за признание создаваемых отдельными государствами и крупными корпорациями технических стандартов, что усугубляет проблему обеспечения цифрового суверенитета современного государства. Кроме того, ярко проявляется противоречие между информационным обменом как глобальным явлением и физической инфраструктурой, которая имеет территориальную привязку, то есть находящуюся под суверенитетом государства. Это же касается вопросов хранения, обработки и перемещения информации по каналам интернет-коммуникаций. Сложился существенный дисбаланс в географическом распределении базовой основы инфраструктуры и национальной принадлежности основных интернет-участников. Сегодня более 60 процентов от общего числа доменов управляются компаниями из США, а свыше 50 процентов сетей доставки контента принадлежат американским корпорациям (Amazon, Akamai, CloudFlare). Все ключевые провайдеры первого уровня являются резидентами США и там же, в США находятся и десять из тринадцати корневых DNS-серверов. Поэтому при такой ситуации

и готовности Соединенных Штатов пойти в односторонних санкциях на весьма крайние меры, государства, которые не являются союзниками Америки, будут стремиться создать альтернативный защищённый контур «национального, суверенного интернета», причем число таких стран растёт. С другой стороны, по оценкам ряда экспертов спутниковый интернет в ближайшие десятилетия может вытеснить интернет кабельный. Но как бы то не было, на земле, в космосе или в верхних слоях атмосферы желание государств оставлять ключевую инфраструктуру в зоне своего суверенного контроля, сохранится [7]. Следует отметить, что изменение принципов функционирования международных отношений и всей модели мировой геополитики и геоэкономики предоставляет ведущим «цифровым неоколониалистам» новые возможности. Сегодня продолжает увеличиваться разрыв между глобальными провайдерами цифровых технологий и государствами-реципиентами, которые подпадают под всё большую зависимость от технологически развитых стран. А эти страны («цифровые неоколониалисты») предлагают льготные условия создания необходимой для перехода в цифровое будущее инфраструктуры, таким образом, уже на начальном этапе формируя их привязку к своим собственным решениям, включая платёжные системы, системы хранения данных и обеспечения электронного документооборота. То есть обеспечивается неограниченный и практически бесплатный доступ к большим данным, а страны, обладающие этими данными, получают прямой экономический эффект, дополнительное преимущество при развитии инструментов искусственного интеллекта и нейросетей (по оценкам экспертов уже к 2025 году глобальный рынок больших данных достигнет 230 млрд долларов) и эффективные инструменты контроля над своими «цифровыми колониями». Поэтому цифровой и технологический суверенитет государства становится необходимым условием суверенитета политического и национальной независимости [8].

#### СПИСОК ИСТОЧНИКОВ

1. Аникин В.И., Абдеев Р.Ф., Сурма И.В. Философские аспекты информационной цивилизации и современные проблемы управления в ракурсе глобаль-

ной безопасности // Вопросы безопасности. 2017. № 2.

2. Мельникова Ю. В поисках оптимальной архитектуры европейской безопасности: ЕС и НАТО — вместе или вместо? Режим доступа: [сайт] — URL: <https://russiancouncil.ru/analytics-and-comments/analytics/v-poiskakh-optimalnoy-arkhitektury-evropeyskoy-bezopasnosti-es-i-nato-vmeste-ili-vmesto/> (дата обращения: 15.08.2022). — Текст: электронный.
3. Мельникова Ю. Маршрут восстановлен? Итоги саммита НАТО в Мадриде. Режим доступа: [сайт] — URL: <https://russiancouncil.ru/analytics-and-comments/analytics/marshrut-vosstanovlen-itogi-sammita-nato-v-madride/> (дата обращения: 05.08.2022). — Текст: электронный.
4. Независимая газета. Режим доступа: [сайт] — URL: <https://www.ng.ru/content/articles/744089/> (дата обращения: 29.07.2022). — Текст: электронный.
5. Путин заявил о стремлении ряда стран подменить архитектуру безопасности. Режим доступа: [сайт] — URL: <https://iz.ru/1354890/2022-06-24/putin-zaiavil-o-stremlenii-riada-stran-podmenit-arkhitekturu-bezopasnosti> (дата обращения: 09.08.2022). — Текст: электронный.
6. Дегтев И. Эволюция стратегии НАТО на современном этапе. Режим доступа: [сайт] — URL: <https://topwar.ru/167898-jevoljucija-strategii-nato-na-sovremennom-jetape.html> (дата обращения: 29.07.2022). — Текст: электронный.
7. Hurst N. Why Satellite Internet Is the New Space Race // PC. 2018. Режим доступа: [сайт] — URL: <https://www.pcmag.com/news/why-satellite-internet-is-the-new-space-race> (дата обращения: 29.09.2022). — Текст: электронный.
8. Безруков А., Мамонов М., Сучков М., Сушенцов А. Конкуренция технологических платформ, или как вести себя в новом мире. Режим доступа: [сайт] — URL: <https://globalaffairs.ru/articles/suverenitet-i-cifra/> (дата обращения: 29.09.2022). — Текст: электронный.

