СБОРНИК ДОКЛАДОВ УЧАСТНИКОВ
ПЯТНАДЦАТОГО МЕЖДУНАРОДНОГО ФОРУМА

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

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

НАМИБ

27–29 СЕНТЯБРЯ 2021 Г.,
МОСКВА, РОССИЯ

СБОРНИК ДОКЛАДОВ УЧАСТНИКОВ
ПЯТНАДЦАТОГО МЕЖДУНАРОДНОГО ФОРУМА

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

27–29 СЕНТЯБРЯ 2021 г.,
МОСКВА, РОССИЯ

УДК 334.021(082)
ББК 65.291я43
П18

АННОТАЦИЯ

В сборнике представлено большинство выступлений участников Пятнадцатого международного Форума «Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности», проходившего в г. Москве в период с 27 по 29 сентября 2021 г[1].

Форум, организованный Национальной Ассоциацией международной информационной безопасности (далее -Ассоциация), 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, посвященное обсуждению современных проблем обеспечения международного мира и поддержания устойчивого развития в глобальном информационном обществе. Кроме того, была организована работа пяти круглых столов, на которых эксперты обсудили следующие вопросы:

- международное сотрудничество в области атрибуции инцидентов в целях мирного разрешения спорных ситуаций в ИКТ-среде;
- обеспечение безопасности объектов критической информационной инфраструктуры;
- международное сотрудничество в области противодействия информационной преступности;
- сотрудничество в области предотвращения военных конфликтов и мирного разрешения спорных ситуаций в ИКТ-среде;
- сотрудничество в области противодействия вмешательству во внутренние дела суверенных государств с использованием средств массовой коммуникации.

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. Обостряются и разногласия в подходах государств к определению приоритетов в противодействии угрозам МИБ.

В 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 безопасности использования ИКТ-среды коммерческими компаниями. Отмечена важность обсуждения имеющихся в этой области проблем с участием представителей бизнеса, 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 международного 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 активизации разъяснения российских подходов к решению проблем обеспечения МИБ. Отмечена необходимость расширения деятельности высших учебных заведений страны по подготовке кадров в области международной информационной безопасности.

В работе Форума, проходившего в комбинированном формате – онлайн и оффлайн – приняли участие 140 экспертов из 13 государств и ряда международных организаций.

Перевод докладов зарубежных участников на русский язык осуществлен сотрудниками Ассоциации А. Цветковой, К. Бойко и Е. Осечкиным.

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

ISBN 978-5-6044055-2-9

1 Ряд выступавших участников не представили тезисы своих выступлений

ПРИВЕТСТВИЕ СЕКРЕТАРЯ СОВЕТА БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

В своем выступлении на заседании Совета Безопасности Российской Федерации 26 марта 2021 года Президент Российской Федерации обратил внимание на необходимость более активного использования возможностей научных и экспертных кругов, делового сообщества для более эффективной реализации государственной политики Российской Федерации в области международной информационной безопасности.

Глава государства подчеркнул важность укрепления действующих международных дискуссионных площадок в России для продвижения российских подходов и инициатив в области международной информационной безопасности.

Организованный Национальной Ассоциацией международной информационной безопасности Международный форум «Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности» в очередной раз собирает ведущих российских и зарубежных экспертов для обсуждения наиболее актуальных проблем безопасности в информационной сфере и для поиска оптимальных решений в интересах формирования системы обеспечения международной информационной безопасности.

За свою пятнадцатилетнюю историю Форум заслуженно стал одной из наиболее авторитетных экспертных площадок, местом зарождения конструктивных идей, нацеленных на конкретный результат.

Уверен, что и в этом году Форум продолжит традиции предметного обсуждения ключевых вопросов обеспечения международной информационной безопасности, предоставит возможность его участникам обменяться опытом противодействия нарастающим вызовам и угрозам в информационной сфере, а также будет способствовать укреплению сотрудничества в целях предотвращения межгосударственных конфликтов в глобальном информационном пространстве.

Желаю организаторам и участникам Форума плодотворной работы!

Секретарь Совета Безопасности
Российской Федерации
Н.П. Патрушев

СОДЕРЖАНИЕ

ПЛЕНАРНОЕ ЗАСЕДАНИЕ

КРУГЛЫЙ СТОЛ № 1
МЕЖДУНАРОДНОЕ СОТРУДНИЧЕСТВО В ОБЛАСТИ АТРИБУЦИИ ИНЦИДЕНТОВ В ЦЕЛЯХ МИРНОГО РАЗРЕШЕНИЯ СПОРНЫХ СИТУАЦИЙ В ИКТ-СРЕДЕ

КРУГЛЫЙ СТОЛ № 5
СОТРУДНИЧЕСТВО В ОБЛАСТИ ПРОТИВОДЕЙСТВИЯ ВМЕШАТЕЛЬСТВУ ВО ВНУТРЕННИЕ ДЕЛА СУВЕРЕННЫХ ГОСУДАРСТВ С ИСПОЛЬЗОВАНИЕМ СРЕДСТВ МАССОВОЙ КОММУНИКАЦИИ

ПЛЕНАРНОЕ ЗАСЕДАНИЕ

Ведущий:
Смирнов А. И., Генеральный директор НАМИБ

В.П. Шерстюк

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

ПАРТНЕРСТВО ГОСУДАРСТВА, БИЗНЕСА И ГРАЖДАНСКОГО ОБЩЕСТВА ПРИ ОБЕСПЕЧЕНИИ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. БЕЗОПАСНОСТЬ И УСТОЙЧИВОСТЬ ИКТ-СРЕДЫ РАДИ СТАБИЛЬНОСТИ И ПРОЦВЕТАНИЯ

Уважаемые участники Форума!
Уважаемые гости!
Дамы и господа!

Позвольте открыть заседание XV международного Форума «Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности». Трансляция Форума ведется из Актового зала Дипломатической академии МИД России, одного из учредителей Национальной ассоциации международной информационной безопасности.

Прежде всего хотелось бы начать со слов искренней признательности всем участникам и гостям Форума, которые просил передать Президент Ассоциации Владислав Петрович Шерстюк. Владислав Петрович открывал и вел все предыдущие форумы и только медицинские обстоятельства не позволили ему это сделать сегодня. Позвольте огласить текст доклада, подготовленный Президентом Ассоциации, советником Секретаря Совета Безопасности Российской Федерации, членом – корреспондентом Академии криптографии Российской Федерации Владиславом Петровичем Шерстюком.

«Уважаемые участники, уважаемые гости XV международного Форума! За 15 лет совместной работы мы с вами убедились в том, что создание открытой, безопасной, стабильной, доступной и мирной ИКТ-среды – это архисложный вопрос. Наши усилия в определенной степени способствовали нужному пониманию государств-членов ООН в вопросах оценки угроз международному миру и безопасности, общих подходов к созданию системы противодействия этим угрозам. Экспертное сообщество активно обсуждает возможные пути создания такой системы. Ни у кого не вызывает сомнения необходимость тесного сотрудничества в этой сфере.

«Важно сообща – подчеркнул Президент России Владимир Путин на заседании Совета Безопасности 31 марта 2021 г. – разработать и согласовать универсальные и справедливые для всех правила ответственного поведения государств в информационном пространстве с чёткими и внятными критериями допустимых и недопустимых действий и придать им юридически обязательный характер».

На этом заседании Президент Владимир Путин дал обязывающую оценку роли нашей Ассоциации.

«…в эффективной реализации государственной политики, обозначенной в новой редакции «Основ», надо активнее использовать возможности научных и экспертных кругов, делового сообщества, **в том числе, конечно, Национальной ассоциации международной информационной безопасности».**

Оргкомитет искренне надеется, что дискуссии на Форуме будут проходить в русле консолидации усилий по поиску путей решения многотрудных проблем МИБ. В этом контексте организаторы Форума сделают все возможное для того, чтобы участники могли свободно и открыто высказать и обсудить 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.

2. Уважаемые коллеги!

Создание и обеспечение системы МИБ – сложнейший процесс. Управление этим процессом предполагает наличие общего видения цели и диалога по конкретным проблемам сотрудничества государств в этой области.

Исходя из этого, на обсуждение участников XV Форума вынесена размещенная на сайтах Совета Безопасности России и НАМИБ, а также розданная участникам Форума новая редакция концепции конвенции ООН о международной информационной безопасности. Будут рассмотрены следующие актуальные проблемы:

- атрибуция инцидентов в ИКТ-среде;
- обеспечение безопасности объектов критической информационной инфраструктуры;
- противодействие информационной преступности;
- предотвращение военных конфликтов и мирного разрешения спорных ситуаций в ИКТ-среде;
- противодействие вмешательству во внутренние дела суверенных государств с использованием средств массовой коммуникации.

Актуальность этих вопросов подтверждается, в том числе, содержанием дискуссий, проведенных в рамках Рабочей группы открытого состава ООН, вебинаров по тематике МИБ, проведенных в 2021 г. ЮНИДИР, результатами круглого стола экспертов США, России и Китая по вопросам стратегической стабильности под эгидой Центра гуманитарного диалога в Женеве, а также проекта Международного исследовательского консорциума информационной безопасности по вопросам практического применения правил ответственного поведения государств в ИКТ-среде, завершенного в 2020 г.

В концепции конвенции в качестве приоритетных областей сотрудничества предлагается выбрать: предотвращение конфликтов в информационном пространстве, противодействие использованию ИКТ в террористических и иных преступных целях, укрепление доверия в сфере МИБ.

Оргкомитет Форума был бы благодарен участникам за их мнение о целесообразности принятия такой универсальной международной конвенции.

3. К числу ключевых проблем обеспечения безопасного использования ИКТ-среды безусловно относится развитие **«Международного сотрудничества в области атрибуции инцидентов в целях мирного разрешения спорных ситуаций в ИКТ-среде».** Эта проблема вынесена на обсуждение участников **Круглого стола № 1.**

В международном праве еще не сложился механизм закрепления факта инцидента в ИКТ-среде, сбора доказательств, подтверждающих данный факт, а также определения государства, виновного в противоправных действиях, приведших в возникновению инцидента. Более того, сложилась практика, при которой государства, между которыми не существует доверительных отношений, не реагируют на официальные обращения за правовой помощью в связи с такими инцидентами. Это обусловлено и отсутствием официально признанных границ зон ответственности государств в ИКТ-среде, а также процессуальных норм закрепления доказательств по фактам инцидентов.

В экспертном сообществе началось обсуждение идеи подключения к процессу атрибуции инцидентов в ИКТ-среде частных компаний и научных организаций. Известны и предложения о создании специальной международной организации, уполномоченной заниматься, в том числе, и атрибуцией инцидентов. Некоторые эксперты полагают целесообразным поддерживать существующий механизм атрибуции инцидента заинтересованными суверенными государствами.

4. На обсуждение участников **Круглого стола № 2** вынесены вопросы **обеспечения безопасности объектов критической информационной инфраструктуры.** Данные вопросы уже длительное время находятся в центре внимания экспертов на площадках ООН, ОБСЕ, ШОС, АСЕАН и других. Предложения по регулированию отношений в этой области нашли отражение в правилах ответственного поведения государств в ИКТ-среде, подготовленных ГПЭ ООН (2015 г.), в резолюции Генеральной Ассамблеи ООН (2018 г.), в Хартии информационной безопасности критических объектов промыш-

ленности, подготовленной компанией «Норильский никель» (2018 г.), в предложениях компании Майкрософт по разработке Цифровой Женевской конвенции по киберпространству (2018 г.), в итоговом докладе Глобальной миссии по стабильности в киберпространстве (2019 г.) и др.

В июле 2020 г. при поддержке НАМИБ был завершен международный исследовательский проект по изучению проблем практического применения некоторых правил ответственного поведения государств в ИКТ-среде, касавшихся, в т.ч. и безопасности объектов критической информационной инфраструктуры. В проекте принимали участие эксперты МГУ имени М.В. Ломоносова, Института киберполитки (Эстония), Института «Восток-Запад» (США) и Фонда «ИКТ для мира» (Швейцария). Отчет о результатах работы на русском и английском языках есть на сайте НАМИБ.

По мнению многих экспертов, опасность злонамеренного использования ИКТ для нападения на критическую информационную инфраструктуру, осуществления иных преступных деяний продолжает расти.

В этих условиях стала самоочевидной необходимость участия организаций бизнес-сообщества в решении задач обеспечения безопасности использования инфраструктуры. Государственно-частное партнерство, как правило, базируется на системе национальных правовых актов, регулирующих отношения в области безопасности бизнеса, критической информационной инфраструктуры, а также использования в этих целях потенциала центров реагирования на чрезвычайные ситуации в ИКТ среде.

Надеюсь, что дискуссии на данном круглом столе будут способствовать развитию сотрудничества экспертов в поиске взаимоприемлемых решений этой чрезвычайно сложной и важной проблемы.

5. В центре внимания участников **Круглого стола № 3** будут проблемы **международного сотрудничества в области противодействия информационной преступности**.

Как известно, проблема противодействия информационной преступности становится все более актуальной.

Поиску путей решения этой проблемы уделяется значительное внимание во всех государствах мира, а также на основных международных переговорных площадках – ООН, ОБСЕ, ШОС, АСЕАН и других.

Понимание государствами необходимости сотрудничества в этой области привел к созданию Спецкомитета ООН по разработке универсальной международной конвенции о противодействии использованию ИКТ в преступных целях. В июле 2021 г. Россия внесла в Спецкомитет ООН проект конвенции, который планируется рассмотреть в январе 2022 г.

В рамках дискуссии на круглом столе участники смогут обсудить российские предложения.

6. В рамках **Круглого стола № 4** состоится дискуссия на тему **«Сотрудничество в области предотвращения военных конфликтов и мирного разрешения спорных ситуаций в ИКТ-среде».**

К сожалению, вредоносный потенциал ИКТ для «силового» сценария разрешения межгосударственных споров, продолжает расти. Еще недавно к числу таких ИКТ эксперты относили, прежде всего, использование специального программного и технического обеспечения для нарушения деятельности критических объектов информационной инфраструктуры и других объектов, оказывающих влияние на жизнедеятельность общества, а также на военный потенциал государства.

В настоящее время активно развиваются системы искусственного интеллекта, внедряемые в военную технику. Совершенствуются способы и методы боевого применения автономных боевых роботов различного назначения. ИКТ широко применяются для повышения боевой эффективности.

Тенденции создания в вооруженных силах государств структурных подразделений по использованию ИКТ для «силового» противоборства особенно опасны, когда отсутствует опыт применения норм международного права для мирного разрешения споров по поводу инцидентов в ИКТ-среде.

Такие инциденты могут иметь самые серьезные последствия для международного мира и безопасности.

Человечество, по сути, в процессе развития ИКТ-среды столкнулось с необходимостью применять международное право для регулирования отношений в принципиально новой среде, в которой пока невозможно объективными способами зафиксировать как признаки нарушения международных обязательств, так

и установить субъектов международного права, причастных к этим нарушениям.

Отсутствие международных механизмов признания враждебного использования ИКТ государствами создает практически непреодолимые препятствия не только для регулирования международных споров, но и определения субъектов этих споров.

Еще раз хочу отметить, что сложившаяся ситуация способствует возникновению у некоторых юристов и политиков иллюзии свободы «силовых» действий в ИКТ-среде.

Самоочевидно, что этим путем нельзя достигнуть закреплённой в Уставе ООН цели – избавить грядущие поколения от бедствий войны.

Решение этих вопросов позволит придать юридическую надежность сведениям о международных инцидентах в ИКТ-среде и создать условия для применения правовых средств разрешения соответствующих опасных ситуаций.

7. Все более острой становится и ситуация с использованием ИКТ для вмешательства во внутренние дела суверенных государств. При этом складывается парадоксальная ситуация. США, бездоказательно обвиняя Россию во вмешательстве в выборы в 2016 г., не делали большой тайны из того, что практически открыто вмешивались в выборы Президента России в 2018 г., в голосование по поправкам в Конституцию в 2020 г., в только что прошедшие выборы 17–19 сентября и в другие политические мероприятия. Аналогичные факты зафиксированы и со стороны ряда других государств. Евросоюз и НАТО под видом борьбы с гибридными угрозами и с дезинформацией из России открыто вбрасывают через средства массовой коммуникации грубую ложь и фейки о России, ведут русофобский роботроллинг в соцсетях, используют весь киберарсенал ментальной войны против России и её союзников, включая инспирирование «пятой колонны».

Сложившаяся ситуация чревата серьезными угрозами международному миру и безопасности. По этой причине мы предложили обсудить данную проблему на отдельном **Круглом столе № 5 «Сотрудничество в области противодействия вмешательству во внутренние дела суверенных государств с использованием средств массовой коммуникации».**

Уважаемые коллеги!

В заключение доклада хочу сообщить, что в работе нашего Форума высказали пожелание принять участие около 250 ученых и экспертов из 14 стран, а также представители ряда уважаемых международных организаций.:

Приятно отметить, что существенно расширилось участие российских экспертов в обсуждении проблем МИБ.

Благодарю за внимание!»

О.В. Храмов

Заместитель Секретаря Совета безопасности Российской Федерации, Председатель Наблюдательного Совета НАМИБ

Доброе утро, уважаемые коллеги!

Сегодня начинает работу XV Международный форум «Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности».

Национальная Ассоциация международной информационной безопасности традиционно собрала на площадке Форума ведущих профессионалов в области международной информационной безопасности – представителей органов власти, научного и экспертного сообщества, деловых кругов из России и иностранных государств.

Позвольте огласить приветствие Секретаря Совета Безопасности Российской Федерации Николая Платоновича Патрушева организаторам и участникам Форума (Приветствие Секретаря Совета Безопасности Российской Федерации Николая Платоновича Патрушева).

В этом году организаторы Форума вынесли на обсуждение приоритетные направления сотрудничества в области формирования системы международной информационной безопасности.

Нарастающие вызовы и угрозы безопасности в информационной сфере, невозможность борьбы с ними в одиночку обусловливают потребность консолидации усилий мирового сообщества на этом направлении.

Поэтому сотрудничество государств на всех уровнях – глобальном, региональном, многостороннем и двустороннем – становится приоритетной задачей.

Российские инициативы в области международной информационной безопасности нацелены на формирование прочного фундамента упомянутой системы – гаранта безопасности и стабильности глобального информационного пространства.

В числе этих инициатив – обновленная концепция Конвенции Организации Объединенных Наций об обеспечении международной информационной безопасности.

Дискуссии на площадке профильной Рабочей группы открытого состава, завершившей свою работу в марте этого года, продемонстрировали поддержку предложения России о принятии под эгидой ООН международного правового акта, регулирующего деятельность государств в указанной области.

Аналогичной поддержкой пользуются и другие российские проекты, которые будут представлены на Форуме.

Также в центре предстоящих дискуссий – двустороннее сотрудничество России, которое, как показывает опыт взаимодействия с зарубежными партнерами, является наиболее эффективным и практико-ориентированным.

Непосредственные контакты в таком формате позволяют снять напряженность в отношениях, укрепить доверие, совместно решать актуальные проблемы обеспечения информационной безопасности, выступать с единых позиций на различных международных площадках.

Рассчитываем, что хорошим подспорьем для государственных органов в ходе трехдневной работы Форума станет экспертная проработка указанных проблем, поиск действенных мер по их решению, выход на конкретные практические результаты.

Благодарю за внимание.

Чен Жимин

Председатель Всекитайской Ассоциации по содействию дружбы

Уважаемый Владислав Петрович!

Всекитайская народная ассоциация содействия дружбе свидетельствует Вам глубокое уважение.

Очень приятно получить от Вас приглашение. Это большая честь для нас.

Разрешите выразить горячие поздравления в связи с проведением Пятнадцатого Международного Форума «Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности». Это важное событие, которое пользуется в научных кругах прекрасной репутацией и оказывает значительное влияние на экспертов всего мира. На заседаниях Форума собираются многие известные специалисты и ученые, получены крупные результаты.

Как Вам известно, кроме председателя Всекитайской народной ассоциации содействия дружбе, я являюсь еще членом руководства Народного Политического Консультативного Совета Китая. По плану работы Совета с сентября мне поручено возглавить рабочую группу по обследованию разных регионов страны. Очень жаль, что не смогу принять участия в Вашем Форуме. Заранее поздравляю вас с его успешным проведением.

Охватившая планету пандемия COVID-19, к сожалению, оказала влияние на наше сотрудничество, но перспективы его расширения в будущем весьма обширны. Нас очень интересует сетевая безопасность и мы ожидаем продолжения сотрудничества в подходящее время после эпидемии.