### КИБЕРВОЙНА ЗАПАДА НА УКРАИНЕ — НОВЫЕ ТЕХНОЛОГИИ ПО СТАРЫМ ЛЕКАЛАМ

Кибервойна в широком смысле относится к новой форме ведения войны, охватывает широкий спектр понятий, в том числе кибератаки на критически важную инфраструктуру на основе информационно-коммуникационных технологий и технологий искусственного интеллекта; она также включает в себя изменение сознания, то есть путём изменения понимания людей приводит к руководству идеями и поведением людей, такие как ментальная война, когнитивная война, манипуляция общественным мнением и т. д.

На уровне сознания, когда у большинства людей нет возможности и условий для самостоятельного расследования информации, им трудно выйти из собственных когнитивных ограничений. Эксплуатируется именно это когнитивное слепое пятно: в социальных сетях использование дезинформации, фейки, дипфейки и другие интернет-средства могут осуществлять манипулирование общественным мнением и влиять на направление познания людей. Когда платформы социальных сетей, контролируемые ИТ-гигантами, монополизируют основные каналы информации, тогда основное познание может быть сформировано.

В украинском кризисе мы действительно наблюдали и наблюдаем широкомасштабную манипуляцию общественным мнением, движимую единым мнением, с использованием социальных сетей, созданных западными ИТ-гигантами, в качестве такой платформы. Страны используют общественное мнение для противодействия, выборочно выпускают и распространяют информацию, контролируют тенденции международного общественного мнения, стремятся к пониманию и поддержке правительств и людей во всем мире.

В силу исторических причин и стремительного развития Интернет-технологий, технологическая база в критических областях многих стран основывается на технологических системах и структурах, созданных западными странами. Мы наблюдали в этом инциденте, что западные ИТ-гиганты, особенно транснаци-



ональные провайдеры с определённым монопольным статусом, больше не являются чисто коммерческими и общедоступными. Конечно, весь мир пользуется удобством и услугами, которые они приносят, однако, когда национальные интересы и безопасность западных стран вступают в противоречие с коммерческими и общедоступными характеристиками ИТ-гигантов, общедоступность будет уступать национальным интересам.

Что-то такое также происходит в Китае. Явления манипуляции социальных сетей на Украине привлек к когнитивной войне большое внимание в Китае, а осведомлённость о когнитивной войне ещё больше повысилась, поднявшись до уровня национальной безопасности и популяризировала его в массах. Это даёт новые исследовательские идеи для исследований экспертов и учёных и добавляет практическое вдохновение исследованиям.

Поскольку Интернет Китая имеет независимую экологическую среду, это даёт возможность манипулировать общественным мнением во вне-китайском Интернете. После разжигания беспорядков в Гонконге в 2019 году и дестабилизации провинции Синьцзян, в последние годы, когнитивная война против Китая через социальные сети усилилась. Некоторые люди и организации используют горячие темы на социальных платформах, широко используемых в Китае, систематически распространяют критические замечания для создания

споров, а затем переводят их на другие языки и размещают на зарубежных социальных платформах, чтобы ещё больше разжечь антикитайские настроения и подняться на политическом и дипломатическом уровне. Исследования когнитивной войны имеют большое значение.

В апреле нынешнего года, ряд социальных сетей в Китае запустил функцию отображения IP-местонахождения пользователя. IP-местонахождение аккаунтов пользователей на территории Китая должно быть отмечено провинцией/автономным районом/городом центрального подчинения, а IP-местонахождение зарубежных аккаунтов должно быть отмечено страной (регионом). Одной из целей этой функции является раскрытие дезинформации, предотвращение мошенничества, борьба с вводящим в заблуждение общественным мнением, помощь людям в идентификации информации и регулирование онлайн-среды. Например, некоторые аккаунты, выдающие себя за китайских пользователей, которые часто публикуют подстрекательские комментарии, чтобы ввести общественное мнение в заблуждение, на самом деле, после раскрытия IP-местонахождения обнаруживаются за границей.

Кроме этого, за последнее десятилетие Китай постоянно подвергается кибератакам. Только в первом квартале 2022 года Китай раскрыл несколько крупномасштабных международных кибератак. Основными объектами кибератак были правительство, финансовые организации, научно-исследовательские институты, операторы сотовой связи и другие учреждения, включая образование, военную, авиационно-космическую, медицинскую и другие сферы, и на долю высокотехнологичных областей приходится большая часть. В сентябре Китай предотвратил ещё одну кибератаку на университет, известный своими авиационными, аэрокосмическими и морскими исследованиями, который выполнял многочисленные оборонные и научно-исследовательские миссии.

Таким образом, кибератака Запада на Украине имеет большое влияние на ход событий, оказывает воздействие на мнение людей во многих странах. В условиях быстро меняющихся и обновляемых интернет-технологий мы сталкиваемся со всё более актуальной задачей управления киберпространством. Это практическая проблема, которую все страны должны решить для национального развития и безопасности.



## **ВИРТУАЛЬНЫЙ УКРАИНСКИЙ ФРОНТ — ВЗГЛЯД ИЗ АРАБСКОГО МИРА**

С появлением новых коммуникационных информационных технологии в мире появились много сложных ситуаций и проблем, больше всего проблем возникло в сфере информационной безопасности. Эта тема одна из самых актуальных тем, так как мир столкнулся с такой проблемой впервые за всю историю человечества.

Интернет и социальные сети не только показали полезность в мире, но и принесли огромное количество проблем за собой, оказались инструментом по распространению дезинформации и фейковых новостей по всей планете.

Глобальная информационная революция привела за собой огромное количество бед в мире, с появлением современных технологий ИКТ все ушло из-под контроля, чем больше прогрессируют ИКТ, тем сложнее становится бороться против распространения дезинформации и приступных фейков. Это все оказывает негативное влияние не только на человечество, но и на национальную безопасность страны, экономику и т.д., а также имеет непосредственное влияние на принятие политических решений как внутренних, так и на международном уровне, вплоть до разрыва отношений между странами.

На данный момент международное информационное поле в большинстве контролируются лидирующими странами, которые предлагают только свою про-западную пропаганду (точку зрения) и политическую модель единого мирового порядка, которая не совсем соответствует теории демократии, либерализма и правил свободы слова, когда запрещается на международном уровне инакомыслие, выражения своего мнения, а также становиться угрозой для тех стран, которые имеют свою правду, свое ведение и часто доходит дело до цветных революции, к примеру «Арабская Весна», которая привела к физической войне, опасности продовольственного кризиса, экономического кризиса, разрушения инфраструктуры, потери тысячи человеческих жизни, климатическим изменениям и загрязнению среды.



Данный доклад посвящён современным проблемам МИБ с украинскими кейсами.

Мир уже никогда не будет прежним, он запутался в большой глобальной паутине. С одной стороны — мы получили много положительного от новейших ИКТ.

С другой стороны — мир столкнулся с различными угрозами и проблемами, которые распространяются со скоростью света, и ситуация уже вышла из-под контроля.

Глобальная информационная революция влияет на все политические процессы, вплоть до формирования нового мирового порядка. «Информационная технология глобальная по своей сути и требует глобального подхода». Из Окинавской Хартии (группа восьми).

Мировое информационное пространство влияет на международные отношения и становится их реальностью, отличающейся от мирового порядка и дипломатии в 20 веке.

Информационная война, по теории М. Либика, это в большей степени негативное влияние на противника, которыми могут быть любые информационные сообщество, включая государство и различные институты.

Существует несколько форм информационных войн: разведывательные, хакерские, экономические, политические, кибервойны, когнитивные и психологические, основная цель психологических войн — это воздействия на сознание людей, воздействия на их



мнение, как они думают и как они должны принимать решение.