С уважением, Чен Жимин,

Председатель Всекитайской Ассоциации по содействию дружбе

Ю.А. Ясносокирский
Начальник отдела ООН и глобальных форумов департамента международной информационной безопасности МИД России

ДЕЯТЕЛЬНОСТЬ РОССИЙСКОЙ КИБЕРДИПЛОМАТИИ ПО ВОПРОСАМ ОБЕСПЕЧЕНИЯ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ПЛОЩАДКАХ ООН

Уважаемые дамы и господа, коллеги!

Рад приветствовать участников и гостей форума!

Информационно-коммуникационные техно-логии (ИКТ) давно стали неотъемлемой частью повседневной жизни каждого из нас. Вместе с тем наряду с безусловными преимуществами технологический прогресс всегда влечет за собой новые вызовы и угрозы. В последние годы интерес к теме обеспечения международной информационной безопасности (МИБ) неуклонно растет. Отрадно отметить, что Российская Федерация движется в авангарде этого глобального тренда. С гордостью можно сказать, что в этих вопросах России исторически принадлежит инициативная роль, прежде всего, в рамках самой авторитетной и представительной международной организации – ООН. Еще в 1998 г. Россия первой с трибуны Всемирной Организации предупредила мир о зарождающихся киберугрозах и предложила путь противодействия им. Наша страна продолжает активно и успешно продвигать различные инициативы в профильном глобальном переговорном процессе под эгидой ООН, эффективно отстаивая национальные интересы и подходы. Именно некоторым аспектам нашей деятельности на ооновской площадке, я и хотел бы посвятить свое сегодняшнее выступление.

Ситуация с распространением в мире коронавирусной инфекции внесла существенные коррективы во все сферы, включая нашу политико-дипломатическую работу и повседневную жизнь. Перевод на удаленный режим государственных учреждений, частных компаний, образовательных и научных организаций обнажил фактически всеобъемлющую зависимость человечества от ИКТ и наглядно продемонстрировал и увеличил уязвимость всех государств перед лицом острых глобальных проблем вне зависимости от их политической ориентации и уровня экономического развития.

В данном контексте как никогда возросла значимость международного сотрудничества. Россия последовательно выступает инициатором объединения международного сообщества для совместного поиска путей и способов решения проблем в области безопасности в сфере использования ИКТ и самих ИКТ путем выработки на международной арене правил, норм и принципов ответственного поведения государств, мер укрепления доверия, повышения предсказуемости киберсреды.

Большим вкладом в реализацию этой идеи стала выработка 11 правил, норм и принципов ответственного поведения государств, которые были согласованы в 2015 г. учрежденной по инициативе России Группой правительственных экспертов (ГПЭ) ООН. Они вошли в свод международных правил, норм и принципов, закрепленный в российской резолюции Генеральной Ассамблеи ООН в 2018 г., которую поддержало подавляющее большинство международного сообщества.

Эти правила, рекомендованные к соблюдению всеми государствами, направлены на предотвращение межгосударственных конфликтов и включают такие важные положения как использование ИКТ в мирных целях, обоснованность обвинений выдвигаемых против

государств, ответственность государств за деятельность на их территории, и из их информпространства.

Важным шагом на пути к построению прозрачной и эффективной системы МИБ послужило создание по нашей инициативе в 2018 г. Рабочей группы ООН открытого состава (РГОС) по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности. Кстати, в ответ наши заокеанские партнеры абсолютно беззастенчиво использовали нашу идею и в том же году воссоздали формат ГПЭ (с 25 участниками) в качестве параллельного, дублирующего РГОС трека.

Несмотря на нагнетание отдельными государствами международной обстановки в области информационной безопасности очередным успехом российской дипломатии стало окончание работы первой РГОС. Без преувеличения исторический процесс РГОС завершился принятием 12 марта с.г. консенсусного итогового доклада.

Все 193 государства-члена ООН поддержали текст доклада, подводящего итог двухлетней работы Группы. При этом большинством участников была отмечена ключевая роль России в организации переговорного процесса под эгидой ООН в данном формате.

Доклад сбалансированно отражает основные элементы состоявшихся дискуссий, причем тематика МИБ корректно подается через призму повестки дня Первого комитета Генеральной Ассамблеи ООН (вопросы глобального мира и безопасности).

В документе закреплены базовые подходы, продвигаемые Россией и ее партнерами в области МИБ, – предотвращение конфликтов в информационном пространстве, недопущение его милитаризации и использование информационно-коммуникационных технологий (ИКТ) исключительно в мирных целях. В нем также четко подтверждаются ранее достигнутые международным сообществом договоренности в данной сфере по правилам, нормам и принципам ответственного поведения государств, зафиксированные в докладах профильных ГПЭ и расширенные российской резолюцией Генеральной Ассамблеи №73/27 2018 г. При этом предусмотрена возможность выработки новых правил и норм, в том числе юридически обязывающего характера.

Доклад признает политическую значимость и практическую полезность РГОС и содержит важнейшую рекомендацию о необходимости продолжения переговорного процесса по МИБ под эгидой ООН в рамках данного механизма в ближайшие пять лет. Кроме того, именно в нем будет сосредоточено рассмотрение всех профильных инициатив государств.

Столь успешное завершение деятельности РГОС транслирует позитивный сигнал о стремлении международного сообщества совместными усилиями решать наиболее острые глобальные проблемы.

28 мая 2021 г. принятием итогового консенсусного доклада завершила свою работу. Для нас важно, что в нем учтены принципиальные российские подходы к обеспечению МИБ, в том числе по наиболее острым вопросам – атрибуции инцидентов в ИКТ-сфере, международно-правовому регулированию данной области, необходимости дальнейшей работы под эгидой ООН над правилами ответственного поведения государств, а также возможности выработки юридически обязывающих норм. В докладе также признается значимость продолжения глобальной дискуссии по МИБ, в частности, в формате новой РГОС по вопросам безопасности в сфере использования ИКТ и самих ИКТ 2021-2025, созданной во исполнение принятой по инициативе России в 2020 г. резолюции ГА ООН 75/240.

Уже 1-го июня с.г. состоялась организационная сессия новой РГОС по вопросам безопасности в сфере использования ИКТ и самих ИКТ 2021–2025.

Мандат Группы предусматривает в качестве приоритета продолжение дальнейшей выработки норм, правил и принципов ответственного поведения государств в информационном пространстве и путей их имплементации, при необходимости, внесения в них изменений или формулирования дополнительных правил поведения; рассмотрение инициатив государств, направленных на обеспечение безопасности в сфере использования ИКТ;

и организацию под эгидой ООН регулярного институционального диалога

с широким кругом государств-участников. Помимо этого, РГОС призвана продолжить выработку общего понимания исследования существующих и потенциальных угроз в сфере информационной безопасности, в том числе

безопасности данных, и возможных совместных мер по их предотвращению и противодействию им, а также общего понимания того, как международное право применяется к использованию ИКТ государствами, мер укрепления доверия и наращивания потенциала.

В ходе заседания консенсусно одобрены ключевые модальности деятельности Группы. Ее председателем избран Постоянный представитель Сингапура при ООН в Нью-Йорке Б. Гафур. Утверждены повестка дня РГОС и правила ее процедуры, включая метод принятия решений консенсусом. Другие организационные вопросы председатель планирует согласовать в рамках широких консультаций с государствами-членами ООН и одобрить их на первой субстантивной сессии Группы (Нью-Йорк, 13-17 декабря 2021 г.).

Государства поддержали российское видение деятельности Группы на основе принципов универсальности, открытости, транспарентности и демократичности, а также ориентированности на достижение практических результатов.

В мае 2021 г. с подачи России был запущен Спецкомитет ООН для разработки универсальной конвенции по противодействию использованию ИКТ в преступных целях. Думаю, что этот вопрос осветят мои коллеги. (Резолюция Генеральной Ассамблеи ООН 75/282 о плане и порядке работы спецкомитета была принята консенсусом, что свидетельствует о признании международным сообществом необходимости выработки такого документа. А ведь еще полтора года назад приходилось преодолевать серьезное сопротивление ряда западных стран, чтобы продвинуть соответствующее решение Генассамблеи ООН).

Подытоживая свое выступление, отмечу, что мы и дальше самым активным и конструктивным образом намерены участвовать в переговорном процессе по МИБ. Новым явлением этого процесса станет активное подключение к нему бизнеса (Об этом более подробно остановится Ольга Андреевна Мельникова, начальник Отдела невоенных аспектов использования ИКТ ДМИБ МИД России).

Пользуясь случаем, хотел бы еще раз поблагодарить организаторов этого замечательного форума за неформальный подход и интересную дискуссию!

Благодарю за внимание!

С.П. Юниченко
Эксперт Министерства обороны Российской Федерации

О НЕКОТОРЫХ АСПЕКТАХ НЕВООРУЖЕННОГО ВМЕШАТЕЛЬСТВА ВО ВНУТРЕННИЕ ДЕЛА ДРУГИХ ГОСУДАРСТВ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ[1]

Уважаемые коллеги!

Виды вмешательства во внутренние дела других государств обозначены в нескольких резолюциях Генеральной ассамблеи ООН[2]. Условно можно разделить все виды вмешательства на вооруженные и невооруженные.

В отношении вооруженного вмешательства на сегодняшний день в международном праве значительно больше ясности. Этот вид вмешательства отождествлен с агрессией, определению которой посвящена отдельная резолюция Генеральной ассамблеи ООН[3].

О содержании «невооруженного вмешательства» можно судить только по косвенным признакам. В упомянутых резолюциях к ним отнесены экономические, политические, подрывные и иные меры, осуществляемые с целью подчинения себе другого государства в осуществлении им своих суверенных прав или насильственного свержение строя другого государства[4]. Среди видов невооруженного вмешательства названы те, которые ныне практически немыслимы без широкомасштабного использования информационно-коммуникационных технологий (ИКТ) – это «клеветнические кампании, оскорбительная или враждебная пропаганда с целью осуществления интервенции, или вмешательства во внутренние дела других государств»[5]. Иными словами, речь идет о распространении различного дезинформации и пропаганды, нацеленной на создание атмосферы враждебности, эскалацию напряженности, побуждение населения к массовым беспорядкам, осуществлению экстремистской деятельности, участию в массовых (публичных) мероприятиях, проводимых с нарушением установленного порядка и т.п.

Для эффективного противодействия невооруженному вмешательству во внутренние дела других государств необходимо сформировать соответствующую прочную международно-правовую основу. В настоящее время отдельные ее элементы уже имеются. В частности, к ним можно отнести отдельные положения упомянутых выше резолюций.

Например, обязанностью государств признана борьба «против распространения фальшивых или искаженных сообщений, которые могут рассматриваться как вмешатель-

1 Выступление подготовлено коллективом экспертов Минобороны России в области международной информационной безопасности в составе: Дылевский И.Н., Базылев С.И., Запивахин В.О., Комов С.А., Юниченко С.П., Шевченко А.Л., Завьялов Е.К., Каргин М.Н.

2 Декларация о недопустимости вмешательства во внутренние дела государств, об ограждении их независимости и суверенитета. Принята резолюцией 2131 (XX) Генеральной Ассамблеи от 21 декабря 1965 года;
Декларация о принципах международного права, касающихся дружественных отношений и сотрудничества между государствами в соответствии с Уставом Организации Объединенных Наций. Принята резолюцией 2625 (XXV) Генеральной Ассамблеи ООН от 24 октября 1970 года;
Декларация о недопустимости интервенции и вмешательства во внутренние дела государств. Принята резолюцией 36/103 Генеральной Ассамблеи от 9 декабря 1981 года.

3 Определение агрессии. Утверждено резолюцией 3314 (XXIX) Генеральной Ассамблеи от 14 декабря 1974 года.

4 Статья I Декларации о принципах международного права, касающихся дружественных отношений и сотрудничества между государствами в соответствии с Уставом Организации Объединенных Наций. Принята резолюцией 2625 (XXV) Генеральной Ассамблеи ООН от 24 октября 1970 года;

5 Статья 2 II j) Декларации о недопустимости интервенции и вмешательства во внутренние дела государств. Принята резолюцией 36/103 Генеральной Ассамблеи от 9 декабря 1981 года.

ство во внутренние дела других государств или как наносящие ущерб укреплению мира, сотрудничества и дружественных отношений между государствами и нациями»[6].

Вмешательством во внутренние дела других государств будет распространение информации, содержащей «угрозы применения силы против территориальной неприкосновенности или политической независимости любого государства»[7] или нацеленной на «подстрекательство подрывной, террористической или вооруженной деятельности, направленной на насильственное свержение строя другого государства»[8].

Частично это вопрос также проработан в Дополнительном протоколе к Конвенции Совета Европы о киберпреступности применительно к криминализации пропаганды расизма и ксенофобии, а также одобрения или оправдания геноцида или преступлений против человечества. В этом документе закреплено положение о криминализации использования ИКТ, которое способствует или подстрекает к дискриминации, связанной с ненавистью или насилием и проведением в обществе каких-либо разделительных линий.

Таким образом, невооруженным вмешательством во внутренние дела других государств с использованием ИКТ может считаться:

- подстрекательство подрывной, террористической или вооруженной деятельности, направленной на насильственное свержение строя другого государства;
- призывы к дискриминации, связанной с ненавистью или насилием и проведением в обществе каких-либо разделительных линий;
- оправдание геноцида или к совершения преступлений против человечества, в том числе пропаганда агрессивной войны.

Анализ этих деяний свидетельствует о том, что основное значение при определении содержания невооруженного вмешательства во внутренние дела других государств с использованием ИКТ следует считать направленность этих действий на призывы к применению силы или оправдание такого применения, а также возбуждение в обществе ненависти и насилия.

С практической точки зрения, представляется целесообразным обсуждение тематики «невооруженного вмешательства во внутренние дела других государств с использованием ИКТ» включить в повестку дня всех международных форматов, рассматривающих вопросы обеспечения международной информационной безопасности (ООН, ОБСЕ, АРФ и др.).

Благодарю за внимание!

6 Статья III d) Декларации о недопустимости интервенции и вмешательства во внутренние дела государств, принятой резолюцией 36/103 Генеральной Ассамблеи ООН от 9 декабря 1981 года.

7 Пункт 4 статьи 2 Устава ООН.

8 Статья I Декларации о принципах международного права, касающихся дружественных отношений и сотрудничества между государствами в соответствии с Уставом ООН, принятая резолюцией 2625 (XXV) Генеральной Ассамблеи ООН от 24 октября 1970 года.

Анн-Мари Бузату
Вице-Президент Фонда ICT4Peace (Швейцария)

ОБЕСПЕЧЕНИЕ ДОВЕРИЯ И ПОДОТЧЕТНОСТИ МЕЖДУ ГОСУДАРСТВАМИ В ИНТЕРЕСАХ МИРНОГО КИБЕРПРОСТРАНСТВА

Уважаемые Превосходительства, Дамы и Господа, Уважаемые Коллеги,

Для меня большая честь получить приглашение и выступить на данной сессии «Сотрудничество в области предотвращения военных конфликтов и мирного урегулирования споров в ИКТ-среде».

Хотя начало было положено еще до моего пребывания в ICT4Peace, я наслышана о раннем сотрудничестве нашего Фонда с российскими экспертами в определении норм поведения государств в киберпространстве. В частности, я говорю о нашем совместном проекте и докладе, именуемом «Методологические вопросы применения норм, правил и принципов ответственного поведения государств» под редакцией профессора А.А. Стрельцова и доктора Энекен Тикк. Этот доклад был опубликован и широко распространен. ICT4Peace гордится тем, что участвовал в этих слишком редких совместных усилиях российских и западных экспертов по изучению будущего кибернетических норм с партнерами из России, Соединенных Штатов, Эстонии и Швейцарии.

Едва ли Вас удивит, если я, как Вице-президент организации гражданского общества ICT4Peace, подойду к сегодняшней теме с позиции, изначально вдохновляющей ICT4Peace – киберпространство, посвященное мирной деятельности. Несмотря на печальную историю злонамеренных и наступательных кибероперациий, проводимых как государствами, так и негосударственными субъектами, мы никогда не должны забывать, что уникальная, созданная человеком среда киберпространства может быть сохранена в мирных целях, если мы коллективно выступаем и действуем, исходя из них.

Исключительным достижением Организации Объединенных Наций в отношении ограничений наступательных кибероперациий стало соглашение 2015 года о своде норм ответственного поведения государств в киберпространстве. Одиннадцать норм стали консенсусным итогом работы Группы правительственных экспертов ООН (ГПЭ). Они легли в основу доклада, который впоследствии был поддержан в резолюции Генеральной Ассамблеи ООН (также принятой посредством консенсуса), рекомендующей государствам руководствоваться указанными результатами деятельности ГПЭ ООН при использовании ими информационно-коммуникационных технологий (ИКТ).

Особо значимой среди этих норм была та, которая запрещала кибератаки на критически важную инфраструктуру, от которой напрямую зависит общество. Тот факт, что эта норма была разработана членами ГПЭ ООН, в состав которой входили представители всех пяти постоянных членов Совета Безопасности ООН (всех держав, обладающих значительными наступательными кибернетическими возможностями), давал основания надеяться, что данная сдерживающая норма будет соблюдаться на практике.

Мы сожалеем, что, несмотря на столь многообещающее начало, наша надежда – что государства, обладающие наступательными кибернетическими возможностями, будут соблюдать норму о ненападении на критическую инфраструктуру, под которой они подписались, – не оправдалась. Почти ежедневно поступают достоверные сообщения о киберпреступлениях, нарушениях нормального функционирования и временами фактическом повреждении

критически важной инфраструктуры в результате наступательных кибероперaций, многие из которых спонсируются или проводятся государством.

Тот факт, что сектор здравоохранения был активно атакован во время пандемии COVID-19, стал причиной оправданного возмущения по всему миру. Но мы не должны сводить общий запрет нападения на критическую инфраструктуру только к тем элементам, которые имеют медицинский логотип. Безусловно, сектор здравоохранения является важнейшим элементом критически важной инфраструктуры, но, если мы будем оценивать его в качестве единственной государственной службы, заслуживающей защиты, мы умалим обязательство защищать всю критически важную инфраструктуру. Не нужно быть экспертом по кибербезопасности, чтобы понять, насколько разрушительными для общества могут быть кибератаки на такие объекты инфраструктуры, как энергетические сети, водоочистные сооружения, транспортные узлы и ядерные объекты.

Нас обнадеживает тот факт, что Рабочая Группа открытого состава ООН (РГОС ООН) в своем заключительном докладе в марте 2021 года подтвердила норму о защите критической инфраструктуры в полном объеме. Эта жизненно важная норма ограничения поведения государства в киберпространстве должна соблюдаться во всей ее полноте, и организации гражданского общества наряду с ответственными правительствами и компаниями должны публично настаивать на этом защитном статусе для всей критически важной инфраструктуры.

ICT4Peace выступает за активное подтверждение государствами своей приверженности соблюдению нормы о ненападении на критическую инфраструктуру. В 2019 году мы инициировали «Призыв к правительствам» – с целью официального подтверждения соблюдения государствами данной ключевой нормы. В то время, когда международное сообщество занято пандемией, крайне важно, чтобы норма о защите критически важных объектов инфраструктуры была усилена, а не ослаблена.

Однако то, что норма подтверждена, не означает, что она будет соблюдаться на практике. Для стимулирования государств к выполнению своих обязательств необходим определенный механизм привлечения государств к ответственности за их кибероперации, затрагивающие другие государства. Такой механизм представлял бы собой процесс сотрудничества, который был бы ориентирован на государство, а также предусматривающий участие других заинтересованных сторон, представляющих подавляющее большинство пользователей и владельцев Интернета.

Среди существующих моделей механизм Универсального периодического обзора Совета по правам человека применим к контексту кибербезопасности при условии его объединения с взаимными проверками под руководством государств, а также обеспечения при этом участия частного сектора и гражданского общества.

В связи с этим ICT4Peace в своем докладе Рабочей Группе открытого состава ООН предложила «Механизм экспертной оценки (коллегиального обзора) киберпространства», который, по нашему мнению, является легко реализуемой формой обеспечения подотчетности государств за поведение в киберпространстве, поскольку он основывается на существующем, хорошо функционирующем механизме структуры ООН. Эта базовая структура будет отвечать принципу прозрачного, управляемого государством механизма оценки и обзора, включающего вклад гражданского общества и частного сектора.

Это также позволило бы растущему числу государств, обладающих возможностями для проведения наступательных кибероперaций, заверить международное сообщество в том, что эти возможности используются в соответствии с международным правом и согласованными нормами ООН об ответственном поведении государств. Создание такого механизма экспертной оценки (коллегиального обзора) киберпространства должно стать ближайшей целью международного сообщества.

РГОС ООН только что была продлена еще на пять лет, но мы считаем, что государства могли бы уже сейчас начать инициировать многосторонние переговоры, которые принесли бы конкретные результаты. Несколько государств, участвующих в РГОС, предложили «Программу действий» по кибербезопасности. Переговоры по такой программе действий должны начаться скорее раньше, чем позже. События в реальном мире указывают на необходимость ускорения темпов действий ООН по предотвращению обострения онлайн-конфликтов.

Программа Действий предусматривает создание постоянного Форума ООН по вопросам кибербезопасности. ICT4Peace уже давно призывает к подобному институциональному проявлению важности кибердеятельности для глобальной безопасности и благополучия. Мы считаем, что пришло время создать постоянный Комитет по кибербезопасности при Генеральной Ассамблее ООН и обеспечить поддержку данного Форума со стороны Управления ООН по кибербезопасности.

Дальнейшие усовершенствования мер укрепления доверия для обеспечения прозрачности и предсказуемости могут быть включены в потенциальную Программу действий. Меры укрепления доверия уже давно способствуют снижению уровня недоверия между государствами, находящимися в противоборствующих отношениях. Процесс ГПЭ ООН уже привел к созданию ряда мер укрепления доверия, а такие региональные организации, как ОБСЕ, ОАГ и АСЕАН, продолжили деятельность по созданию мер укрепления кибербезопасности. Как и в случае с нормами, простого присоединения к набору мер укрепления доверия недостаточно – для мониторинга их реализации требуются отслеживающие механизмы. Именно поэтому ICT4Peace подчеркивает важность механизмов подотчетности и институциональной поддержки для стимулирования государств к выполнению своих политических обязательств по обеспечению реализации согласованных мер укрепления доверия в политике и на практике.

Ощутимая поддержка наращивания потенциала в области кибербезопасности также должна фигурировать в любой возможной программе действий. В связи с этим ICT4Peace выступает за то, чтобы Комитет содействия развитию (КСР) Организации экономического сотрудничества и развития (ОЭСР) обеспечил предоставление кредитов в рамках официальной помощи в целях развития (ОПР) для финансирования расходов на укрепление потенциала. Если мы серьезно настроены на преодоление цифрового разрыва и предоставление развивающимся странам возможности равного участия в многосторонних форумах по кибербезопасности, международным организациям необходимо предпринять шаги для содействия финансированию со стороны доноров.

Любая возможная Программа Действий по международной кибербезопасности должна будет противостоять нынешнему зияющему пробелу в подотчетности. Если на кибердержавы будет оказано давление, чтобы они вели себя ответственно, участвуя в кибероперациях за пределами своих границ, международному сообществу для обеспечения подотчетности необходимо будет применять всеобъемлющий механизм обзора действий государств посредством прозрачного процесса с участием многих заинтересованных сторон.

Подотчетность и атрибуция кибератак идут рука об руку – мы не можем достичь первого без второго. Понятно, что суверенные государства желают сохранить атрибуцию в качестве национальной прерогативы, но, учитывая присущую им предвзятость, исключительно национальный подход не получит достаточного доверия.

Нам необходимо разработать независимый механизм для получения выводов об атрибуции, основанных на фактических данных. Как уже видно из многочисленных отчетов о киберугрозах, подготавливаемых компаниями по кибербезопасности, в этом направлении существуют широкие возможности для доступа к возможностям частного сектора.

На раннем этапе работы РГОС ICT4Peace представляла предложение с изложением возможного подхода, учитывающего технические и политические проблемы, связанные с эффективной атрибуцией, и предложила простую идею по улучшению, а именно – создание независимой сети организаций, занимающихся экспертной оценкой атрибуции. Нам нужно продумать, как подобная автономная сеть атрибуции может быть подключена к официальным многосторонним процессам для рассмотрения инцидентов на основе эмпирических данных.

Когда мы смотрим на современный киберландшафт, деформированный постоянно растущими киберугрозами, связанными с безопасностью человека и нарушением согласованных норм, становится ясно, что мировому обществу приходится решать множество проблем. В то же время растет число действующих лиц в правительствах и за их пределами, которые разрабатывают творческие решения этих проблем. Если мы хотим восстановить киберпространство в интересах мира и устойчивого развития, нам потребуются согласованные усилия всех заинтересованных сторон.

Спасибо!

Дэниел Вурм
Генеральный директорат оборонной политики, Федеральное министерство обороны (Австрия)

ПРЕДОТВРАЩАЯ КИБЕРКОНФЛИКТЫ ПОСРЕДСТВОМ ПРОЗРАЧНОСТИ

Прозрачность имеет ключевое значение при обсуждении возможностей предотвращения киберконфликтов в будущем. В нашем современном цифровом мире злонамеренное использование кибертехнологий создает угрозу глобальной безопасности. Таким образом, возникновение киберконфликтов не является надуманным, но уже является проблемой, которую нам необходимо обсудить. Поэтому я утверждаю, что обеспечение прозрачности в киберпространстве является ключом к предотвращению киберконфликтов в долгосрочной перспективе.

Итак, что означает прозрачность в киберпространстве и как ее можно достичь? Для ответа на этот вопрос многосторонний подход, международное право и киберпотенциал – три ключевые сферы, которые необходимо принять во внимание для дальнейшего обсуждения.

1) Прозрачность посредством многостороннего подхода

Многосторонний подход означает способность эффективно реагировать на глобальные угрозы и общие вызовы посредством как институционализированного, так и неинституционализированного сотрудничества между государствами и всеми другими соответствующими заинтересованными сторонами.

В киберпространстве этого можно достичь посредством следующих действий:

- Содействие диалогу по кибербезопасности, обеспечение широкой поддержки на международных форумах (таких как Рабочая группа открытого состава ООН) для достижения общего понимания, а также применения норм и принципов в киберпространстве, внедрение мер укрепления доверия в институты и укрепление кибердипломатии между всеми государствами. Все эти меры являются важным первым шагом для укрепления доверия друг к другу, что является необходимым условием для всех дальнейших шагов.
- Укрепление глобального управления Интернетом также имеет важное значение. Поэтому необходимо поддерживать существующие платформы, такие как Форум по управлению Интернетом, с участием всех соответствующих заинтересованных сторон в киберпространстве, включая представителей бизнеса и гражданского общества. Особенно негосударственные субъекты, такие как технологические компании, играют важную роль в цифровой сфере и должны быть включены в дискуссии о будущем Интернета, соответственно киберпространства.
- Кроме того, необходимо и далее укреплять и обновлять Международное право и Международное гуманитарное право при решении проблем и использовании возможностей в таких областях, как кибербезопасность и новые технологии, включая искусственный интеллект, дезинформацию, защиту данных и конфиденциальность.

2) Прозрачность посредством введения в действие международного права (должная осмотрительность)

То, что мы видим сейчас, – это возрождение дискуссии о суверенитете в различных областях. Для киберпространства это означает, что мы должны признать тот факт, что цифровой суверенитет возможен только при

наличии минимальной степени контроля над технологическими ресурсами, которые обязательно используются – от узлов Интернета и облачной инфраструктуры до установления международных стандартов.

Этот процесс сохранения суверенитета в киберпространстве может быть достигнут только в рамках международного права, которое, следовательно, нуждается в обновлении и применении в связи с растущими вызовами, возникающими в киберпространстве.

Для того чтобы ввести в действие международное право, мы должны:

- усилить принцип должной осмотрительности в киберпространстве, что означает, что все государства серьезно относятся к своим обязательствам по предотвращению вредоносных инцидентов и злонамеренного использования киберпространства и критически важной инфраструктуры в пределах своего территориального суверенитета для нападения на третьи стороны.
- Кроме того, прозрачная атрибуция неизбежна для содействия практической реализации международного права. Поскольку, не зная о происхождении, серьезности и намерениях нападения, невозможно должным образом отреагировать. Это требует лучшего и прозрачного понимания применимости таких принципов международного права, как разграничение, пропорциональность и необходимость. Для обеспечения прозрачной атрибуции крайне важно, чтобы все государства определили и обнародовали свои национальные критерии и интерпретацию атрибуции.
- Одновременно все государства также должны определить и обнародовать свое понимание пороговых значений вооруженных атак в киберпространстве. Только установив четкие пороговые значения и назвав критерии для них, государства могут укрепить взаимное доверие и понять красные линии друг друга. Это может непосредственно поддержать и усилить вышеупомянутые аспекты мер укрепления доверия и кибердипломатии.
- Когда мы обсуждаем киберконфликты, нам также необходимо учитывать будущие технологические разработки, которые изменят характер киберпространства, такие как искусственный интеллект или Квантовые технологии, и это лишь некоторые из них. В долгосрочной перспективе мы столкнемся со слиянием реального (физического) и виртуального (логического) мира, что изменит методы конфликта в будущем.

Давайте рассмотрим три реальных примера технологических разработок, о которых я говорю:

- во-первых, дальнейшее углубление взаимодействия человека и машины изменит будущие поля сражений, а также системы военной поддержки, например, для улучшения процессов принятия решений;
- во-вторых, совершенствование человека, означающее улучшение человеческих способностей, таких как нейрональные интерфейсы, для повышения способности так называемых «суперсолдат» видеть, чувствовать, слышать или понимать события, которые были бы слишком сложными для человеческого разума;
- и, наконец, нейро- и биотехнологические системы приведут к новым формам ведения войны, таким как когнитивная война, непосредственно затрагивающая умы и мысли людей, которую ученые также называют «взломом мозга».

Если мы не адаптируем наши существующие нормы и принципы, эти разработки снизят барьер применения силы ниже установленного в настоящее время порога вооруженных нападений и, таким образом, создадут проблемы для практической реализации международного права.

3) Транспарентность в процессе укрепления киберпотенциала и возможностей в области безопасности

Киберпотенциал и возможности должны быть развиты по всему спектру кибернетических вопросов и включать кибербезопасность, киберзащиту и кибердипломатию. Это важно для обеспечения должной осмотрительности в целях предотвращения кибератак и создания зависимостей. Поэтому разумное развитие киберпотенциала и возможностей для обнаружения, определения

и управления киберинцидентами имеет решающее значение.

Эти киберпотенциал и возможности – особенно с учетом того, что различие между оборонительными и наступательными возможностями постоянно размывается – должны разрабатываться под эгидой международного права, чтобы предотвратить неконтролируемую милитаризацию киберпространства. При этом, развитие возможностей киберзащиты является законным, но должно быть прозрачным и в идеале – происходить в рамках общепринятого режима контроля над вооружениями. Это требует функциональной многосторонности и соблюдения международного права в качестве предварительного условия.

Заключение

В заключение следует отметить, что прозрачность необходима для успешного предотвращения киберконфликтов в будущем. Для достижения прозрачности ключевое значение имеют многостороннее взаимодействие и укрепление международного права.

Кроме того, развитие киберпотенциала и возможностей также необходимо, важно и законно. Только если государства будут обладать возможностями для обнаружения, определения и защиты от кибератак, они смогут сохранить свой суверенитет в цифровой сфере, выполнять свои обязательства по должной осмотрительности, быть устойчивыми, определять и объявлять четкие красные линии (так называемые пороги) и, следовательно, снижать вероятность возникновения киберконфликтов.

Если нам удастся обеспечить прозрачность на глобальном уровне во всех упомянутых мною областях, киберконфликты с гораздо большей вероятностью будут предотвращены в будущем.

О.Г. Карпович
Проректор по научной работе
Дипломатической академии МИД России,
д.ю.н., д.полит.н., профессор

МИР ЦИФРОВОГО БУДУЩЕГО СТАНЕТ ИНЫМ?

Сегодня мы наблюдаем стремительный перевод в цифровую сферу многих аспектов повседневной жизни, включая государственное управление, бизнес, образование. Не отстают от этой тенденции и межгосударственные связи. Более того, значительно возрастает скорость внедрения прорывных технологий и обеспечение широкого доступа к ним.

Все это открывает большие возможности, но несет и немалые риски. Поэтому закономерно, что вопросы надежного обеспечения международной информационной безопасности (МИБ) выходят на передний план глобальной повестки дня.

Увы, на текущий момент ситуация в этой области далека от идеальной. Мировое сообщество сталкивается с самой настоящей «киберпандемией», которая проявляется не только в виде посягательства на частную жизнь рядовых граждан. Глубокую озабоченность вызывают акты кибертерроризма, рост количества «нападений» на международные организации, органы государственной власти, финансовые, образовательные структуры, объекты здравоохранения. Преступная активность в онлайн-режиме угрожает существованию и успешному функционированию целых отраслей.

Беспокойство вызывает намерение отдельных стран милитаризировать «Интернет», развязать гонку кибервооружений. Они не стесняются публично рассуждать о своем «праве» наносить превентивные кибердары по потенциальным противникам, в том числе по объектам их критической инфраструктуры. В этом контексте информационно-коммуникационные технологии (ИКТ) все чаще используются в целях вмешательства во внутренние дела суверенных государств, занимая первое место среди обширного инструментария «цветных революций».

В частности, применительно к России, ИКТ уже давно используются коллективным Западом в рамках агрессивной линии на сдерживание нашей страны. Для максимально возможного ослабления и замедления ее развития путем создания внутренней нестабильности и «горячих точек» по периметру наших границ.

Как Вы знаете, сейчас особое внимание наших геостратегических противников приковано к прошедшим недавно выборам депутатов Государственной Думы. В интернете и мессенджерах предпринимались шаги по координации действий российской внесистемной оппозиции, стимулированию протестной активности населения. В киберсфере начались информационные атаки с целью поставить под сомнение итоги голосования и легитимность нового состава высшего законодательного органа власти в России.

Все это – в том числе и последствия уязвимостей, связанных с отсутствием универсального международного «кодекса поведения» в киберсфере. В этих условиях устойчивое социально-экономическое и научно-техническое развитие всех без исключения стран оказывается под ударом. Человечество рискует быть втянутым в опасную масштабную конфронтацию в онлайн-пространстве, которую невозможно будет удержать в локальных рамках в силу трансграничности современных средств коммуникаций и взаимозависимости национальных экономик.

Очевидно, что мировому сообществу давно пора сделать должные выводы относи-

тельно того, как цивилизованно, не в ущерб прогрессу, основным правам человека и свободам следует применять ИКТ и регулировать деятельность государств в данной области. На достижение этой цели ориентированы российские принципиальные подходы.

Продолжаем напоминать всем нашим партнерам, что еще более 20 лет назад, в 1998 году, Россия – с трибуны ООН – первой предупредила мир о рисках, которые таила в себе тогда еще зарождающаяся киберсфера, и предложила конкретные пути противодействия. Сегодня наша позиция остается неизменной и сводится к следующему:

- в решении и обсуждении данной глобальной проблемы должны участвовать все без исключения государства. Важен учет мнений всех заинтересованных сил (бизнес, гражданское общество, научные круги);
- поиск универсального решения возможен только путем переговоров под эгидой Всемирной Организации;
- магистральная цель таких переговорных усилий – предотвращение конфликтов в информационном пространстве и обеспечение использования ИКТ исключительно в мирных целях. В связи с этим все более насущной становится задача оперативного согласования правил ответственного поведения государств, закрепляющих в цифровой среде принципы уважения суверенитета, невмешательства во внутренние дела, неприменения силы и угрозы силой, права на индивидуальную и коллективную самооборону, уважения прав и основных свобод человека, а также равные права для всех государств на участие в управлении сетью Интернет.

Примечательно, что именно российские принципиальные установки пользуются самой широкой поддержкой. В 2018 году 73-я сессия Генеральной Ассамблеи ООН подавляющим большинством голосов приняла нашу резолюцию, которая сформулировала первоначальный перечень правил поведения государств в информпространстве и создала под ооновской эгидой эффективный переговорный механизм в формате профильной Рабочей группы ООН открытого состава (РГОС) по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности.

В 2019 г. Россия инициировала в рамках ООН разработку всеобъемлющей международной конвенции о противодействии использованию ИКТ в преступных целях. На 74-й сессии Генассамблеи нами был внесен проект резолюции «Противодействие использованию информационно-коммуникационных технологий в преступных целях». Соавторами выступили 47 государств. Резолюция, принятая при поддержке большинства стран Азии, Африки, Латинской Америки, постановила учредить специальный межправительственный комитет экспертов открытого состава для разработки конвенции.

12 марта с.г. значимым успехом российской дипломатии завершилась деятельность РГОС. Все 193 государства-члена ООН поддержали консенсус по принятию доклада, подводящего итог двухлетней работы Группы. В документе закреплены базовые подходы, продвигаемые Россией и ее партнерами в области МИБ (предотвращение конфликтов в информпространстве, недопущение его милитаризации и использование ИКТ исключительно в мирных целях). В нем также четко подтверждаются ранее достигнутые международным сообществом договоренности по правилам, нормам и принципам ответственного поведения государств. При этом большинством участников была отмечена ключевая роль России в организации переговорного процесса под эгидой ООН в данном формате.

27 июля с.г. в Вене мы внесли в вышеупомянутый спецкомитет российский проект первого в истории универсального договора по борьбе с киберпреступностью. Таким образом, Российская Федерация первой наполнила конкретным содержанием процесс разработки столь важного и необходимого международного договора, который призван поднять международное сотрудничество в этой сфере на качественно новый уровень. Работу над итоговым проектом конвенции планируется завершить в 2023 году в ходе 78-й сессии Генассамблеи ООН. Первая переговорная сессия специального комитета намечена на январь 2022 г. в Нью-Йорке.

Восприимчивость международного сообщества к российскому начинанию свидетельствует, что заключение подобного договора –

это объективное веление времени, осознание новой реальности, связанной со стремительно возрастающей ролью ИКТ и возникающими в этой связи вызовами.

Однако подобную инклюзивную линию поддерживают далеко не все. Ряд стран стремятся подменить борьбу за равную и неделимую кибербезопасность желанием навязать свои «порядки». Их задачи сохранить технологические преимущества и возможность принимать односторонние силовые шаги в сфере ИКТ, окончательно присвоить право единолично назначать ответственных в киберинцидентах. Ради этого они готовы превратить мировое информационное пространство в новый театр военных действий.

Некоторые категорически против выработки международно-правовых инструментов, предотвращающих использование ИКТ в узкокорыстных военно-политических целях, а также проясняющих, в каких случаях кибератаки могут быть квалифицированы как вооруженное нападение, и, соответственно, приводить в действие статью 51 Устава ООН о праве государств на самооборону. Не поддерживаются идеи об укреплении роли ООН и создания под ее эгидой международного киберарбитража или иного постоянно действующего органа, занимающегося тематикой МИБ. Отрицается необходимость вовлечения Совбеза ООН в разбор и урегулирование межгосударственных инцидентов и конфликтов в киберсфере. Оспаривается право государств на суверенитет в области обеспечения национальной информационной безопасности и над информационно-коммуникационной инфраструктурой, находящейся на собственной территории.

Провозглашая свое «право» вмешиваться во внутренние дела других стран в интересах «развития демократии», они не приемлют ни малейшей критики в свой адрес, с ходу отметая любые предложения начать равноправный диалог по соответствующим сюжетам.

На этом фоне против нас развернута беспрецедентная пропагандистская кампания с безапелляционными и бездоказательными обвинениями: от «попыток вмешательства в демократические процессы за рубежом» до «организации кибератак на объекты критической инфраструктуры западных стран».

Несмотря на это каждый раз в ходе контактов с зарубежными партнерами мы подтверждаем свой твердый настрой на совместную работу в сфере кибербезопасности. В этом плане, как отметил В.В.Путин, показательно, что, по данным американских же источников, большинство кибернападений в мире происходят с адресов на территории Соединенных Штатов (в 2020 г. – 45, в 2021 г. – уже 35, в т.ч. на медучреждения Воронежской области). К слову, на наши 45 запросов в прошлом году и около 40 с начала текущего года не последовало никакой реакции, тогда как мы ответили на все 10 американских запросов.

Объективная востребованность постоянного, неполитизированного и профессионального диалога в этой сфере очевидна. Поэтому Россия продолжает наращивать сотрудничество по всему комплексу актуальных вопросов обеспечения МИБ, в том числе в интересах противодействия угрозам масштабного использования ИКТ в военно-политических целях. В числе наших приоритетов остается принятие международных актов, регламентирующих применение в ИКТ-сфере принципов и норм международного гуманитарного права, создание условий для установления международного правового режима нераспространения информационного оружия, разработка и реализация многосторонних программ, способствующих преодолению информационного неравенства между развитыми и развивающимися странами.