Информационные войны целенаправленно управляют массовым сознанием, используя различные способы манипуляции, помогают гегемонам, в т.ч. ИТ-гигантам, возглавлять лидирующие позиции в мире, инспирировать оппозиционную точку зрения и распространять различные фобии. К примеру, распространение русофобии, ксенофобии, исламофобии, фейки против вакцинации и ложной провокационной экстремистской конспирологической информации.

При современных ИКТ становится очень просто создать фейковую информацию, а также опровергать и фальсифицировать действующую информацию, к примеру использования метода (deep fake).

Информационные войны и угрозы связаны с новейшими ИКТ и различными НКО, которые нацелены на изменение ценностей общества и «Окна Овертона». Большая работа идет по работе с молодежью, так как на эту категорию граждан легко влиять, управлять и убеждать, также попадает под легкое влияние оппозиция, которая разделяет их взгляды и смену кодов целых культур отдельных стран при помощи когнитивного воздействия на сознание народов. Пример — Украина.

Информационные войны теоретики и аналитики рассматривают, в первую очередь, как оказание влияния на психику и сознание человека. Американский профессионал в области кибервойн, проработавший 30 лет в правительственных органах по безопасности, Р. Кларк интерпретировал кибервойну,

как воздействия одного государства на сети другой страны, ради нанесения ущерба и разрушения. По его мнению, гибридные атаки более эффективные и обходится без физических жертв<sup>1</sup>.

Украинский кейс рассматривается в Арабском мире по-разному, но чаще всего мнение местных экспертов, журналистов и аналитиков не совсем совпадает с мейнстримовой глобальной повестке.

В различных арабских медиа альтернативные мнения очень сильно отличаются от привычной глобальной пропаганды, к примеру, новостной портал АЛЬ-Арабия в своих расследованиях написали про украинских националистов и причины специальной операции<sup>2</sup>.

Араби пост, немало известный новостной портал, исследовал дело ультраправых националистов на Украине и их негативное и опасное влияние на западную культуру<sup>3</sup>.

Сана новостной портал также разместил разную информацию про Азов, ультраправую армию на Украине<sup>4</sup>, с похожей темой не отличился новостной сайт ЕЛЬ-Набаа, который в деталях указал на участие современных украинских националистов и как они появились и какую идеологию они продвигают<sup>5</sup>.

Интересное исследование политического религиозного сайта Вайс по теме специальной операции на Украине, о том, что ультраправые националистические украинские группировки протирали салом пули для борьбы против мусульманских солдат из Чеченской республики, также в деталях рассказали какие националистические знаки и эмблемы используются и что они обозначают<sup>6</sup>.

1 Международная информационная безопасность: Теория и практика: В трех томах. Том 1: Учебник для вузов / Под общ. ред. А.В. Крутских. — 2-е изд. доп. — Москва: Издательство «Аспект Пресс», 2021. — 384 с. — Текст: непосредственный.

2 Alarabiya. تحرير أوكراينا.. من هم النازيون الجدد الذين يحاربهم بوتين؟  
<https://www.alarabiya.net/arab-and-world/2022/02/26/%D8%AA%D8%AD%D8%B1%D9%8A%D8%B1-%D8%A3%D9%88%D9%83%D8%B1%D8%A7%D9%86%D9%8A%D8%A7-%D9%85%D9%86-%D8%A7%D9%84%D9%86%D8%A7%D8%B2%D9%8A%D8%A9>

3 Arabipost. النازيون الجدد.. من هم القوميون الأوكرانيون الذين يتهمهم بوتين بالتطرف ويتعهد بالقضاء عليهم؟  
<https://arabicpost.net/%D8%AA%D8%AD%D9%84%D9%8A%D9%84%D8%A7%D8%AA/2022/03/09/%D8%A7%D9%84%D9%8A%D9%85%D9%8A%D9%86-%D8%A7%D9%84%D9%85%D8%AA%D8%B7%D8%B1%D9%81-%D9%81%D9%8A-%D8%A3%D9%88%D9%83%D8%B1%D8%A7%D9%86%D9%8A%D8%A7/>

4 Sana. فظائع وجرائم خطيرة.. النازيون الجدد يكشفون وجههم الحقيقي في أوكراينا.  
<http://www.sana.sy/?p=1616014>

5 enabaa. من هم «النازيون الجدد» التي تريد روسيا اجتثاثهم من أوكراينا وعلاقتهم باليهود.. ولماذا تدعمهم إسرائيل؟  
<https://www.elnabaa.net/932059>