В.А. Уваров

Директор Департамента информационной безопасности Банка России

Спасибо большое, коллеги, за возможность выступить на таком представительном мероприятии. 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. Для этого необходимо скоординировать усилия регуляторов, правоохранительных органов, организаций кредитно-финансовой сферы. И сейчас я хочу поделиться с Вами опытом Банка России по организации такого взаимодействия.

Для начала давайте посмотрим на основные показатели предыдущих лет по операциям без согласия клиентов. Эти сведения Банк России ежеквартально и ежегодно публикует на сайте в своих отчетах. Это параметры хищений по итогам 2019 и 2020 годов. Как мы видим, число хищений растет, потому, как объем операций, совершенных без согласия клиентов с использованием электронных средств платежа, составил в 2020 году 9,8 млрд. рублей. Это больше, чем годом ранее на 53%. Количество таких операций в 2020 году выросло на 34%, практически на 200 тысяч. Коллеги, впечатляющие данные, не правда ли? Выросла и сумма одной операции без согласия клиента по счетам физических лиц до 11,4 тысяч рублей в 2020 году, а вот у юридических лиц практически в 2,5 раза.

Есть и положительная динамика в показателях, которая, несомненно, радует. В 2020 году на 7 процентов снизился показатель по доле операций без согласия клиентов, совершенных в результате обмана или злоупотребления доверием клиентов методами так называемой социальной инженерии. Позитивная динамика данного показателя стала результатом слаженной работы Банка России и правоохранительных органов по своевременному информированию населения в средствах массовой информации, на объектах социальной и транспортной инфраструктуры.

Кроме того, в 2021 году Банк России выпустил рекомендации для банков по усилению информационной работы, направленной на повышение осмотрительности клиентов. Поэтому работа самих финансовых организаций в том числе нашла отражение и в динамике данного показателя.

Сейчас я расскажу подробнее о ресурсах Банка России, позволяющих выявлять и реагировать на мошеннические операции. В Банке России создано специальное подразделение ФинЦЕРТ. ФинЦЕРТ – центр взаимодействия и реагирования на компьютерные атаки в кредитно-финансовой сфере. Это структурное подразделение Департамента информационной безопасности. Центр взаимодействует с поднадзорными Банку России организациями, разработчиками антивирусного программного обеспечения, операторами связи и, конечно, с иностранными участниками финансового рынка. В рамках его деятельности выявляются фальшивые сайты, номера телефонов, которые используются в мошеннических целях.

Тремя основными задачами ФинЦЕРТА являются:

1. Мониторинг и аналитика, что включает в себя сбор и анализ информации о кибератаках, признаках и характере операций, совершенных без согласия клиента.
2. Взаимодействие. В эту задачу входят информационный обмен со всеми участниками, разработка и распространение оперативных и аналитических материалов. На этих двух этапах очень важно

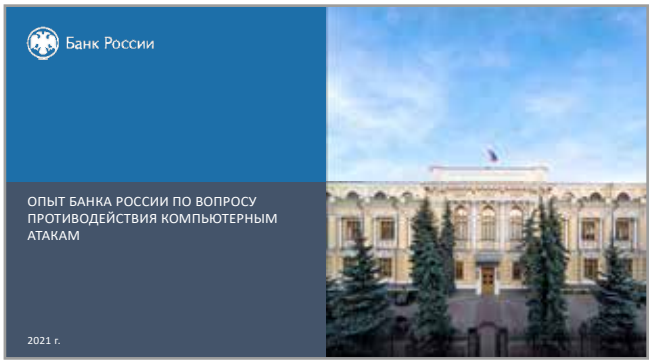
оказать помощь коллегам из финансовых организаций в оперативном выявлении и, что еще не менее важно, путем своевременного информирования предотвратить новые попытки хищения.

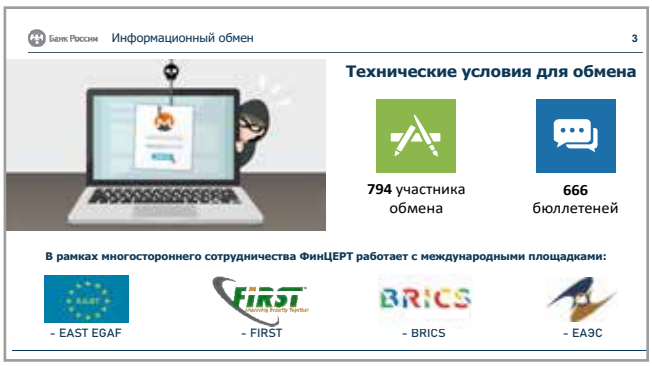
3. Третья задача – реагирование. В нее входят мероприятия по запуску процедуры блокировки доменов в сети Интернет и инициация меры реагирования на мошеннические телефонные номера. ФинЦЕРТ работает 24 часа в сутки 7 дней в неделю. За 2020 год в сторону партнеров Банк России направил более 660 бюллетеней. На текущую дату с начала 2021 года направлен 131 бюллетень. На сегодняшний день зафиксировано почти 800 участников информационного обмена. В рамках сотрудничества ФинЦЕРТ работает с международными площадками по двум направлениям – интеграционному и двустороннему. Об этом сотрудничестве расскажу немного позже.

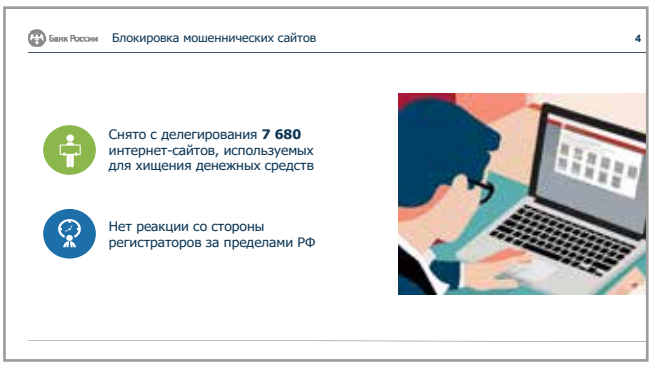
Сейчас я хочу остановиться на задаче ФинЦЕРТа по осуществлению реагирования и результатах решения этой задачи. Одним из важных направлений по противодействию кибермошенничеству является борьба с мошенничеством, осуществляемым с использованием Интернет-сайтов и социальных сетей. Эту работу мы ведем совместно с Генеральной прокуратурой Российской Федерации, а также в рамках соглашений о взаимодействии, заключенных 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 разделегирования доменов регистратором занимает от трех часов до трех дней.

Также в целях противодействия увеличению масштабов использования в сети Интернет сайтов для совершения мошеннических действий на финансовом рынке Банк России инициировал изменения в федеральном законодательстве, на основании которых он получил право обращаться в Генеральную прокуратуру Российской Федерации для внесудебной блокировки сайтов. Полномочия Банка России вступят в силу с 1 декабря 2021 года.

В 2020 году Банк инициировал блокировку более 7600 сайтов в различных доменных зонах. Основное большинство, чуть более 6000 единиц, как и годом ранее, составляли мошеннические сайты, маскирующиеся под разные социальные выплаты, под опросы, продажу авиа- и железнодорожных билетов. Если у ФинЦЕРТ нет права на разделегирова-







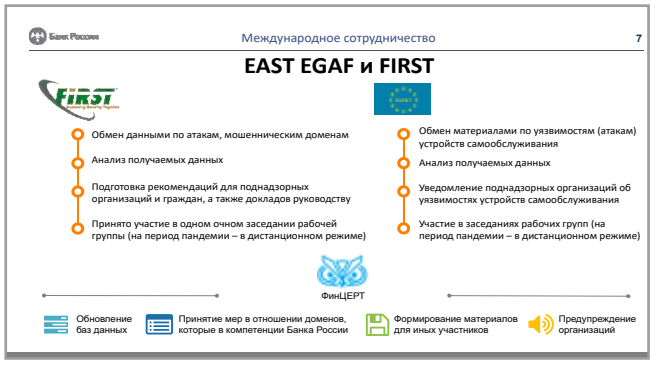
ние ресурсов, направляется запрос регистраторам на общих основаниях. Поэтому, я думаю, не нужно объяснять, как важно и нужно развивать наше взаимодействие и сотрудничество в данном направлении. Именно при такой реализации действий мы сможем оперативно и эффективно пресекать мошеннические действия и прочие виды противозаконной деятельности, и мы очень рассчитываем на Вашу поддержку.

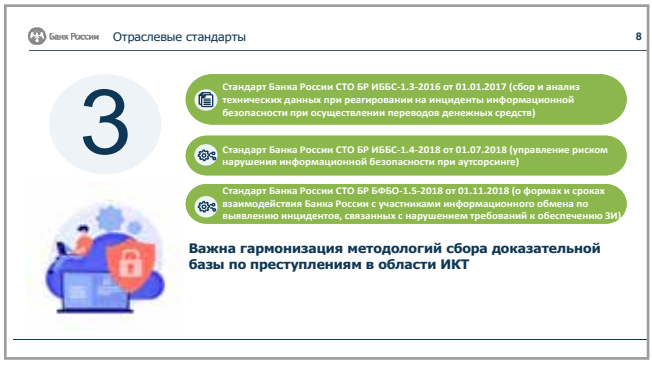
В эпоху глобализации невозможно справиться с проблемами кибермошенничества в одиночку. Как я уже говорил ранее, мы развиваем международный информационный обмен по двум направлениям: интеграционному, соответственно, и двустороннему. По первому направлению работа ведется в рамках сотрудничества с Центральными банками государств – членов ЕАЭС и государств – участников БРИКС. И сближение с национальными банками государств – членов ЕАЭС уже приносит свои плоды. За 2019 – 2020 годы от финансовых регуляторов государств – членов нами было получено более 170 сообщений по вопросам информационной безопасности.

В рамках работы на площадке ЕАЭС уже разработаны и утверждены единый глоссарий по вопросам информационной и кибербезопасности, а также единые правила обмена информацией об операциях без согласия клиента и механизмы реагирования на такого рода инциденты.

Аналогичное сотрудничество развивается и в рамках БРИКС. Уже разработаны и утверждены и опубликованы регламент взаимодействия канала БРИКС, электронный буклет регуляторных актов государств – участников БРИКС, сборник лучших практик, доклад по цифровой финансовой доступности. Успешно начат информационный обмен данными о компьютерных атаках. Следует отметить, что в июне 2021 года Банк России проводил обучение для коллег из Центральных банков государств – членов ЕАЭС и государств – участников БРИКС в области кибербезопасности. В рамках курса обсуждались актуальные вопросы, ведущие эксперты делились опытом и реальными кейсами. Такой подход высоко оценили на международном уровне, и наша программа получила приз конкурса Всемирной встречи на высшем уровне по вопросам информационного обмена под эгидой Организации Объединенных Наций.

Есть еще две площадки, где мы также присутствуем. В рамках сотрудничества с международным сообществом команд реагирования на инциденты и экспертной группой по противодействию мошенничеству, связанному с банкоматами, Банк России получает данные о способах мошенничества и атаках, связанных с устройствами самообслуживания и пла-





тежными картами, о мерах противодействия им, информацию о компьютерных атаках и рекомендации по реагированию на компьютерные угрозы, а также информацию о мошеннических доменах. Получаемая информация позволяет нашим поднадзорным обновить базы данных, предотвратить компьютерные атаки и минимизировать риски хищения денежных средств у иностранных кредитных организаций, а также принять меры в отношении выявленных ресурсов. Хочу отметить, что в рамках двустороннего сотрудничества Центральным банком Российской Федерации также ведется работа с 15 Центральными банками иностранных государств по вопросам информационной безопасности.

Банк России участвует в процессах стандартизации в области информационной безопасности на всех уровнях: международном, национальном, отраслевом. Эксперты Департамента принимают участие в работе профильных групп Международной организации по стандартизации, Международной электротехнической комиссии, Международного союза электросвязи, Национального технического комитета по стандартизации, стандарты финансовых операций, мы все его знаем, как ТК 122. Наши эксперты вносят свой вклад в работу перечисленных организаций по стандартизации, также основываясь на уникальном опыте коллег, мы принимаем за основу лучшие практики и наработки в области регулирования вопросов информационной безопасности при разработке своих нормативных актов и стандартов, как отраслевых, так и национальных.

В рамках ВТО Банк России также принял участие в подготовке совместной инициативы по вопросам регулирования электронной торговли в форме соглашения. На текущий момент в России в основе организации информационного обмена лежит комплекс отраслевых стандартов, разработанных Банком России. Это стандарты реагирования на инциденты информационной безопасности, стандарт о формах и сроках взаимодействия и порядок управления риском.

Уважаемые коллеги, ни для кого не секрет, что мы живем в эпоху тотальной глобализации, где весь мир как единый организм, здоровье которого зависит напрямую от слаженной работы всех 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 процессы получения денег. Злоумышленник может находиться практически в любые точки мира и атаковать граждан практически из любой страны, причем массово, глобальная сеть Интернет позволяет это сделать.

Опыт нашего общения с коллегами из ЕАЭС свидетельствует, что работает, как правило, следующая схема: сначала техника вывода средств и атаки отрабатываются в Российской Федерации, а 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.

В России показатель операций без согласия клиента находится на допустимом уровне. По данным международных платежных систем, Российская Федерация не входит в число стран-лидеров по уровню мошенничества в мире. Однако именно здесь злоумышленники часто разрабатывают методы вывода денег, а далее отрабатывают методы воздействия, конкретные приемы социальной инженерии. А затем идут туда, где русский понимается на природном уровне и очень распространен. В первую очередь это страны постсоветского пространства, страны СНГ. А вообще преступность в этом смысле не имеет четкой географии, и любая страна может стать интересом для интернациональных двуязычных бригад, специализирующихся на обналичивании средств.

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. Со своей стороны, мы предлагаем взять за основу комплекс разработанных нами стандартов, уже показавших себя в действии, о них я говорил ранее. Полагаю, что наше со-

трудничество уберет границы между странами в вопросах борьбы с кибермошенничеством.

В завершении своего выступления я 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.

Спасибо за внимание!

И. Асланов
Глава региональной делегации в России, Беларуси и Молдове Международного Комитета Красного Креста

Уважаемые участники Конференции! Дамы и господа!

Я очень рад возможности выступить сегодня от имени Региональной делегации Международного Комитета Красного Креста (МККК) в Российской Федерации, Беларуси и Молдове. Мне хочется искренне поблагодарить организаторов в XV Международного Форума за приглашение. Тематика форума очень актуальна для МККК – организации, оказывающей всестороннюю помощь и поддержку жертвам вооруженных конфликтов по всему миру. В своем выступлении я затрону тему информационно-коммуникационных технологий и вызовов гуманитарной деятельности.

Цифровые технологии все глубже входят в жизнь общества. Но вместе с новыми возможностями приходят и новые угрозы. На сегодняшний день **любой объект может стать целью кибероперaций.** От них страдают правительства, частные компании и физические лица. Мы, как гуманитарная организация, озабочены потенциальным негативным влиянием **цифровых рисков,** с которыми сталкивается население, получающее нашу поддержку. Среди таких рисков можно выделить **вопросы защиты персональных данных** и угрозы, связанные с **цифровизацией таких данных** и последующему несанкционированному доступу к ним. Опыт МККК дает четкое понимание того, что в кризисных ситуация конфиденциальность и защита информации могут являться вопросом жизни и смерти, поэтому ответственное использование данных является абсолютной необходимостью. Другим риском, которому МККК уделяет серьезное внимание, является **дезинформация и язык вражды.** Это усугубляющий и ускоряющий фактор конфликтной динамики, насилия и ущерба с ужасными последствиями как для населения, так и для гуманитарных организаций.

Главный фокус деятельности МККК направлен на защиту жертв войны. Гражданские лица, раненые и больные, военнопленные, медицинские учреждения и врачи – все они находятся под защитой международного гуманитарного права. Для МККК нет сомнений в том, что международное гуманитарное право применимо и ограничивает использование ИКТ в качестве средств и методов ведения войны. Итоговый документ Группы правительственных экспертов ООН, выпущенный в мае этого года и поддержанный Российской Федерацией, подтверждает применимость ключевых норм МГП – принципов гуманности, военной необходимости, соразмерности и проведения различия в ситуации вооруженных конфликтов. Примером запрещенных операций является кибернападения на медицинскую инфраструктуру во время вооруженных конфликтов. В отчете Рабочей группы открытого состава, выпущенном в марте 2021 г. подчеркиваются «потенциально разрушительные […] гуманитарные последствия злонамеренной деятельности ИКТ для критически важной инфраструктуры […], поддерживающей основные сферы жизнедеятельности населения». Мы надеемся, что пандемия COVID-19 привлечет необходимое внимание и побудит международное сообщество недвусмысленно подтвердить, что международное право полностью запрещает кибероперации направленные против медицинских служб.

В своей работе МККК старается поддерживать максимальную близость к людям, которым мы оказываем помощь и поддержку. Для обеспечения этой близости **доверие** является безусловным условием. В связи с этим

МККК призывает государства создать такую **доверительную среду,** которая позволит гуманитарным организациям успешно выполнять свой мандат в условиях стремительного развития цифровых технологий. МККК также ведет работу по так называемой «**цифровой эмблеме**». Эмблемы красного креста и красного полумесяца защищают и идентифицируют медицинские службы и гуманитарных работников в реальном мире. Однако на данный момент не существует отличительной эмблемы или отличительного сигнала в мире «цифровом». Поэтому, МККК работает над тем, чтобы оценить техническую осуществимость, перспективы и риски разработки такой эмблемы. И мы рады отметить, что российские эксперты также принимают участие в процессе консультаций по данному проекту.

Позиция и экспертиза Российской Федерации по вопросам международной информационной безопасности имеет важное значение. Для нас важно, чтобы позиция России была представлена на максимально широком количестве международных форумов. Именно в широкой дискуссии мы видим возможность укрепления МККК как нейтральной и беспристрастной организации. Помимо ранее упомянутого мною проекта по «цифровой эмблеме», другим примером сотрудничества МККК и России в этой области является включение руководителя компании «Бизон», в состав **Всеобщего консультативного совета МККК по международно-правовым нормам в сфере защиты гражданских лиц от цифровых угроз во время конфликтов.**

Международный Комитет Красного Креста всегда открыт для диалога и совместных инициатив в сфере международной информационной безопасности. Мы ищем поддержку России в вопросе применения существующих норм права и прогрессивного их развития. Мы со своей стороны готовы всемерно делиться своим опытом и способствовать тому, чтобы защита, предоставляемая нормами МГП усиливалась.

Еще раз благодарю Вас за возможность выступить здесь сегодня, и желаю организаторам и участникам успешного и продуктивного форума. Спасибо!

КРУГЛЫЙ СТОЛ № 1
МЕЖДУНАРОДНОЕ СОТРУДНИЧЕСТВО В ОБЛАСТИ АТРИБУЦИИ ИНЦИДЕНТОВ В ЦЕЛЯХ МИРНОГО РАЗРЕШЕНИЯ СПОРНЫХ СИТУАЦИЙ В ИКТ-СРЕДЕ

Модератор:
Мурашов Н. Н., Национальный координационный центр
по компьютерным инцидентам,
заместитель Директора

Э.В. Чернухин
Начальник отдела Департамента
МИБ МИД России

О ПОДХОДАХ РОССИИ К ОБЕСПЕЧЕНИЮ ЦИФРОВОГО СУВЕРЕНИТЕТА

В современных условиях сохранение цифрового суверенитета является не только непреложной основой, но и залогом возможности существования самого государства, способом избежать потенциальные конфликты в информационной среде. Это обусловлено формированием глобального информационного пространства и становлением информационного общества на международном и национальном уровнях.

Одновременно с этим происходят перемены, связанные с трансформацией мирового информационного порядка. Ведущие промышленно развитые державы стараются сохранить статус доминирующей силы в информационном поле и затормозить переход к полицентричной, основанной на юридически обязательных нормах, моделе его управления.

Президент Российской Федерации В.В.Путин, выступая в марте 2021 г. на заседании Совета Безопасности России, в ходе которого рассматривался проект «Основ государственной политики Российской Федерации в области международной информационной безопасности» в частности подчеркнул, что «Россия выступает за незыблемость цифрового суверенитета государств. Это означает, что каждая страна может самостоятельно определять параметры регулирования собственного информационного пространства и соответствующей инфраструктуры».