6 Vice. «الأوكرانية تدهن الرصاص بـ"شحم الخنزير" للتصدي للقوات الشيشانية المسلحة " في بلادنا لن تذهبوا إلى الجنة».  
<https://www.vice.com/amp/ar/article/z3ngp3/%D9%81%D8%B1%D9%82%D8%A9-%D9%85%D9%86-%D8%A7%D9%84%D9%86%D8%A7%D8%B2%D9%8A%D9%8A%D9%86-%D8%A7%D9%84%D8%AC%D8%AF%D8%AF-%D8%A7%D9%84%D8%A3%D9%88%D9%83%D8%B1%D8%A7%D9%86%D9%8A%D8%A9-%D8%AA%D8%AF%D9%87%D9%86-%D8%A7%D9%84%D8%B1%D8%B5%D8%A7%D8%B5-%D8%A8%D9%80%D8%B4%D8%AD%D9%85-%D8%A7%D9%84%D8%AE%D9%86%D8%B2%D9%8A%D8%B1-%D9%84%D9%84%D8%AA%D8%B5%D8%AF%D9%8A-%D9%84%D9%84%D9%82%D9%88%D8%A7%D8%AA-%D8%A7%D9%84%D8%B4%D9%8A%D8%B4%D8%A7%D9%86%D9%8A%D8%A9>

Иорданский сайт Араб-джо также не прошел мимо украинского кризиса и опубликовал статью о том, как Израиль использует Украинский кризис, чтобы атаковать Сирию<sup>7</sup>, новостной сайт Хибер в своей статье также доказали участие Израиля в украинской специальной операции<sup>8</sup>. Таких примеров очень много, они не имеют огромного веса в информационной повестке как мейнстримовая пропаганда.

После появления интернета и социальных сетей резко выросло количество различных проблем во всем мире. Используются все социальные платформы недоброжелателями ради своей односторонней политической повестки, подминая мир под единую мировую систему, дают им возможности изобретать все новые технологии влияния на сознание

людей, управления умами и использование массы для борьбы против «авторитарных» режимов и создания хаоса в мире, пытаюсь поделить мир на «свободных» «демократичных» и на «диктаторов» «нарушителей человеческих свобод». Такое поведение нарушает основу теории демократии, либерализма и правила свободы слова, когда разрешается только одно единственное мнение на весь мир, считая других экстремистами, многополярность как раз-таки даст возможность плюрализма в информационном поле и таким образом будет возможно бороться на международном уровне против фейков и дезинформации, ведь, как всем известно, что мифы, фейки и конспирология разлетаются быстрее и воспринимаются людьми больше чем факты.

7 Arabjo. / الكيان الصهيوني يستغل أزمة اوكرانيا لتكريس اعتدائه ضد سورية. <https://www.arabjo.net/?p=95251>

8 7iber. إسرائيل «والحرب في أوكرانيا: الظاهر والباطن». <https://www.7iber.com/politics-economics/%D8%A5%D8%B3%D8%B1%D8%A7%D8%A6%D9%8A%D9%84-%D9%88%D8%A7%D9%84%D8%AD%D8%B1%D8%A8-%D9%81%D9%8A-%D8%A3%D9%88%D9%83%D8%B1%D8%A7%D9%86%D9%8A%D8%A7/>

**В.И. Булва**

*Эксперт, помощник директора Центра международной информационной безопасности и научно-технологической политики МГИМО МИД России*

## **ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ МОЛОДЕЖИ В ИНФОРМАЦИОННОМ ПРОСТРАНСТВЕ В УСЛОВИЯХ ГЕОПОЛИТИЧЕСКОЙ ТРАНСФОРМАЦИИ**

Сегодня информационно-коммуникационными технологиями (ИКТ) пользуется подавляющая часть населения планеты, в т.ч. представители подрастающего поколения. С 2006 по 2010 год число подростков, проводящих за компьютером не менее трех часов каждый день, увеличилось в четыре раза (с 5,7% до 21,7%). К 2018 году уже 56% детей постоянно находятся в Сети<sup>1</sup>. Более 80% российских подростков имеют профиль в соцсетях, причем каждый шестой имеет около 100 друзей и только около 40% детей впоследствии начинают встречаться с сетевыми знакомыми в офлайне<sup>2</sup>. В 2021 г. в возрастной категории от 12 до 24 лет доля Интернет-пользователей достигла 97,1%, в категории от 25 до 34 лет Интернетом как минимум раз в месяц пользовались 95,8% россиян<sup>3</sup>.