Однако, достижение цифрового суверенитета понимается многими государствами по-разному. Так, технологически развитые страны считают необходимым отстаивать свои интересы на дальних «информационных» подступах за пределами своих национальных юрисдикций. Естественным инструментом и проводником таких идей выступает крупный IT бизнес. При этом, информационные гиганты зачастую диктуют и навязывают свои условия, вступая в прямую конфронтацию с законодательством страны пребывания. Это связано с тем, что IT гиганты на системной основе занимаются активным лоббированием своих интересов, затрачивая на это из бюджетов компаний сотни миллионов Долл.США. В десятку основных лоббистов мира в частности входят Google, Facebook, Microsoft, Apple, IBM, Intel, Qualcomm, Vodafone и др.

Являясь, по сути, монополистами, международные корпорации могут зачастую грубо нарушать или обходить отдельные правовые нормы государств в части правил по защите, сбору и обработки персональных данных. Фактически речь здесь может идти о попытках расширения юрисдикции одного отдельно взятого государства на часть глобального информационного пространства. При этом страны (преимущественно развитые), в которых созданы и зарегистрированы такие компании заявляют, что никакой ответственности за их деятельностью за рубежом не несут. В свою очередь многие государства не имеют достаточных административных, технических и политических ресурсов для воздействия на таких нарушителей.

По мнению международных экспертов, число таких потенциальных «цифровых» конфликтов и правовых коллизий в ближайшее время будет стремительно расти. Об этом, в частности свидетельствуют многочисленные судебные разбирательства, иски и штрафы по отношению к международному бизнесу внутри самих ведущих технологически развитых держав (например, в Австралии, Великобритании, Ирландии, КНР, РФ, Франции, США и др.).

К числу наиболее резонансных нарушений в частности относят: оперативную неблокировку запрещенных веб сайтов; неудаление противоправного контента; вмешательство в выборные процессы; проведение сомнительных рекламных технологий; искажение сведений о финансовой политике; нарушение неприкосновенности частной жизни и потребительских прав детей; нарушение национальных регламентов по защите данных в части незаконного сбора персональных данных пользователей и отслеживание их местоположения в т.ч. через системы видеонаблюдения и др.

Процесс глобальной цифровизации открывает инновационные возможности для развития государств, но также возрастает необходимость адекватного реагирования на появляющиеся угрозы в сфере обеспечения международной информационной безопасности (МИБ), своевременного их прогнозирования и отражения. Так, например, по оценкам экспертов, число подключенных к глобальному интернету электронных приборов в ближайшие несколько лет может превысить 40 млрд. единиц. Более половины из них станут устройствами Интернета вещей. К ним, в частности относятся не только камеры видеонаблюдения, различные промышленные и торговые терминалы, научные-исследовательские комплексы, но и значительная часть современного медицинского и образовательного оборудования.

В этом смысле информационная безопасность превращается в жизненно необходимое условие защиты интересов личности, общества и государства.

На международном уровне Россия отстаивает принципы мирного использования информационно-коммуникационных технологий (ИКТ), создания системы предотвращения киберконфликтов, выработки под эгидой ООН принципов, норм и правил ответственного поведения государств в информационном пространстве, а также юридически обязательного международного договора универсального характера по противодействию использования ИКТ в преступных целях.

Соответствующую линию на обеспечение таких подходов Российская Федерация проводит в многосторонних и двусторонних форматах на всех ключевых международных направлениях. Прежде всего, под эгидой ООН, а также региональных площадках – ОБСЕ, СНГ, ШОС, АРФ, АСЕАН и др.

К примеру за последние несколько лет серьезное развитие получила проблематика борьбы с информационной преступностью. Которая, ввиду своего глобального масштаба и нанесенного ущерба от совершения противоправных деяний стала многими государствами сравниваться с еще одним видом кибероружия, влияющего на стратегическую стабильность в мире. А глобальное использование современных информационно-коммуникационных технологий, по сути, является заложником отсутствия разработанного под эгидой ООН международно-правового договора по противодействию информационной преступности.

Политическая декларация, принятая по итогам 14-го Конгресса ООН по предупреждению преступности и уголовному правосудию, состоявшегося в марте 2021 г. в Японии (г.Киото), в том числе подчеркнула необходимость улучшения координации международного сотрудничества для эффективного предупреждения киберпреступности и укрепление государственно-частного партнерства с представителями цифровой отрасли и поставщиков услуг связи при должном соблюдении требований национального законодательства и принципов международного права.

Именно поэтому Россия вместе с единомышленниками выступает за разработку под эгидой ООН Конвенции по противодействию преступлениям в сфере использования ИКТ, которая учитывала бы интересы всех без исключения стран и основывалась бы на принципах суверенного равенства сторон и невмешательства во внутренние дела государств.

26 мая 2021 г. Генассамблеей ООН консенсусом была одобрена инициированная Россией резолюция 75/282 «Противодействие использованию информационно-коммуникационных технологий в преступных целях» по модальностям работы Спецкомитета открытого состава по разработке под эгидой ООН первой универсальной конвенции по борьбе с информпреступностью, учрежденного в декабре 2019 г. резолюцией ГА ООН 74/247 по предложению России и еще 46 государств.

Таким образом, после многолетних дебатов о необходимости разработки конвенции

ООН по борьбе с информационной преступностью мировым сообществом был дан политический мандат на запуск работы над таким международным договором. Резолюцией предусматривается разработка универсального договора за 2,5 года с тем, чтобы представить его на рассмотрение 78-й сессии ГА ООН.

Учитывая сжатые сроки, отведенные на разработку конвенции, 27 июля 2021 г. Россия в качестве национального вклада в работу Спецкомитета внесла и распространила собственный проект подобного документа.

Документ был разработан ведущими российскими экспертами под руководством Генеральной прокуратуры Российской Федерации.

В разработке также принимали участие представители МИД РФ, МВД РФ, Минюста РФ, Следственного комитета Российской Федерации и других заинтересованных ведомств.

Проект имеет универсальную юрисдикцию с возможностью для каждого государства стать ее участником без какого-либо ущерба для своего национального законодательства. Конвенция основывается на принципах суверенитета и невмешательства во внутренние дела других государств.

Настоящий документ представляет собой обновленную версию российского проекта 2017 г., разработанного под руководством МИД России и распространенного в ходе 72-й сессии Генассамблеи ООН и ставшего ее официальным документом.

В документе использованы хорошо знакомые государствам положения КПК, КТОП и Будапештской конвенции. Это позволит не менять уже устоявшиеся элементы и правила функционирования международного сотрудничества, а лишь дополнить их спецификой ИКТ-среды и упростить внедрение в национальное законодательство государств.

В заключение хотелось бы отметить, что Российская Федерация готова к проведению серьезного и обстоятельного диалога по разработке проекта Конвенции со всеми заинтересованными партнерами как в двухстороннем, так и многостороннем форматах на различных международных площадках.

Санжай Гоэл
Государственный университет штата Нью-Йорк (США)

ПОНИМАНИЕ РАСЧЕТОВ КИБЕРСДЕРЖИВАНИЯ США

Кибервойна между США и Россией имеет асимметричный характер и основывается на ложных предположениях, что привело нас в опасный тупик. Эта асимметричность констатируется в том смысле, что США обладают гораздо более развитой инфраструктурой, которая в настоящее время опирается на кибернетику и более открытый Интернет, что делает их более уязвимыми для кибератак как со стороны национальных государств, так и преступных групп, стремящихся извлечь выгоду из нарушений. Серия атак, в том числе атака вымогателей на Colonian Pipeline, атака цепочки поставок на программное обеспечение для мониторинга сети SolarWinds и атака на мясоперерабатывающие заводы JBS, отражает уязвимость критически важной инфраструктуры США. Опасность этой первичной асимметрии очевидна: США могут потерять гораздо больше, чем другие национальные государства и/или преступные организации, которые совершают нападения.

Еще одна фундаментальная асимметрия в расчете глобальной безопасности заключается в различиях относительно толерантности различных стран к киберпреступности. США не допускают и не поощряют существование киберпреступников на своей территории, в то время как другие страны не только терпят их, но и молчаливо поощряют и облегчают подобную деятельность. Кибератаки стали для некоторых стран очень полезным инструментом геополитического позиционирования. Хотя США, вероятно, обладают самым мощным в мире потенциалом кибератак и могут наносить ответные удары по организациям, занимающимся киберпреступностью, без поддержки тех национальных государств, которые принимают эти организации, влияние таких усилий ограничено. В этом отношении также существует финансовая асимметрия, поскольку борьба с несколькими преступными группировками обойдется США намного дороже, чем это скажется для любой из этих организаций. Предлагаемый бюджет США на кибербезопасность на этот финансовый год (2021) составил почти 19 миллиардов долларов, эта сумма соперничает с ВВП многих стран мира. (Statista, 2021) Кибератаки в конечном счете сопряжены с низким риском и высокой наградой, в то время как борьба с ними – наоборот: очень дорого, с относительно минимальной отдачей. Эти позиции изменились относительно недавно, когда США смогли вернуть 2,3 миллиона долларов в биткоинах, выплаченных вымогателям Dark Side – группировки, которая, как полагают, является российской преступной организацией, в ходе атаки Colonial Pipeline.

До сих пор США вели дела с национальными государствами и их доверенными лицами главным образом с помощью угроз и санкций. К сожалению, нет общедоступных оценок, которые свидетельствовали бы о достижении этими санкциями своих целей. По данным Фонда Карнеги «За международный мир» и других организаций, Соединенные Штаты вводили санкции 35 раз, нацеливаясь на более чем 300 человек и организаций, в ответ на вредоносную кибердеятельность в рамках нескольких различных структур власти, включая программу кибер-ориентированных санкций. (Thompson, 2020) Киберсанкции правительства США в основном были применены против физических или юридических лиц, связанных с национальными государствами, в трех странах: Иране (36%), Северной Корее (6%) и Рос-

сии (45%). В апреле этого года администрация Байдена ввела 35 новых санкций в отношении России, связанных с киберпространством, причем почти все они были введены в соответствии с программами санкций в отношении КИБЕР2 и конкретных стран или вмешательства в выборы. (Ophel, 2021).

Санкции и другие методы принуждения имеют в лучшем случае краткосрочную эффективность, но в долгосрочной перспективе они теряют свою действенность. Экономические санкции США против России, угрозы изоляции на многосторонних форумах и ограничения на поездки принесли незначительный эффект. Применение санкций также чревато циклом эскалации. Возможно, сейчас самое время подумать о более оптимистичных вариантах.

Основное ложное предположение, лежащее в основе нашего кибернетического тупика, - это вера в сдерживание посредством атрибуции. Киберсдерживание по-прежнему остается основополагающей концепцией для политических дебатов по киберполитике. Борьба с кибернападениями на национальные государства требует надежного сдерживания, и, хотя мы добились прогресса в определении вины, за три десятилетия исследований появилось мало практических решений и не было достигнуто консенсуса относительно дальнейших действий. В недавней статье о сдерживании отмечалось, что даже написание и размышления о киберсдерживании постепенно выходят из моды среди ученых, то ли потому, что эта концепция в корне неправильно применяется в киберпространстве, то ли потому, что другие стратегические концепции приобретают все большее значение. (Soesanto, 2021) В любом случае ясно, что в вопросе международных кибератак все еще достаточно неопределенности, с тем, чтобы всегда оставалось место для правдоподобного отрицания и, следовательно, для слабой правовой основы для рассмотрения дела в международном суде. Меры укрепления доверия и международные договоры также основаны на надлежащей атрибуции и адекватной видимости возможностей противника. Неопределенность в отношении намерений других государств и трудность определения того, используются ли атаки для нападения или для защиты, порождают классическую дилемму безопасности, увеличивая бюджеты разведывательных ведомств и их стимулы для наращивания (наступательных) возможностей (Cavelty, 2020). Отсутствие как договоров, так и мер укрепления доверия не порождает большого доверия к международному праву, и каждая страна продолжает развивать свой кибернетический арсенал и наращивать свои киберармии. Другими словами, гонка кибервооружений продолжается.

Использование социальных сетей для пропаганды и социальных ботов для кампаний по дезинформации в других странах вызывает огромные трения на международном уровне, но, опять же, проблема последовательной и правильной атрибуции удерживает эти трения на кипящем, нерешенном уровне обвинений и встречных обвинений. И США, и Россия уязвимы для кампаний дезинформации, для США проблема заключается в поддержании честности своих выборов, а для России главной заботой является ограничение или недопущение внутренних разногласий.

В то время как Соединенные Штаты угрожают начать ответные атаки против России и других противников на киберфронте, эскалация не отвечает интересам США; киберпреступление не является жизнеспособным вариантом. Вместо этого эта низкосортная кибервойна продолжает существовать и действует как раздражитель для двусторонних отношений.

К 2020 году многие военные и специалисты по планированию разведки пришли к мнению, сформулированному Джошуа Ровнером – бывшим ученым-резидентом Агентства национальной безопасности и Киберкомандования США до 2019 года. Почти во всех случаях, писал г-н Ровнер в эссе для сайта “Война на скалах”, хакерство стало не связанным с войной, а «открытым соревнованием между конкурирующими государствами», напоминающим шпионаж. Такого рода тупик или постоянное раздражение требуют готовности жить с неопределенностью. Шпионские конкурсы не выигрываются, но существуют в своего рода “серой зоне”, которая не является ни войной, ни миром. Одна из идей заключается в том, что по мере того, как правительства узнают, какие операции вызовут какой-то ответ, мир постепенно разрабатывает неписаные правила киберконкуренции. Ученые Майкл П.

Фишеркеллер и Ричард Дж. Харкнетт описали результат этого как «конкурентное взаимодействие в пределах этих границ, а не эскалацию конфликта до новых уровней». (Fisher, 2021)

Однако, я хотел бы предложить несколько иную точку зрения. В то время как государства продолжают откладывать установление правил поведения в киберпространстве, изощренность субъектов угроз, обладающих разрушительным киберпотенциалом, имеется и будет только возрастать.

Важно признать большого слона в комнате. Геополитическое ухудшение отношений между США и Россией, включая санкции против России и отдельных российских граждан, нельзя рассматривать в "кибер–вакууме" – это во многом связано с негативом отношений США и России. Обе страны сталкиваются со слишком многими внутренними проблемами, включая пандемию и экономические проблемы, и обе не могут позволить себе отвлекаться на киберпространство. Слишком многое поставлено на карту для обеих стран, чтобы игнорировать проблему киберпространства или продолжать участвовать в дорогостоящем, но в конечном счете бесплодном соревновании в кибершпионаже.

В то же время сегодня предпринимаются серьезные попытки использовать многосторонние форумы для решения киберконфликтов. В ООН были достигнуты некоторые начальные успехи благодаря сотрудничеству США и России в Группе правительственных экспертов, но с двумя сверхдержавами, Россией и Соединенными Штатами, находящимися по разные стороны дебатов, мало шансов на значимые результаты. Рабочая группа открытого состава ООН (РГОС) по информационно-коммуникационным технологиям (ИКТ), ее последняя инициатива, созданная в соответствии с резолюцией, поддержанной Россией, привела к принятию консенсусного доклада в марте 2021 года. К сожалению, ясно, что давние разногласия между странами по поводу необходимости глобального, взаимодействующего и открытого Интернета привели к появлению доклада, в котором в значительной степени не рассматриваются коренные причины глобальной кибернетической нестабильности сегодня. Возможно, двумя самыми большими упущениями в консенсусном докладе РГОС ООН являются отсутствие руководящих принципов в отношении подотчетности и международного гуманитарного права (МГП). ООН должна активизировать свои усилия, чтобы сохранить и укрепить уверенность в своей способности прокладывать путь вперед в области международных кибернорм и безопасности.

Есть более продуктивный способ продвижения вперед. Я бы сказал, что нам нужно следующее:

1. Всесторонне изучить точки трения –политические и кибернетические – между странами, а не заниматься разовыми проблемами.
2. Продвигаться вперед вместе в сотрудничестве с ООН, вместо того, чтобы двигаться разными путями.
3. Смягчить риторику друг против друга и негласно признать конфликт.
4. Работать над встречами на треке 2.0, чтобы вернуть дипломатию в нужное русло.

Источники:

1. Льюис, Джеймс и Смит, Жанна. "Скрытые издержки киберпреступности", Центр стратегических и международных исследований, 9 декабря 2020 г., https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-costs-of-cybercrime.pdf.
2. Цепной анализ. "Криптопреступность резюмирована: Мошенничество и рынки Даркнета доминировали в 2020 году по доходам, но вымогатели - это большая история". 19 января 2021 года. https://blog.chainalysis.com/reports/2021-crypto-crime-report-intro-ransomware-scams-darknet-markets.
3. Линч, К. (20 мая 2021 года). Сообщение Совета: Кибербезопасность – это глобальная проблема, так где же глобальный ответ? Использовано 18 сентября 2021 г., https://www.forbes.com/sites/forbestechcouncil/2021/05/20/cybersecurity-is-a-global-problem-so-wheres-the-global-response/?sh=b98df2a5e41f.
4. (https://www.statista.com/topics/3387/us-government-and-cyber-crime/)
5. Томпсон, Натали, "Противодействие вредоносной кибератаке: Целевые

финансовые санкции" Фонд Карнеги за международный мир, октябрь 2020 г., https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3770816.)
6. Офель, М., и Бартлетт, Дж. (4 мая 2021 года). Санкции по номерам: Уделите особое внимание кибер-санкциям. Центр новой американской безопасности. Использовано 18 сентября 2021 г., https://www.cnas.org/publications/reports/sanctions-by-the-numbers-cyber.
7. Соесанто С., Сметс М. (2021) Кибернетическое сдерживание: Прошлое, настоящее и будущее. В: Осинга Ф., Вайс Т. (ред.). Ежегодный обзор военных исследований Нидерландов. Ассер Пресс, Гаага. https://doi.org/10.1007/978-94-6265-419-8_20
8. Кавелти, Мириам Данн и Венгер, Андреас (2020) Кибербезопасность соответствует политике безопасности: сложные технологии, фрагментированная политика и сетевая наука, Современная политика безопасности, 41:1, 5-32, DOI: 10.1080/13523260.2019.1678855
9. Фишер, М. (20 июля 2021 года). Постоянный, но замаскированный шквал кибератак дает представление о новой эре. "Нью-Йорк Таймс". Использовано 18 сентября 2021 г., https://www.nytimes.com/2021/07/20/world/global-cyberattacks.html.
10. (Басу и др., "ООН изо всех сил пытается добиться прогресса в обеспечении безопасности киберпространства", Фонд Карнеги за международный мир, 19 мая 2021 г.)

Т.А. Полякова
Главный научный сотрудник, и.о. заведующего сектором информационного права и МИБ, доктор юридических наук, профессор, Института государства и права РАН

РАЗВИТИЕ СИСТЕМЫ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И СТРАТЕГИЧЕСКИЕ ЗАДАЧИ ПРАВОВОГО ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА НАЦИОНАЛЬНОМ И РЕГИОНАЛЬНОМ УРОВНЯХ

Сегодня вопросы развития системы международной информационной безопасности (далее – МИБ), включая обсуждение концептуальных положений проекта соответствующей Конвенции ООН, разработанной и размещенной на официальном сайте Совета Безопасности Российской Федерации, приобретают не только теоретическое, но и огромное практической значение.

К сожалению, мир не становится более устойчивым, а отношения между государствами, что особенно ощутимо и очевидно в информационной сфере, в ИКТ-среде, в целом нельзя признать доверительными. Несмотря на то, что эти проблемы находятся в фокусе внимания во всем мире, инициативы Российской Федерации и региональных сообществ, на площадке ООН продвигаются крайне медленно. При этом в условиях цифровой трансформации возрастающее значение информационной безопасности во всех ее проявлениях, очевидно. В связи с этим МИБ требует повышенного внимания в политике государств, в стратегических и концептуальных документах, поскольку акцент на проблеме обеспечения международной безопасности информационной безопасности как одной из ключевых на повестке дня внутренней и внешней политики России на современном этапе развития государства, общества и международной политики в условиях мирового кризиса. В условиях ускоряющихся процессов развития глобального информационного общества и перехода к цифровой цивилизации, характеризующихся не только трансформацией экономики (четвертой промышленной революции), возрастает международная политическая конфронтация, появляются новые риски, вызовы и угрозы в информационном пространстве.