При этом, большую часть времени молодежь проводит за видеоиграми (92% девушек и 95,3% юношей в возрасте от 16 до 24 лет<sup>4</sup>) и в социальных сетях. Социальные сети и мировая паутина представляют для них не только инструмент для развлечения, но и основной источник информации. Помимо этого, молодежь (16–24 года) значительно чаще других возрастных групп использует мобильные телефоны для онлайн-покупок (63% девушек, 55,8% юношей<sup>5</sup>), причем 5 из 10 юзеров посещают соцсети специально для изучения брендов и продуктов<sup>6</sup>.



Обладая неустойчивым сознанием и только формирующимся мировоззрением, молодежь становится уязвимой мишенью перед лицом вызовов информационного пространства<sup>7</sup>. Важно отметить, что большинство угроз обусловлено поведением самих пользователей. Так, для онлайн-покупок и регистрации в социальных сетях они раскрывают личную информацию, что снижает уровень конфиденциальности их данных. Угроза заключается в том, что эта информация (а также данные, полученные на основе анализа поисковых запросов) потом используется для осуществления таргетинга, в т.ч. в противоправных и военно-политических целях.

Одним из отрицательных последствий Интернет-зависимости молодежи является размывание грани между реальностью и виртуальным миром, сведение до минимального уровня реальных социальных связей. Сегодня, возрастают случаи манипулирования общественным сознанием с целью подрыва духовно-нрав-

1 Статистика Интернет-зависимости у российских подростков // Безопасность в Интернете – URL: <http://security.mosmetod.ru/internet-zavisimosti/127-statistika-internet-zavisimosti-u-rossijskikh-podroستkov> (дата обращения: 24.08.2022).

2 Там же.

3 Доля пользователей интернета в России среди молодежи приблизилась к 100% // РБК. 12.01.2021 – URL: [https://www.rbc.ru/technology\\_and\\_media/12/01/2021/5ffde01e9a79478eb5230426](https://www.rbc.ru/technology_and_media/12/01/2021/5ffde01e9a79478eb5230426) (дата обращения: 24.08.2022).

4 Вся статистика интернета и соцсетей на 2021 год — цифры и тренды в мире и в России // WebCanape. 2021 – URL: <https://www.web-canape.ru/business/vsya-statistika-interneta-i-socsetej-na-2021-god-cifry-i-trendy-v-mire-i-v-rossii/> (дата обращения: 24.08.2022).

5 Там же.

6 Digital 2022: global overview report // DataReportal. 26 January 2022 – URL: <https://datareportal.com/reports/digital-2022-global-overview-report> (дата обращения: 24.08.2022).

7 Бирюков А.В. Алборова М.Б. Социально-гуманитарные риски информационного общества и международная информационная безопасность. – М.: Издательство «Аспект Пресс», 2021. — с. 25.

ственных основ государства. Ввиду низкой способности к критическому анализу, вызванной привычкой получать готовую информацию из блогов и социальных сетей, именно молодые люди оказываются идеальным объектом для психологического воздействия.

И хотя психологические войны не представляют собой изобретение XXI века, появление ИКТ способствовало их качественной трансформации. Возникла опасность ментальных войн, цель которых не просто внушить определенную установку противнику для реализации конкретной узкой задачи, а оказать влияние на формирование мировосприятия целого поколения. При этом, как отмечал российский эксперт А.И. Смирнов, для ликвидации последствий потребуется смена нескольких поколений.

Когнитивное воздействие на сознание молодежи осуществляется в различных целях, в т.ч. для создания угроз личной безопасности (призыв к суицидам), для вербовки новых сторонников в террористические и преступные группировки. Однако в условиях турбулентности геополитических процессов, особую угрозу, в т.ч. для молодежи, представляет использование информационного пространства в военно-политических целях.