Экспоненциальное развитие цифровых технологий – это, несомненно, благо, но именно ИКТ в условиях отсутствия императивности обязывания государств соблюдения общепризнанных принципов и норм международного право в ИКТ-среде, а не только предлагаемых правил, становятся и одним из ключевых драйверов возрастания угроз использования ИКТ в военно-политических, террористических целях, для вмешательства во внутренний дела суверенных государств, для совершения преступлений, в том числе связанных с неправомерным доступом к компьютерной информации, с созданием, использованием и распространением вредоносных компьютерных программ и информации, противоречащей принципам международного права.

В фокусе внимания находится вопрос научного осмысления проблем реализации новых документов стратегического планирования, влиянии на современном этапе ковидной реальности пандемии covid-19 на развитие системы принципов обеспечения международной информационной безопасности в условиях цифровой трансформации.

Сегодня в эпоху активных процессов цифровой трансформации, мирового кризиса, связанного еще и с проблемами, обусловленными мировой пандемией Covid-19, остро ощутимо их влияние и на систему права, как

международного, так и национального. Очевидно, что внедрение в жизнь социума различных конвергентных, прорывных (сквозных) технологий, и динамика развития информационно-телекоммуникационной индустрии в мировой экономике влияет и на благосостояние граждан и развитие России как демократического, федеративного, правового государства. При этом представляется особенно важным отметить, что в 2021 году, объявленным в России годом науки и технологий, на происходящие в мире процессы, связанные с развитием его научно-технологического потенциала, безусловно, влияет как на международном, так и национальном уровне возрастание новых рисков, вызовов и угроз информационной безопасности. В связи с этим требует повышенного внимания вопрос об определении и решение новых задач стратегического характера, направленных на укрепление системы МИБ.

Знаковым событием стало утверждение Указом Президента РФ от 12 апреля 2021 г. № 213 новых «Основ государственной политики Российской Федерации в области международной информационной безопасности», в которых одним из направлений реализации государственной политики в области МИБ определено содействие выработке с учетом специфики информационно-коммуникационных технологий новых принципов и норм международного права, регулирующих деятельность государств в глобальном информационном пространстве.

В связи с этим особо важно отметить, ключевое значение новелл в Конституцию РФ (статьи 71 и 114) внесенных в 2020 г. в целях не только развития информационного общества и обеспечения информационной безопасности, а также напрямую связанных с закреплением суверенитета государства и его территориальной целостности, как важнейших государственных задач, что напрямую связано с соблюдением ключевых принципов международного права, включая и информационную сферу.

Это приобретает, несомненно, приоритетное значение, как правовое, так и политическое в условиях обострения противостояния и цивилизационного кризиса в мире для обеспечения стабильности. В целях развития государственной политики в рассматриваемой сфере и развития системы МИБ особое значение имеет также новелла, включенная в ст.79.1 Конституции РФ, где указывается, что: «Российская Федерация принимает меры по поддержанию и укреплению международного мира и безопасности, обеспечению мирного сосуществования государств и народов, недопущению вмешательства во внутренние дела государств». Следует отметить, что внесенные в 2020 г. поправки в Конституцию РФ относят к ведению Российской Федерации обеспечение безопасности личности, общества и государства при применении информационных технологий, обороте цифровых данных (ст. 71, пункт «м»).

Кроме того, на обеспечение стабильности и устойчивого развития Российской Федерации, также направлены поправки, связанные с перераспределением отдельных полномочий между органами государственной власти и местного самоуправления, касающиеся формирования Президентом РФ Государственного Совета, а также Совета Безопасности Российской Федерации. Впервые также включены исходные положения обеспечения безопасности, использующиеся в непосредственной связи с безопасностью личности, общества и государства.

Тема обеспечения информационной безопасности как составляющей национальной безопасности, особенно в эпоху нового этапа информационной революции – «цифровой трансформации», занимает центральное место не только в стратегических документах, определяющих векторы государственной политики современного государства, но и отражается на развитии всей правовой системы, особенно это касается информационного права [3]. Такая цифровая трансформация, несомненно, повлияет и на изменение системы научных специальностей в праве, их укрупнений и информационное право наряду с конституционным, административным, финансовым и другими отраслями планируется объединить в публичной отрасли права.

В краткосрочной, среднесрочной и долгосрочной перспективе прогнозируется дальнейшее нарастание вызовов, угроз и рисков в цифровой сфере, что подтверждается и особенно проявляется в условиях пандемии (COVID-19) в России и во всем мировом сообществе. Например, к ним сегодня можно

отнести в эпоху короновирусной реальности «инфодемию», «кибердемию». Полагаем, что противодействие этим явлениям, учитывая их трансграничный характер, следует рассматривать как принципы обеспечения МИБ. Эти вопросы требуют межотраслевых исследований, включая и правовые. [4. С.229-231].

Стратегической задачей, вытекающей из новой Стратегии национальной безопасности, утвержденной Указом Президента РФ 2 июля 2021 г, является необходимость научного потенциала, включая вопросы развития науки и образования, для формирования адекватной системы правового регулирования новых отношений, их институционализации, определения статуса субъектов, современных подходов и моделей регулирования сквозных технологий, включая технологии искусственного интеллекта, робототехники.

Информационная безопасность, являясь одной из ключевых составляющих национальной безопасности, представляет собой сложную, динамично развивающуюся систему, имеющую закономерные связи между ее элементами, процессами организации и самоорганизации, принципами функционирования и развития. Доктрина информационной безопасности (2016 г.) в современных условиях необходимости реализации конституционно-правовых новелл, нуждается в научно-правовом осмыслении и выработке новых подходов к решению приоритетных целей и задач, поиска моделей регулирования.

Роль цифровизации очевидна при совершенствовании государственного управления в условиях формирования системы органов публичной власти, развития системы государственных услуг, в расширении пространства доверия, включая неурегулированность на законодательном уровне институтов идентификации и аутентификации, необходимость развития правового обеспечения критической информационной инфраструктуры, вопросы атрибуции инцидентов и т.д. Все это требует новых концептуальных подходов системного характера в целях защиты информационного пространства, а также защиты цифровых прав граждан, оборота цифровых данных, обеспечения неприкосновенности частной жизни, и защиты персональных данных граждан и т.д. Несомненно, это ключевые, приоритетные вопросы особенно актуальные как в теоретическом, так и в практическом отношении для обеспечения национальной безопасности и системы МИБ, которые должны найти отражение в государственной политике.

Кроме того, нельзя оставить без внимания и вопросы как соблюдения конституционных прав и свобод граждан, реализуемых в информационной сфере, так и деятельность организаций, направленную на насильственное изменение основ конституционного строя, целостности РФ, разжигание социальной, расовой, национальной и религиозной вражды, по распространению этих идей в средствах массовой информации.

Самостоятельных исследований заслуживают вопросы, касающиеся отнесения к федеральному ведению информационных технологий и оборота цифровых данных. Необходимы научные разработки и предложения по правовому регулированию этих вопросов. Принятие указанных поправок к Конституции РФ направлено на расширение функции государства при обеспечении информационной безопасности общества и личности. В связи с этим положение статьи 71 коррелируется со статьей 24 Конституции РФ, в которой по сути ключевой является информационная безопасность личности, связанная со сбором, хранением, использованием и распространением информации о частной жизни гражданина и его персональных данных, а именно эти личные данные сегодня очень чувствительны и требуют усиления их правовой защиты. В связи с этим необходим документ стратегического планирования в области формирования в обществе в такой социально значимой сфере как культура кибербезопасности и информационная грамотность.

Требует продолжения такое научное направление как развития использование различных моделей правового регулирования (саморегулирования, сорегулирования, гибридного регулирования), а также неправовых регуляторов (этических, технических, базовых принципов правового регулирования в информационной сфере). Этими исследованиями занимается и сектор информационного права и международной информационной безопасности Института государства и права Российской академии наук. Сегодня выделяются такие принципы правового регулирования отношений в сфере информации, инфор-

мационных технологий и защиты информации как неприкосновенность частной жизни, недопустимость сбора, хранения, использования и распространения информации о частной жизни лица без соответствующего согласия.

Полагаем, что на национальном уровне требуют научного осмысления также правовые положения о Российской Федерации (государстве) как субъекте, обеспечивающем безопасность граждан и общества в целом при применении информационных технологий и обороте цифровых данных. Кроме того, в организационно-правовой системе обеспечения информационной безопасности в России расширяется роль соответствующих государственных органов в сфере надзора за оборотом персональных данных и обеспечения их защиты, правовой статус которых должен быть закреплен в положениях государственных органов, обеспечивающих информационную безопасность личности, общества и государства. В целях развития конституционно-правовых основ в области информационной безопасности необходима новая концепция правового регулирования общественных отношений, обеспечивающих реализацию государственных мер в вопросах информационной безопасности личности и защиты граждан от современных цифровых угроз. И, несомненно, новеллы в Конституции РФ являются определенным импульсом для доктринального развития системы правового регулирования обеспечения национальной системы информационной безопасности и совершенствования государственной политики в области МИБ, международного сотрудничества в соответствии с новыми стратегическими задачами в этой сфере.

Эти вопросы относятся к правовому регулированию МИБ, представляющей собой такое состояние глобального информационного пространства, при котором на основе общепризнанных принципов и норм международного права и на условиях равноправного партнерства должно обеспечиваться поддержание международного мира, безопасности и стабильности. Система обеспечения МИБ в целях предотвращения или минимизации рассматриваемых угроз должна стать совокупностью международных и национальных институтов, регулирующих деятельность в глобальном информационном пространстве. На достижение этих целей направлена государственная политика России по предотвращению (урегулированию) межгосударственных конфликтов в глобальном информационном пространстве, а также учету национальных интересов России при формировании системы обеспечения МИБ.

Для реализации новых стратегических задач развития, как национальной информационной безопасности, так и системы МИБ сегодня необходимы не только фундаментальные междисциплинарные, правовые научные исследования, включая проблемы трансформации системы прав человека, принципов, но и, безусловно, продвижения российских инициатив в этой области в целях достижения консенсуса, а также возрастающей «морально-психологической мотивации востребованности научно-аналитической работы», как справедливо отмечает А.В.Зинченко в работе «Архитектоника международной информационной безопасности». Необходима интеграция усилий, направленных на комплексные научно-обоснованные исследования, связанные с обеспечением развития системы МИБ. Концепция Конвенции ООН об обеспечении международной информационной безопасности, размещенная на сайте Совета Безопасности РФ, безусловно, представляет научный интерес и нуждается в правовом осмыслении, структуризации на основе современных научных методов, включая конструктивизм, антропоцентризм, феноменологию и других.

Джеймс Эндрю Льюис
Старший Вице-президент и Директор Программы стратегических технологий Центра стратегических и международных исследований (CSIS), Вашингтон (США)

НОРМЫ И ПОДОТЧЕТНОСТЬ. БЕЗОПАСНОСТЬ И МЕЖДУНАРОДНОЕ СОТРУДНИЧЕСТВО В КИБЕРПРОСТРАНСТВЕ

Наиболее важные обязательства и правила поведения государств в киберпространстве содержатся в Уставе ООН – уважение суверенитета, невмешательство во внутренние дела и воздержание от применения силы или угрозы применения силы против другого государства. В ответ на возросшую озабоченность по поводу киберугроз миру и стабильности государства также разработали дополнительные нормы кибербезопасности и достигли консенсуса по одиннадцати нормам в Группе правительственных экспертов ООН 2015 года (ГПЭ). В этом докладе было также определено ответственное поведение государств в киберпространстве. Примечательно, что с тех пор эти нормы были одобрены всеми государствами-членами ООН по завершении Рабочей группы открытого состава (РГОС) в мае 2021 года. ГПЭ 2021 года, завершившаяся месяц спустя, добавила полезные разъяснения.

Глобальное соглашение об основах ответственного поведения государств является существенным шагом вперед в построении международной кибербезопасности и управлении стабильной, основанной на правилах средой, но опыт, накопленный с 2015 года, показал, что соглашения о нормах самого по себе недостаточно для достижения этого. Нормы включены в национальное законодательство и политику, но их имплементации недостаточно. Нормы должны соблюдаться государством в его поведении и в его отношениях с другими государствами. Неудача отражается в решении государства игнорировать нормы. Построение системы подотчетности требует установления последствий за эту неудачу. Это ключ к тому, чтобы сделать согласованные нормы значимыми.

Если государства не несут ответственности за злонамеренные действия, то в сегодняшней напряженной международной обстановке это означает, что нет никаких препятствий для игнорирования норм, когда это удобно. Для того чтобы нормы вступили в силу, должна быть ответственность и последствия для стран, которые решат их не соблюдать. Прошлая практика показывает, что подотчетность может быть усилена, если есть какие-то последствия в несоблюдении этих норм и других международных обязательств. Последствия включают в себя диапазон международно-правовых мер реагирования, доступных государствам, являющимся жертвой или объектом вредоносных кибердеяний, противоречащих согласованным нормам. Несмотря на некоторый прогресс в применении последствий (таких, как санкции Европейского союза или обвинения и санкции со стороны США), до сих пор это был разрозненный и разрозненный процесс, который не способствовал глобальному соблюдению норм и повышению уровня стабильности в киберпространстве.

Необходимость применять последствия в адрес злоумышленников указывает на центральную роль государств в придании нормам значимости. Несоблюдение норм не разрешается путем создания дополнительных норм. В этом контексте особо ценно тесное сотрудничество между гражданским обществом, частным сектором и правительствами, а неспособность привлечь гражданское об-

щество и частный сектор ослабит кибербезопасность в тех странах, которые решили этого не делать. Однако, прямая ответственность за создание и обеспечение соблюдения норм ложится на государства, которые должны разработать дипломатические, военные и разведывательные стратегии для повышения приверженности тому, что было согласовано в рамках ООН. Государства обладают уникальными возможностями для исправления ситуации, когда другое государство не соблюдает согласованные нормы. Усилия государства должны быть подкреплены гражданским обществом и частным сектором, но опыт показывает, что страны, которые не соблюдают согласованные нормы, вряд ли будут поколеблены действиями только гражданского общества или частного сектора.

Это объясняется тем, что сила или угроза применения силы остается основным источником ответственности в отношении другого государства, когда убеждение или побуждение потерпели неудачу. Государственные стратегии в отношении последствий и подотчетности должны отражать давно сложившуюся государственную практику применения дипломатии и силы. Государства обладают уникальными возможностями для применения силы и дипломатии, поскольку у них есть институты, занимающиеся применением силы и принуждения. Государства имеют право применять силу, чего не могут частные субъекты.

Установление последствий не является сдерживанием. Здесь не место для более продолжительной критики того, как стратегическое мышление времен холодной войны влияет и искажает обсуждение киберконфликта, но сдерживание – это концепция холодной войны, которая, как можно увидеть, имеет ограниченную ценность для киберконфликта. Другие концепции холодной войны, которые заслуживают пересмотра, включают эскалацию и просчеты. Эскалация и просчет остаются гипотетическими – примеров того и другого не существует, несмотря на высокий уровень вредоносной киберактивности в течение многих лет. Драматические сравнения между оружием массового уничтожения, ядерным оружием и кибератаками нереалистичны и искажают наше восприятие рисков, включая риск просчета и эскалации. В то время как любое введение последствий должно быть встроено в более широкую дипломатическую стратегию для объяснения и формирования восприятия международного сообщества и цели последствий, неуместный страх просчета и эскалации слишком часто становится оправданием бездействия. Вооруженный конфликт не будет соответствовать образцам 20-го века. Он был изменен новыми технологиями, в том числе кибертехнологиями. Результатом этих изменений является не то, что страны отказались от силы и принуждения; а то, что они нашли другие и более современные способы их использования, и наши стратегии должны адаптироваться к этому.

Конфликт теперь изменен таким образом, что кибероперации становятся все более важными. Называть этот новый вид конфликта серой зоной – значит вводить в заблуждение. Это не серая зона; это одно из главных мест для враждебных действий. В этом новом, часто скрытом конфликте атрибуция является одним из основных элементов, необходимых для создания подотчетности. Политическая атрибуция создает информационные условия, необходимые для подтверждения и объяснения действия. Это атрибуция, требуемая судом, но достаточная для того, чтобы убедить лиц, принимающих решения, и как внутреннюю, так и глобальную аудиторию в том, что ответ оправдан. Соразмерность ответа является еще одним требованием для наложения последствий, но это не та пропорциональность, которая описана в Женевской конвенции. Это тщательный расчет того, какие действия будут сочтены оправданными, а также эффективными для того, чтобы заставить целевое государство пересмотреть риски продолжения вредоносных действий.

Сочетание атрибуции и пропорциональности создает основу для наложения последствий. Необходимо рассмотреть вопрос об актуальности атрибуции не только для международного сообщества, но и для укрепления доверия с внутренней аудиторией. Прозрачность может укрепить доверие к атрибуции, но государства и субъекты частного сектора неохотно делятся данными, источниками и методами. Обеспечение ясности в отношении того, что имеют в виду разные страны, когда они говорят о правовой, политической, общественной или технической атрибуции, может

стать полезным первым шагом для будущих многосторонних дискуссий.

Но атрибуция и пропорциональность остаются суверенными вопросами. Идея многостороннего механизма атрибуции или какого-либо списка пропорциональных наказаний за неправильные действия маловероятна. Государства не захотят отказываться от суверенных полномочий определять источник нападения и форму, которую должен принять любой ответ. Ни одна страна не будет делегировать эти полномочия третьей стороне. Это не означает, что сотрудничество невозможно. В Совместном заявлении, опубликованном 28 странами о продвижении ответственного поведения государств в киберпространстве в сентябре 2019 года, эти страны согласились «работать вместе на добровольной основе, чтобы привлекать государства к ответственности, когда они действуют вопреки этим рамкам, в том числе путем принятия мер, которые являются прозрачными и соответствуют международному праву».

В конечном счете, согласованные РГОС нормы могут укрепить международное право и снизить уровень киберконфликтов. Однако, в промежуточный период полезно рассмотреть как перечень добровольных мер по привлечению государств к ответственности, так и вопросы, которые неизбежно возникают в связи с подотчетностью. К ним относятся стандарты доказывания, атрибуция и обмен информацией; механизмы координации коллективных действий; связь с другими мерами, такими как рамки для совместного дипломатического реагирования ЕС на вредоносную кибер-деятельность; гармонизация с международным правом и последствия других договорных обязательств для коллективной самообороны.

Если цель норм состоит в том, чтобы повысить стабильность в киберпространстве, то прогресс не так велик, как можно было бы надеяться. Успех РГОС 2021 года в достижении консенсуса в отношении норм ответственного поведения государств сместил дискуссию на то, что делать, когда нормы не соблюдаются. В связи с этим обсуждение было сосредоточено на политической атрибуции, соразмерных ответах и областях потенциального сотрудничества между государствами-единомышленниками. Дальнейший прогресс на пути к стабильности в киберпространстве требует не просто большего обсуждения, но и развития подотчетности с использованием атрибуции и применения последствий.

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

МЕЖДУНАРОДНО-ПРАВОВЫЕ АСПЕКТЫ АТРИБУЦИИ В ИКТ-СРЕДЕ В КОНТЕКСТЕ РАЗРЕШЕНИИ МЕЖДУНАРОДНЫХ СПОРОВ

Спасибо большое, Николай Николаевич.

Дорогие друзья, МИБ-овская семья, очень рад вас всех приветствовать! Сегодняшняя конференция уже выполнила свою функцию, по крайней мере для меня – я обрел друзей и услышал обстоятельные точки зрения наших партнеров.

Но все еще впереди, прекрасный диалог в течение трех насыщенных дней.

Традиционно так складывается ситуация, что с тринадцатой конференции, которая для меня была первой (хотя приглашения поступали гораздо раньше), мои выступления превращались в некие зарисовки и «фантазии на тему», что, в принципе, обоснованно, ввиду отсутствия четкого правового регулирования данной сферы.

Включение меня в спикеры этой секции достаточно неожиданно, но ее тематика является очень интересной, собственно в прошлом году я в ней и выступал. Хочется поделиться тем, что накопилось за год, соображениями, идеями, мнениями коллег, партнеров.

Первое, считаю важным отметить, что как и в прошлом году, позиция не изменилась: атрибуция должна строиться на универсальных, это раз, два –четких и всеобъемлющих международно-правовых нормах. Из этого исходит сообщество юристов-международников, представительства государств, погруженных в этот сюжет людей.

Второе – те или иные претензии по совершению компьютерных атак должны осуществляться на основании четких юридических критериев, имеющих универсальный характер.