Западные страны расширяют практику проведения информационно-психологических операций, направленных на дискредитацию политики России и оправдание собственных действий на международной арене. Учитывая доминирование западных информационных ресурсов, многократно увеличивается риск «потери целого поколения», причем как в национальном, так и мировом масштабе. Так, после начала Специальной военной операции активизировали деятельность Центры информационно-психологических операций на Украине, специализирующиеся на антироссийской пропаганде: 16-й центр ИПсО (воинская часть А1182, Гуйва, Житомирская обл.); 72-й центр ИПсО (воинская часть А4398, Бровары, Киевская обл.); 74-й центр ИПсО (воинская часть А1277, Львов); 83-й центр ИПсО (воинская А2455, Одесса). Кроме того, для этих же целей продолжают функционировать Центры передового опыта НАТО в Таллине, Риге и Вильнюсе<sup>8</sup>.

В данных условиях, важной задачей в сфере обеспечения информационной безопасности молодежи является с одной стороны, недопущение милитаризации информационного пространства и применения ИКТ в противоправных целях, а с другой стороны — стимулирование мирного использования технологий.

В первом случае, ответственность возлагается на государства. Одной из ключевых задач является формирование международного режима МИБ, основанного на добровольных и юридически обязательных нормах, принципах и правилах ответственного поведения в информационном пространстве, а также основополагающих положений Устава ООН. При наличии должного механизма верификации исполнения обязательств и порядка введения санкций за их неисполнение, будет минимизирован риск неправомерного использования ИКТ.

Однако в силу текущей геополитической ситуации в ближайшей перспективе решение всех вопросов на глобальном уровне (в рамках ООН) маловероятно. На данном этапе следует сосредоточить усилия на активизации точечного сотрудничества с государствами-единомышленниками. При этом, в отношении обеспечения безопасности молодежи в Интернете, особенно важно углублять двустороннее и региональное сотрудничество в рамках подготовки кадров. В данной связи, актуальность приобретают такие меры, как проведение совместных семинаров и конференций для укрепления научно-образовательных связей, реализация совместных научно-исследовательских проектов для расширения учебно-методической базы в сфере МИБ, а также разработка образовательных программ с включением как технических, так и гуманитарных дисциплин. Примечательно, что на данном треке большое значение имеет привлечение других заинтересованных сторон (частного сектора, вузов).

Помимо этого, в важную роль в защите молодежи в ИКТ-среде играет развитие государственно-частного партнерства в сфере МИБ. В частности, 1 сентября 2021 г. 9 крупных российских компаний (Mail.ru Group, Яндекс, Лаборатория Касперского, Национальная Медиа Группа, Газпром-медиа холдинг, Мегафон,

8 Сурма И.В. НАТО-2030: Новая киберполитика Североатлантического Альянса // XV Международный форум «Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности», 2021 – с. 188-189.

Ростелеком, МТС, Вымпелком) приняли Хартию по безопасности детей в цифровой среде («Добровольные обязательства»)<sup>9</sup> и учредили соответствующий Альянс под председательством президента по корпоративным отношениям Яндекса Антона Шингарёва. Разработанные участниками данного объединения «Добровольные обязательства» включают целый комплекс мер, в том числе: самостоятельное выявление и ограничение доступа детей к контенту, способного причинить вред их развитию и здоровью, удаление противоправного контента, формирование «созидательно-го» контента.

В октябре 2021 г. крупные IT-компании и СМИ (ТАСС, Яндекс, Mail.ru Group, Rambler&Co, Rutube, Ura.ru, the Bell, Likee, МирТесен, Интерфакс, РБК, Бизнес ньюс медиа (Ведомости), Известия, центр компетенций в сфере интернет-коммуникаций «Диалог») подписали Меморандум о борьбе с фейками<sup>10</sup>. Среди мер: разработка и принятие на добровольных началах общих механизмов и правил выявления, проверки, верификации (фактчекинга), опровержения и удаления недостоверной информации, предложение создать Совет участников меморандума.

Наконец, крайне значимым является поощрение развития контактов между молодежью разных государств, причем речь идет как о реализации совместных проектов в сфере международных научно-технологических отношений, ориентированных на стимулирование использования ИКТ в мирных целях, так и участия молодых экспертов в международных дискуссиях (неформального характера) на международных площадках.

В первом случае, следует обратить внимание на недавние инициативы в области МНТО

на постсоветском пространстве, инициаторами и/или участниками которых становились представители подрастающего поколения. На базе Международного инновационного центра нанотехнологий СНГ в 2022 г. в Дубне планируется проведение Стажировки молодых ученых и специалистов стран СНГ<sup>11</sup>. В целях расширения образовательных связей в рамках Союзного государства Россия-Беларусь увеличено количество стипендий для обучения граждан Республики Беларусь в российских вузах. Так, Минобрнауки России рассчитывает выделить в 2022-2023 гг. порядка 2 тыс. квотных мест для белорусской молодежи<sup>12</sup>.