Второй аспект этого процесса с нашей точки зрения – любая компьютерная атака является преступлением.

Далее уже могут идти различного рода вариации. Я бы предложил зафиксировать эти два момента и, дальше двигаться основываясь именно на них.

Что касается первого, а именно отсутствия или наличия правовых норм в данной сфере, хочется поделиться соображением – ощущением себя, как я недавно на двухсторонних переговорах сказал, «legal alien» («Englishman in New York»). Ты вроде как взращивался в системе международного права: чему-то учился, приобретал знания, знакомился с теоретиками, практиками, в том числе создателями огромного количества правовых норм, и тут ты сталкиваешься с огромным количеством мнений со стороны определенного ряда государств, что правовых норм достаточно, ничего не нужно, регулирование уже устоялось, и следует действовать в его рамках. И здесь сразу всплывает ряд примеров, довольно странных.

В космической отрасли «бурление» происходит, я имею в виду в международно-правовой части данной отрасли.

Соответственно, конвенции по дорожному движению, например, ставят перед собой вопросы как же быть с беспилотниками, с искусственным интеллектом и так далее, как регулировать этот универсальный процесс, который охватывает все государства.

Международное морское право, которое зарождалось массой обычаев, процессов, норм, более двадцати лет желалась конвенция, потом происходило различное развитие этих норм, в том числе Конвенция ООН по подводному культурному наследию, когда че-

ловечество пришло к пониманию, что нужно заниматься объектами историческими, которые под водой находятся, сто лет, не сто лет, что мы с ними будем делать, как спасать, куда двигаться и так далее.

В итоге, начинают присоединяться государства, регулирование новых сфер, в том числе с развитием технологий, обновляется и совершенствуется. И тут вот возникает закономерный вопрос, почему мы, собственно, пытаемся закрыть глаза и сделать вид, что для ИКТ-сферы вопросов нет: все урегулировано, все закрыто, есть Устав ООН, есть принципы, и ничего менять и дорабатывать не нужно.

Здесь Россия все время выступает с интересными инициативами. При том, не могу сказать, что они заведомо обречены на успех.

Что касается Конвенции по противодействию преступлениям в сфере ИКТ, это серьёзный огромный документ, в котором придётся очень много лет мировому сообществу работать.

Успеем ли мы за скоростью движения преступников неизвестно, но, тем не менее, когда мы переходим к разговору о том, что можно расследовать, любой правоохранитель сразу говорит: а где основание, где запрос, где документ, где формальное обличение всех действий, с чем я пойду в суд, и так далее. Соответственно, тот или иной документ нужен, хотя бы минимально.

Дальше, у нас была инициатива, которая презентована у всех в пакетах, это концепция Конвенции ООН по международной информационной безопасности. Никто не говорит о том, что это совершенно готовый к работе документ. Мы просто тем самым демонстрируем, что международно-правовое регулирование этой сферы необходимо.

Более семидесяти лет назад были заложены международно-правовые правила игры для всех государств. Мы об этом договорились, перед этим очень много миллионов человек полегло. А теперь мы пытаемся закрыть на это глаза, и сделать вид, что ничего не происходит. Появляются новые сферы, новые процессы, новые коммуникации, и регулировать мы это не хотим. Большая надежда на то что мы дойдем до того, что нам нужна эта серьезная дискуссия и на самом деле есть совершенно прикладные признаки того, что она действительно необходима. Если глубоко погрузиться в анализ докладов ГПЭ, РГОС совершенно очевидно, как интенции меняются и потихоньку просачивается четкое понимание, что международно-правовое регулирование этой сферы будет и должно развиваться.

Прорывом было, я считаю, последнее признание того, что гуманитарное право применимо только в случае вооруженного конфликта. На мой взгляд, просто финализация двадцатилетнего диалога о том, что в мирное время применять, что-то с ним делать, его модифицировать. Представители Красного Креста, замечательные наши коллеги, разработали документ то ли 2007, то ли 2009 года, two-page, в котором написано, что есть природа гуманитарного права. Там все четко сказано – только в случае вооруженного конфликта. Удобно и понятно, соответственно.

Тем самым, попадая в эту практическую секцию со своими правовыми нюансами, я все время погружаю в них большое количество наших гостей. В связи с этим традиционно предлагаю переносить юридическую дискуссию в отдельную ветвь Конференции и выходить только с качественным результатом. Мы, собственно, пытаемся это делать внутри страны, у нас есть и большая группа по международному праву и большая группа по глоссарию, который мы вырабатываем и делаем, формируем позицию и видение Российской Федерации на данном направлении. Мне кажется, мы неплохо продвинулись по сравнению с многими зарубежными коллегами, с которыми у нас строится дискуссия, обмениваемся опытом и есть понимание, что в принципе мы достаточно активны и результативны. Здесь речь идет о том, что международно-правовой диалог совершенно необходим и все равно так или иначе мы придем к такому правовому состоянию, когда эти отношения между государствами будут урегулированы. Лучше это понять раньше, чем позже.

Это первый блок. Второй блок касательно преступлений. Надо сказать, что пока критерии и правовые основания атрибуции не установлены. У нас есть неплохо существующие правовые механизмы для того, чтобы устанавливать те или иные негативные действия государств или физических лиц в отношении третьих лиц. Это и механизмы правовой помощи по уголовный делам, и механизмы полицейского сотрудничества в области противодействия

преступлениям, это и взаимодействие по каналам Интерпола, это и, если переходить на более высокий уровень, урегулирование международных споров мирными средствами (то есть путем переговоров, консультаций и т.д.)

Хочу отдельно подчеркнуть, что когда мы поднимали речь о преступлениях, то есть привязывая любую компьютерную атаку к преступлению, я предлагал подумать на тему состава преступления как такового. Здесь я предложил секретариату нашей конференции зафискировать, что у нас присутствуют правоохранители, с которыми мы постоянно в дискуссии – Тимерлан Салихов и Николай Гудков. Это очень большие активные умы, и я бы вышел с таким предложением, чтобы мы к следующему заседанию, к следующей нашей конференции коллективно, я себя не устраняю от этой работы, а готов, наоборот, в нее включиться, представили бы вам анализ того, как соотносятся с нашей точки зрения компьютерная атака и состав преступления, в принципе. Разложили действия тех или иных лиц, осуществляющих компьютерные атаки, по элементам и признакам состава преступления. В этом контексте, мы с нашими самыми главными партнерами разговариваем на достаточно разных языках. Состав преступления у нас содержит субъект, объект, субъективную, объективную сторону, а, по моим данными, в США – факт преступления, и факт наличия вины, то есть более сокращенная сущность этого процесса. Соответственно, и здесь нам нужно беседовать и находить компромисс.

Важно помнить о том, что у нас есть договоренности, которые позволяют осуществлять совершенно четкий правовой обмен и переводить обвинение в плоскость правовой помощи по уголовным делам. Мы всегда открыты к запросам, готовы их верифицировать, реализовывать, проверять и, если есть на то основания, наказывать. Но возникает момент, что обвинения поступают в некое пространство, а официальные запросы поступают в диаметрально уменьшающейся пропорции, то есть практически не поступают.

Речь о том, что на данный момент у нас есть в руках правовой механизм, которым можно пользоваться, чтобы устанавливать источник совершения противоправных деяний и, соответственно, налаживать взаимодействие между государствами с целью их прекращения.

Благодарю за внимание!

А.В. Шевченко
Доктор политических наук, профессор, и.о. декана факультета национальной безопасности Института права и национальной безопасности РАНХиГС при Президенте РФ

ПОЛИТИЧЕСКАЯ ЛЕГИТИМАЦИЯ АКТОВ ПРИМЕНЕНИЯ СИЛЫ В ИКТ-СРЕДЕ

Угроза милитаризации киберпространства относится к одной из наиболее опасных угроз и вызовов международному миру и безопасности. Она исходит из стратегической политико-идеологической позиции США: информационная война с Россией, Китаем, Ираном, Северной Кореей признана Капитолием более важной задачей, чем противодействие терроризму. Стратегические подходы США к проведению операций в киберпространстве включают ряд самопровозглашенных (сформированных вопреки международному праву и соглашениям об обеспечении международной информационной безопасности) установлений, которые следует рассматривать как вызов эффективности применения международного и гуманитарного права к регулированию информационных конфликтов.

В официальные документы военного ведомства введено понятие «атака в киберпространстве», означающее действия, приводящее к значимым негативным последствиям не только в самом киберпространстве, но и в других сферах жизнедеятельности человека. Такое определение приравнивает атаку по силе воздействия к огневому поражению[1].

На безответственном в политическом смысле основании, что киберпространство не имеет государственных границ, американское законодательство разрешает проводить кибероперации в любом иностранном киберпространстве – в так называемых «красной» и «серой» зонах – без уведомления органов власти этих государств. Инициировать и проводить операции в киберпространстве США могут в превентивном порядке, якобы, чтобы создать препятствия предполагаемому противнику для осуществления им некой злонамеренной деятельности, а не только в ответ на воздействие на киберпространство США.

Такая политика полностью противоречит предписаниям международного права о неприменении силы в международных отношениях. При этом усилия госдепа и силовых ведомств США направлены на обеспечение легитимности милитаризации киберпространства, поддержки эскалационной политики мировым сообществом и транснациональными компаниями. Ибо оценка мощи государства определяется и показателями международного признания правовой и моральной допустимости его действий[2].

Легитимность отражает фундаментально значимое для правящего режима свойство государственной власти осуществлять политическую диффузию, посредством которой политический выбор одного субъекта оказывает влияние на политический выбор другого. Очевидна цель США в создании процессов международно-политической диффузии в киберпространстве – проникновения проамериканской властной интенции в мировое общественное сознание. Здесь налицо откровенное прене-

1 Запивахин В.О. Милитаризация киберпространства – главная угроза международной информационной безопасности /Сборник докладов участников четырнадцатого международного форума «Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности». 7-9 декабря 2020 г. Москва

2 Коростелев С.В. Политическая легитимация актов применения силы в международных отношениях. Дис…д.полит. н. СПбГУ, 2021 г.

брежение ст. 4 Конвенция Монтевидео о правах и обязанностях государств.

В исполнении США обеспечение легитимности однозначно направляет силовые линии международно-политического коммуникативного пространства, или пространство международно-политического дискурса, на отрицание норм международного права. При этом общеизвестно, что легитимация конкретного акта применения силы устанавливается на дискуссионных площадках Совете Безопасности ООН. Устав ООН предопределяет характер обоснования актов применения силы, требуя от государств гарантий того, что их действия во всяких случаях будут проводиться в соответствии с миссией ООН, признающей каждый акт применения силы заведомо «неправомерным». И любое государство обязано доказать, что его действия являются «справедливыми» и должны быть признаны легитимными. Именно поэтому агрессор стремится получить поддержку и СБ ООН как структуры международно-политического органа, и благодаря ей снизить политические и репутационные издержки обращения к силе.

С очевидностью встает вопрос о необходимости противодействия практике и попыткам осуществлять правовую и политическую легитимацию актов применения силы в информационно-коммуникационной и информационно-коммуникативной среде. Он касается, во-первых, проблем теоретико-методологического характера, охватывающих широкое междисциплинарное поле политической науки, международных отношений, международного права и международного информационного права. Так, ни на одном из этих направлений не сформулировано определение понятия «применение силы» в ИКТ-среде, что порождает терминологическую неопределенность. А именно это понятие должно облечь политический процесс принятия решений о применения силы в ИКТ-пространстве в правовые нормы международного информационного права и соответствующие положения документов ООН. Критерии соразмерности для исключительного большинства инцидентов, происходящих в традиционных сферах применения силы международным гуманитарным правом, определены (чего нельзя сказать о сфере ИКТ).

Второй аспект проблемы политической легитимации акта применения силы, то есть, обеспечения признания его справедливым способом достижения национальной цели, в межгосударственных отношениях в целом и в ИКТ-среде, в частности, связан с процессами поиска и заявления обоснования необходимости и соразмерности такого акта степени угрозы или встречной агрессии.

Справедливо утверждение о том, что необходимость легитимации акта необоснованного применения силы является по сути политической, приемлющей морально-этическое оправдание, а правовой дискурс является лишь риторическим оформлением, скрывающим сущность факта[3].

Установлены алгоритмы действий заинтересованных государств, вписывающиеся в процедуры апелляции к значимым международным институтам, но прежде всего – к международному праву. Причем агрессор обычно, если не всегда, находит юридические аргументы в свою поддержку со стороны СБ ООН (так было в ситуациях с оправданием применения силы США против Югославии, Ливии, Ирака и т.д.). Однако в случае с политико-информационными инцидентами такие аргументы пытаются привести к зачастую сфальсифицированным фактам или введенным в общественный дискурс симулякрам и фейкам (пресловутое «вмешательство» России в ИКТ-пространство США во время выборов президентом Д. Трампа и последовавшие политические санкции против РФ).

Данное явление петербуржский политолог и правовед-международник, доктор политических наук С.В. Коростелев определяет как «стратегический легализм», т.е. использование норм права, либо юридической аргументации для обеспечения достижения масштабных политических целей, вне зависимости от фактических обстоятельств или содержания норм права. Разъяснение основным международным акторам рациональности своих действий по продвижению национальных интересов (реализация стратегии национальной

3 Кириленко В.П., Коростелев С.В. К вопросу о праве государств на упреждающее применение военной силы. Ч. I, II // Военная мысль. №8-9 2011; Пыж В.В., Фролов А.Е., Козлов С.В., Кононович И.А. Национальная безопасность и военная политика государства: Монография. – Чебоксары: Новое время, – 2010.

безопасности) в терминах парадигмы ООН составляет сущность процесса «стратегического легализма»[4].

Объектом метода стратегического легализма, разработанного С.В. Коростелевым, является обеспечение органов государственной власти и военного управления международной правовой аргументацией для обоснования того, что государство справедливо применяет силу, а противник не имеет ни правовых, ни моральных оснований для ее применения.

В основе метода лежит избегание обобщений, присущих нормам права. Каждая из сторон конфликта стремится сформулировать такое узкое толкование нормы, чтобы оно могло быть применено для обоснования правомерности позиции государства только в данной ситуации, и ни в коем случае не могло бы быть использовано для его осуждения в иных сходных ситуациях.

Анализируя дискурсивное поле, перманентно наполняемое за счет новых международно-политических инцидентов, захватывающих информационно-коммуникативную сферу, общественность всякий раз вопрошает и с высоких трибун официальных форумов, и в сетевых сообществах: есть ли какие-либо методы для оценки моральности поведения государств при обеспечении ими своих корыстных интересов с позиций международного права? Каким образом государству присваивается юридическая ответственность за решение на применение силы?

Ответ однозначно исключает возможность присвоения международной ответственности при нарушении государством норм международного права в рамках метода стратегического легализма, поскольку метод не является правовым по сути. А использование государством-агрессором международного права лишь в качестве эпифеномена имеет целью уменьшить или вовсе снять с себя международно-политическое давление, спровоцированное неправомерным применением силы. Иными словами, прием «правового прикрытия» неправовых действий сам по себе нелегитимен.

Россия имеет признанный опыт исследования феноменов политического легализма, выявления эффектов двойных стандартов в международно-политической практике организации и функционирования информационного пространства, формулирования инициатив правомерного поведения государств в ИКТ-среде. Факты недобросовестного использования терминологии Устава Организации Объединенных Наций, тезауруса международного права и гуманитарного права должны быть не только юридически профессионально распознаваемыми, но и политически публично осуждаемы. Учитывая степень угроз международной информационной безопасности, к противоборству дискурсов российской стороне следует привлечь дополнительные коммуникативные ресурсы дипломатических миссий, средств массовой информации, сетевых сообществ. Для достижения целей правового обеспечения международной информационной безопасности нужно постоянно пресекать спекуляции нормами международного информационного права. Возможно, это направление будет включено в исследовательскую повестку-2022 Рабочей группы открытого состава ООН.

4 Коростелев С.В. Проблема классификации объектов применения силы в информационных конфликтах // Управленческое консультирование. 2020. № 8; Коростелев С.В. Внешнее вмешательство путем информационного воздействия: проблема нормативной оценки // Пути к миру и безопасности. 2019. Т. 57. № 2. 223. Коростелев С.В. Действие метода стратегического легализма в международных отношениях / Глобальный экономический кризис: реалии и пути преодоления. Сборник научных статей, Вып. 7 / Под общей редакцией проф. В.В. Тумалёва. – СПб.: НОУ ВПО Институт бизнеса и права, 2009.

Ашраф Патель
Институт глобального диалога (ЮАР)

ФИНАНСОВО-ТЕХНОЛОГИЧЕСКАЯ И ЦИФРОВАЯ ИДЕНТИФИКАЦИЯ ДЛЯ РАЗВИТИЯ В АФРИКЕ

Повестка дня Организации Объединенных Наций на период до 2030 года, включая Цели в области устойчивого развития, является революционной в своих намерениях: никого не оставлять позади. Этот план устойчивого развития, принятый ООН в 2015 году, предусматривал лучший мир для всех людей. После трех лет реализации страны постепенно начинают разрабатывать политику, планы и даже несколько бюджетов для достижения этой цели. Однако, как мы можем отслеживать прогресс в достижении Целей устойчивого развития, когда примерно две трети показателей не сопровождаются данными? Хотя в наших коллективных усилиях по отслеживанию Целей устойчивого развития существуют очень серьезные проблемы с данными, несколько многообещающих тенденций дают нам надежду на то, что мы движемся в правильном направлении.

Во-первых, широко признается важность общественного договора в отношении статистики и людей. Страны по всему миру уделяют особое внимание тому, как мы укрепляем и поддерживаем доверие к нашим данным и к решениям, основанным на этих данных. Мы не должны принимать это доверие как должное. Нам нужно постоянно его зарабатывать, активно защищать и относиться к нему как к фундаменту, на котором мы работаем. Доверие – это валюта, с помощью которой мы зарабатываем возможность влиять на общественное обсуждение и принятие решений.

Финансовые технологии, в просторечии называемые «финтехом», ускоряют расширение доступа к финансовым услугам в странах Африки к югу от Сахары – регионе, который традиционно страдает от ограниченного доступа к официальным финансовым услугам, таким как кредит, страхование и банковское дело. В то время как в последние годы возможности, открывшиеся благодаря этой технологии, открыли двери для многих в регионе, особенно для семей с низкими доходами, пользователи финтеха используют этот инструмент все более и более изощренными способами, как видно из недавней статьи Financial Technology Partners, бутик-инвестиционно-банковской фирмы, в которой раскрываются перспективные инвестиционные тенденции в африканской индустрии финтеха. Население Африки, вероятно, продолжит использовать растущее проникновение сотовой связи и Интернета в регионе и внедрять новые цифровые платежные, банковские, страховые и кредитные услуги. Таким образом, авторы предполагают, что спрос Африки на финансовые услуги – особенно с учетом того, что население по-прежнему в значительной степени не имеет или недостаточно обеспечено банками, а также является вторым в мире по темпам роста рынком платежей и банковских услуг – скоро обойдет традиционные банковские системы. Важно отметить, что континент уже является крупнейшим разработчиком систем мобильных денежных переводов, включает почти половину зарегистрированных клиентов мобильных денег в мире, примерно 70 процентов глобальных транзакций мобильных денег и две трети объема транзакций по стоимости. Несмотря на этот успех, сохраняются проблемы с использованием инструментов новыми и инновационными способами: действительно, авторы утверждают, что сохраняющееся низкое проникновение сетей сотовой связи и Интернета, особенно в сельских районах Африки, свидетельствует о том, что услуги мо-

бильных денег все еще имеют значительный потенциал роста в регионе.

Всемирный банк определяет цифровую идентификацию как набор электронных и сохраненных атрибутов и учетных данных, которые могут однозначно идентифицировать человека. Согласно отчету Identification for Development (ID4D), в 2018 году в мире насчитывалось около миллиарда человек, у которых не было какой-либо признанной идентификации. Отсутствие какой-либо приемлемой идентификации может ограничить способность людей получать доступ к важнейшим услугам (например, здравоохранению и образованию), а также их участие в официальной политической жизни (например, голосование) и экономической жизни (например, занятость). Некоторые из проблем, с которыми сталкивается Южная Африка в плане создания безопасного и инклюзивного реестра населения, проистекают из отсутствия политики и законодательной базы или недостаточных попыток ее создания. Другие проблемы включают устаревшие и фрагментированные административные системы.