Другой приоритетной сферой сотрудничества является реализация совместных молодежных проектов, в том числе с привлечением молодых ученых. В качестве примеров, можно упомянуть 7-й Форум молодых ученых стран БРИКС<sup>13</sup>, Молодежный Научно-технический и Инновационный Форум ШОС<sup>14</sup>, IV Форум Ассоциации вузов России и Беларуси<sup>15</sup>. Кроме того, для стимулирования участия молодых исследователей в научной деятельности по инициативе белорусской стороны в 2022 г. была инициирована Премия Союзного государства молодым ученым.

Во втором случае, целесообразно упомянуть о возможности молодых экспертов, представляющих Российскую Федерацию, выступить с позицией представляемых ими организаций в рамках неформального диалога РГОС, организованного председателем Группы.

Таким образом, сегодня обеспечение безопасности молодежи в информационном пространстве зависит от комплекса внутренних (связанных с особенностями, присущими дан-

9 Подписание добровольных обязательств компаниями – учредителями Альянса по защите детей в цифровой среде // Официальный сайт Президента России. 01.09.2021 – URL: <http://kremlin.ru/events/president/news/66557> (дата обращения: 05.08.2022).

10 Крупнейшие российские IT-компании и СМИ подписали в ТАСС меморандум о борьбе с фейками // ТАСС. 07.10.2021 – URL: [https://tass.ru/ekonomika/12604685?utm\\_source=google.com&utm\\_medium=organic&utm\\_campaign=google.com&utm\\_referrer=google.com](https://tass.ru/ekonomika/12604685?utm_source=google.com&utm_medium=organic&utm_campaign=google.com&utm_referrer=google.com) (дата обращения: 05.08.2022).

11 Образовательные контакты: МИЦНТ СНГ объявляет о проведении Стажировки молодых ученых и специалистов стран СНГ в Дубне в 2022 г. // МИЦНТ СНГ – URL: <https://ininc.jinr.ru/page.php?id=362> (дата обращения: 12.07.2022).

12 Развитие науки и образования в Союзном государстве стали темами IX Форума регионов Беларуси и России // Интернет-портал СНГ [Электронный ресурс]. – URL: <https://e-cis.info/news/569/101579/> (дата обращения: 12.07.2022).

13 7-й Форум молодых ученых стран БРИКС // Национальный комитет по исследованию БРИКС – URL: <https://www.nkibrics.ru/posts/show/626a62826272694935010000> (дата обращения: 12.07.2022).

14 Успешно завершился Молодежный Научно-технический и Инновационный Форум ШОС // CISION PR Newswire – URL: <https://www.prnewswire.com/ru/press-releases/uspeshno-zavershilsia-molodezhnyi-nauchno-tehnicheskii-i-innovatsionnyi-forum-shos-897752620.html> (дата обращения: 12.07.2022).

15 Развитие науки и образования в Союзном государстве стали темами IX Форума регионов Беларуси и России // Интернет-портал СНГ – URL: <https://e-cis.info/news/569/101579/> (дата обращения: 12.07.2022).



ной возрастной категории) и внешними (угрозы МИБ) факторами. Для формирования эффективного защитного механизма молодого поколения в ИКТ-среде требуется как участие государства (отвечающего за выработку «правил игры» в информационном пространстве), так и привлечение частного сектора и науч-

но-академического сообщества (в первую очередь, в области развития кадрового потенциала соответствующего профиля). При этом, весомое значение отводится реализации молодежных инициатив, их непосредственному подключению к неформальным диалогам на международных площадках по тематике МИБ.

СБОРНИК ДОКЛАДОВ УЧАСТНИКОВ  
XVI МЕЖДУНАРОДНОГО ФОРУМА  
«ПАРТНЕРСТВО ГОСУДАРСТВА, БИЗНЕСА  
И ГРАЖДАНСКОГО ОБЩЕСТВА  
ПРИ ОБЕСПЕЧЕНИИ МЕЖДУНАРОДНОЙ  
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

Подписано в печать 02.12.2022. Гарнитура Helios.  
Формат 60x84/8. Объем 21,39 усл. печ. л.  
Тираж 200 экз.