При тщательной разработке цифровая идентификация может позволить людям более полно участвовать в экономике и обществе в качестве потребителей, работников и граждан, принося пользу себе, а также компаниям и государственным учреждениям, с которыми они взаимодействуют. Но что мы подразумеваем под хорошим цифровым удостоверением личности и как это работает? В отличие от бумажного удостоверения личности, такого как большинство водительских прав и паспортов, цифровое удостоверение личности можно проверить удаленно, часто по более низкой цене. В то же время атрибуты хорошей идентификации (ID), созданные и используемые с индивидуального согласия, будут способствовать укреплению доверия и защите конфиденциальности. Хорошая цифровая идентификация работает, открывая ценность для людей, когда они взаимодействуют с фирмами и правительствами, как потребители, работники, микропредприятия, налогоплательщики, бенефициары. Это могло бы помочь в предоставлении финансовых услуг для 1,7 миллиарда с лишним человек, которые, по оценкам Всемирного банка, в противном случае будут исключены из банковской деятельности. Это также может помочь сэкономить около 110 миллиардов часов за счет оптимизации электронных государственных услуг, включая социальную защиту и прямые выплаты пособий. Чтобы понять, насколько все эти преимущества могут быть полезны, мы проанализировали почти 100 способов использования цифрового удостоверения личности в семи различных странах: Бразилии, Китае, Эфиопии, Индии, Нигерии, Соединенном Королевстве и Соединенных Штатах. Экстраполируя глобально, мы обнаружили, что среди развивающихся экономик средняя страна может достичь экономической ценности, эквивалентной шести процентам ВВП в 2030 году, в то время как в развитых экономиках средняя страна может достичь экономической ценности, эквивалентной примерно трем процентам – и то, и другое при условии высокого уровня внедрения с поддержкой цифровой инфраструктуры.

Получение значения хорошего цифрового удостоверения личности ни в коем случае не является определенным или автоматическим. Требуется тщательная разработка системы и продуманная государственная политика для содействия ее реализации, снижения рисков, подобных тем, которые связаны с крупномасштабным сбором персональных данных или систематическим исключением, а также для защиты от проблем, связанных с потенциальными технологиями двойного назначения. Подобно ядерной энергии и GPS, технологии двойного назначения предназначены для пользы, но также могут быть использованы во вред. Люди будут использовать цифровое удостоверение личности, если оно обеспечивает ценность, вызывает доверие и защищает конфиденциальность. Учреждения будут привлечены к использованию, которое снижает затраты, улучшает качество обслуживания клиентов или, в случае государственных учреждений, улучшает благосостояние. По мере расширения программ цифровой идентификации политики, бизнес-лидеры и международные организации должны работать вместе, чтобы лучше понимать риски и разрабатывать стандарты и методы управления для их снижения. Хотя это может показаться большим усилием, оно того стоит. В конце концов, цифровое удостоверение личности может стать следующим рубежом глобального инклюзивного роста.

Цифровое удостоверение личности в Африке – Проблемы и возможности

Создание и укрепление доверия вверх и вниз по линии ценности данных начинается в первую очередь с прозрачности. За последние пять лет как государственный, так и частный секторы, включая Фонд Билла и Мелинды Гейтс, Фонд Wellcome Trust, разработали политику обмена данными, которая поощряет бесплатное использование и повторное использование данных и улучшает доступность через открытые порталы данных. Группа Всемирного банка сделала доступ к данным основным принципом и частью нашей приверженности обмену знаниями для улучшения жизни людей.

Правовая идентификация стала решающей для социальной защиты, финансовой интеграции, миграции и даже для преодоления кризисов, таких как пандемия Covid-19. Вот почему важной целью Повестки дня Организации Объединенных Наций в области устойчивого развития (2015 год) является обеспечение правовой идентичности для всех к 2030 году. Многие утверждают, что работа по достижению этой цели должна начинаться в Африке, где, как сообщается, проживает более 40% тех, у кого нет удостоверений личности в мире. Усилия по совершенствованию национальных систем идентификации совпали с растущим внедрением мобильных технологий, а это означает, что глобальные процессы идентификации быстро развиваются. Растущая доступность мобильных телефонов привела к тому, что некоторые субъекты поощряют цифровые вмешательства для облегчения форм идентификации – часто с помощью биометрических атрибутов. Цифровые удостоверения личности, например, становятся все более популярными с 2015 года из-за их относительной простоты, низкой стоимости и удобства по сравнению с аналоговыми системами.

Например, на межправительственном уровне Всемирный банк разработал Принципы идентификации в контексте развития (одобренные многочисленными партнерами) и объединил различные заинтересованные стороны в рамках партнерства ID2020, в котором основное внимание уделяется тому, как цифровые технологии могут способствовать внедрению юридических идентификационных данных. А в 2021 году Комиссия Африканского союза, как сообщается, также работает над разработкой континентальной системы цифровой идентификации для принятия в октябре. Континентальный энтузиазм в отношении мероприятий по цифровой идентификации часто поддерживается глобальными инициативами или финансированием, направленными на извлечение большей выгоды из Африканской зоны свободной торговли. Различные многосторонние учреждения, глобальные НПО и иностранные доноры в то же время оказывают техническую поддержку, а также финансируют внедрение цифровых удостоверений личности в странах Африки к югу от Сахары.

Помимо заверений, которые цифровой идентификатор, по-видимому, обещает выполнить для экономического развития и вклада в ВВП, он также может способствовать достижению других целей, от социальной защиты до миграции и преодоления кризисов, таких как пандемия. Однако, эти возможности сопровождаются рисками, которые необходимо смягчать с точки зрения политики.

Популярные обеспокоенности, связанные с цифровыми удостоверениями личности, включают в себя то, как государственные и частные цели влияют на внедрение цифровых удостоверений личности; являются ли вмешательства обязательными или добровольными; какова степень предлагаемого сбора данных и как (индивидуальная и коллективная) затрагивается конфиденциальность; кто получает выгоду и кто исключен из таких вмешательств; кто имеет право на доступ к данным и для каких целей; существует ли риск срыва миссии; и каковы другие сопутствующие риски и преимущества таких вмешательств. Например, в недавнем докладе о цифровом удостоверении личности в Уганде утверждается, что национальная система цифрового удостоверения личности страны – Ndaga Muntu – привела к «массовому отчуждению, закрытию до трети взрослого населения Уганды и стала препятствием для женщин и пожилых людей, а также многих других маргинализованных лиц, для доступа к их правам человека».

Учитывая растущее число примеров, подобных этой критике системы Ndaga Muntu, растущий интерес к цифровым удостоверениям личности на континенте и во всем мире сопровождается острой необходимостью изу-

чить их влияние на права человека, верховенство закона и людей, которые будут включены (или исключены) из соответствующих социально-технических систем. Граждане могут оказать большое влияние, особенно на начальном этапе, на формирование приоритетов и спроса на данные. Это может означать, что национальные статистические управления будут играть более активную роль в партнерстве с гражданами и гражданским обществом, участвующими в подготовке и использовании данных для устойчивого развития, активно укрепляя доверие и используя важные новые источники данных. Например, в Индии насчитывается более 3 миллионов организаций гражданского общества, многие из которых способны собирать данные, связывать ученых с местными лидерами изменений и способствовать улучшению мониторинга социальных условий. Поиск путей согласования и сотрудничества, включая использование данных, полученных от граждан, имеет важное значение для будущего обсуждения данных о развитии и будет способствовать более эффективному отслеживанию прогресса в достижении Целей устойчивого развития.

Во-вторых, признается, что ключевая роль данных в разработке политики заключается в том, чтобы сделать невидимое видимым. Данные на национальном и субнациональном уровнях должны быть дезагрегированы по возрасту, полу, социально-экономическому положению, миграционному статусу и другим характеристикам. Располагая точными, репрезентативными, всеобъемлющими и дезагрегированными статистическими данными, мы можем определить, кто отстает и на сколько, и, следовательно, проводить целенаправленную политику для решения их проблем.

Включение в статистику часто начинается с включения в общество. Даже при беспрецедентном количестве новых инициатив и подходов к совершенствованию производства данных «никого не оставлять без внимания» часто является сложной задачей в некоторых странах с низким и средним уровнем дохода, где формы идентификации могут быть нестандартными. Хотя в таких странах, как Перу и Индия, где национальные статистические управления начали публиковать дезагрегированные данные, были достигнуты улучшения, многие страны страдают от нехватки соответствующего потенциала. Это критически важная миссия для таких инициатив, как Идентификация для развития (ID4D), по оценкам которой 1.1 миллиард человек во всем мире не могут официально подтвердить свою личность, и почти половина из них – дети, рождение которых не зарегистрировано. Когда они умрут, мы вряд ли узнаем почему, упустим шанс того, что эти трагедии могут послужить основой для политики, способной улучшить здоровье будущих поколений. Для того чтобы эти люди были учтены в официальной статистике и имели доступ к возможностям, созданным экономическим ростом, им необходимо иметь официальную запись о своем существовании.

В-третьих, существует огромный потенциал для трансформационной роли новых технологий в информационном пространстве развития. Хотя мы признаем, что не можем предсказать влияние конкретных технологий, мы можем предсказать, что стоимость сбора, анализа и визуального представления данных будет продолжать быстро снижаться. Революция в области больших данных помогает правительствам переосмыслить решения и улучшить предоставление услуг для достижения Целей устойчивого развития. Например, на Гаити мобильные телефоны используются для подключения городских жителей к рабочим местам, услугам и экономическим возможностям. На Филиппинах правительства используют данные GPS от такси для уменьшения числа несчастных случаев и улучшения работы экстренных служб. Проекты Группы Всемирного банка используют большие данные и искусственный интеллект, чтобы помочь правительствам лучше контролировать политику достижения Целей устойчивого развития, часто работая с партнерствами, ведущими эту работу. Хотя существуют важные проблемы и риски, связанные с большими данными (включая риски конфиденциальности), эта развивающаяся технология открывает огромные возможности в части улучшения результатов развития для людей.

Во время Международной конференции Движения Красного Креста и Красного Полумесяца в декабре 2019 года прозвучал четкий призыв к более широкому и эффективному распространению знаний и стандартов в области защиты данных в рамках Движения. В ответ на этот призыв на основе Руковод-

ства была разработана учебная программа. Европейский центр по вопросам конфиденциальности и кибербезопасности, юридический факультет Маастрихтского университета и Управление по защите данных Международного Комитета Красного Креста (МККК) в сотрудничестве с Центром гуманитарных данных Управления Организации Объединенных Наций по координации гуманитарных вопросов, Международной организацией по миграции, Международной Федерацией Обществ Красного Креста и Красного Полумесяца (МФКК) предлагают эту программу обучения и сертификации, специально разработанную для сотрудников в целях защиты данных в гуманитарной деятельности. Этот курс стал возможен при поддержке Директората по сотрудничеству в целях развития и гуманитарным вопросам Министерства иностранных и европейских дел Люксембурга.

Мобильные деньги для развития в Африке

Сегодня пользователи мобильных денег могут инициировать международные денежные переводы непосредственно со своих мобильных телефонов только в 16 из 93 стран, где доступны мобильные деньги. Отчасти это объясняется тем, что регулирование во многих странах запрещает операторам мобильной связи отправлять, а в некоторых случаях и получать международные денежные переводы. Необходимы смелые реформы для содействия усилению конкуренции и снижению цен, чтобы ускорить достижение Целей устойчивого развития ООН.

Международному союзу электросвязи ООН и международному сообществу следует включить мобильные деньги в качестве ключевого компонента любой политической инициативы, направленной на снижение стоимости денежных переводов, и регулирующим органам необходимо создать открытые и равные условия для международных денежных переводов. Нетрадиционные поставщики услуг, такие как поставщики мобильных денег, должны быть в состоянии конкурировать с традиционными поставщиками услуг по переводу денежных средств. Преобразования, которые мы наблюдаем во многих областях – от энергетики и мобильности до здравоохранения, сельского хозяйства и финансовых услуг, – все это зависит от цифровых технологий, а также множества связанных с ними бизнес-экосистем. Все эти технологии и системы должны быть надежными, безопасными и заслуживающими нашего доверия. Глобальная инициатива по расширению доступа к финансовым услугам представляет собой открытую основу для сотрудничества, возглавляемого Международным союзом электросвязи (МСЭ), Группой Всемирного банка и Комитетом по платежам и рыночной инфраструктуре.

Партнерство объединяет экспертные знания для ускорения доступа к цифровым финансовым услугам. При поддержке Фонда Билла и Мелинды Гейтс мы собрали весь спектр заинтересованных сторон, готовых воспользоваться этим опытом. Группа Всемирного банка и Комитета по платежам и рыночной инфраструктуре помогли сформировать четкое понимание политических соображений, связанных с цифровой идентификацией и стимулированием использования электронных платежей. Работа МСЭ сосредоточена на безопасности, инфраструктуре и доверии – защищенных финансовых приложениях и услугах, надежной цифровой инфраструктуре и, как следствие, уверенности потребителей в том, что наши деньги и цифровые удостоверения в безопасности. Для дальнейшего развития цифровой идентификации в Африке требуется гораздо больше инвестиций.

П.Л. Пилюгин
К.т.н., Центр проблем информационной безопасности ВМК МГУ

АТРИБУЦИЯ ИНЦИДЕНТА ИБ ПО КОСВЕННЫМ ПРИЗНАКАМ (СОБЫТИЯМ БЕЗОПАСНОСТИ)

На международной научно-практической конференции «Цифровой след как объект судебной экспертизы» отмечалось, что «за последние 3 года более 200 экспертных заключений и постановлений о назначении судебной экспертизы… при расследовании дел, связанных с незаконным доступом к охраняемой законом информации…. в 98% случаев следственные и судебные органы обращаются за помощью к специалисту в области судебной компьютерной технической экспертизы»[1]. При этом существенна «невозможность восприятия (цифровых следов) непосредственно органами чувств, а только с помощью специальных устройств и программ; (это выдвигает) требование (создания) новых, отличных от традиционных, способов, методов и процедур по обнаружению, фиксации и обеспечению сохранности (цифровых следов)»[2].

При этом особо важно отметить не только роль эксперта и соответственно предъявляемые к нему требования, чтобы исключить субъективный фактор. Но и также на какой информации основаны его выводы и как он к ним пришел. То есть существующие возможности использования сертифицированных способов и процедур по обнаружению, фиксации и обеспечению сохранности цифровых следов.

В частности последние известные это атаки на систему выборов в РФ. По опубликованной сначала информации атак было за пятницу – субботу 3 и последняя из них DDOS. В то же время президент «Ростелекома» Михаил Осеевский рассказал, что на системы онлайн-голосования и связанные с выборами порталы, включая сайт ЦИК, за три дня голосования совершили 19 атак. При этом некоторые из атак были очень короткими и продолжались всего несколько минут. Наиболее масштабную зафиксировали в последний день выборов: она наблюдалась в течение 5 часов 32 минут. Были атакованы разные ресурсы – «порталы ЦИК, портал выборов, портал госуслуг, портал ЕСИА, портал mos.ru». «В этих атаках участвовали зараженные устройства из самых разных стран: Индия, Индонезия, Бразилия, Украина, Иран, Таиланд, Бангладеш, Китай, Россия, Соединенные Штаты, Германия, Вьетнам, Литва и многие-многие другие»[3].

Эти события вызывают вопросы в отношении их атрибуции:

- Сколько все же атак было и с какой интенсивностью они происходили?
- В чем состояли эти атаки?
- Что значит половина атак из США? Как это определили?

Обычно источники признаков событий ИБ определяемые в процессе расследования инцидента получаются в результате следующих действий[4]:

- Поиск по артефактам в ОС следов вредоносной активности
- Использование меток времени и воссоздания сценария инцидента
- Анализ истории браузера и электронной почты
- Идентификация и восстановление удаленных файлов
- Анализ сетевого трафика с применением различных инструментов
- Идентификация и отслеживание вредоносной активности в дампах памяти
- Идентификация и дампинг представляющих интерес областей памяти
- Восстановление хронологии инцидента с использованием меток времени
- Создание единой хронологии для всех артефактов

То есть когда инцидент уже произошел и есть возможность исследовать его последствия и состав получаемых признаков может быть совершенно различным.

Однако следует учитывать и предыдущие события, так как атака не только целенаправленная деятельность, но последовательная цепочка таких действий, которые мы можем наблюдать как последовательности событий. Зная последовательность действий противника, можно не только противостоять нападению, но и зафиксировать эту последовательность как атрибут атаки.

Обычно укрупненная цепочка таких событий рассматривается как этапы атаки, если мы ее обнаружим и прервем, то чем раньше и тем меньше негативных последствий. Но чем короче цепочка тем более условным становится ее значение как признака – атрибута атаки. И если инцидент удалось предотвратить совокупность зафиксированных событий ИБ будет только косвенным признаком атаки – покушения на инцидент.

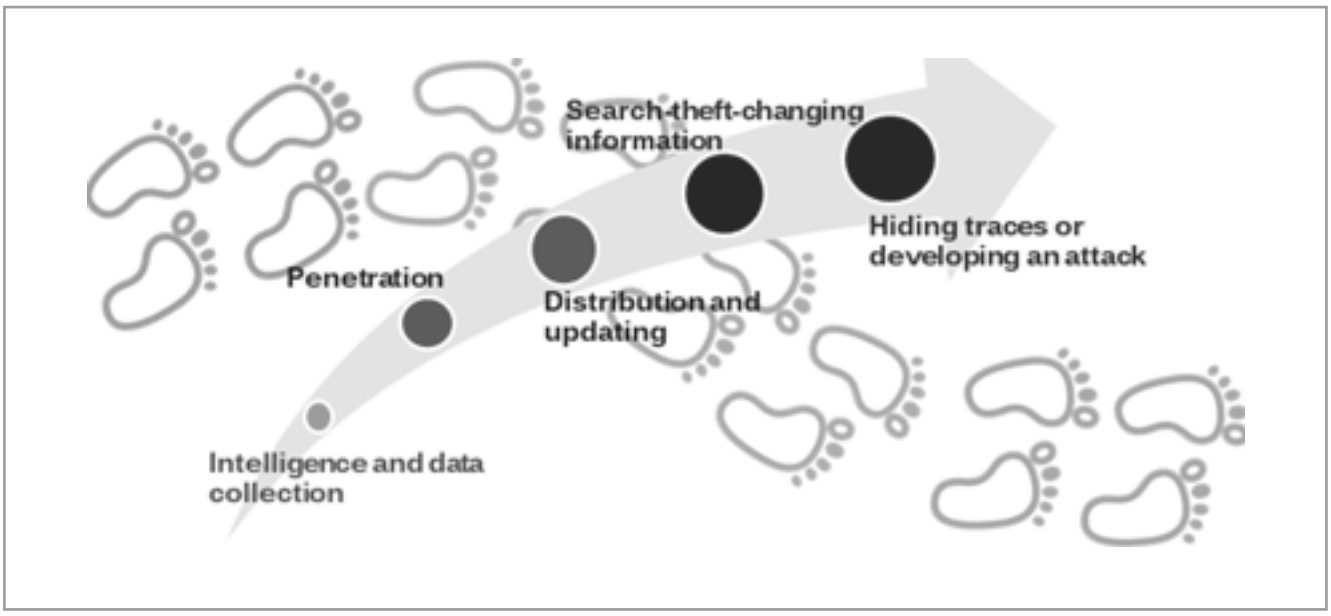
Как правило, на всех этапах злоумышленник оставляет следы, по которым его действия можно обнаружить.

Хотя здесь важно определить, что является атакой, например если разведку (1 этап) уже понимать как атаку, то таких «атак» может быть много, но негативные последствия они не несут и могут исходить не от злоумышленника.

Развернутое представление о цепочке событий безопасности дает матрица техник и тактик MITRE ATT&CK [5]. В верхней части матрицы MITRE расположено 14 категорий. Каждая категория это тактика, которую может использовать злоумышленник. Столбцы наборы возможных техник (и процедур) для реализации тактики. Сама матрица результат обобщения расследований множества компьютерных атак.

Тактики это этапы развития атаки, техники а точнее процедуры используемые для их реализации это события, которые нужно обнаружить. Сами события и их признаки это следы атаки.

Состав TTP: тактик, техник и процедур – может быть уточнен для различных областей применения. Использование матрицы MITRE



позволяет унифицировать подход к анализу угроз и расследованию инцидентов и позволяет использовать общие понятия.

Использование матрицы для атрибуции атак позволило описать преступный «почерк» и создать профили активности различных кибергруппировок. Однако матрица не абсолютная истина и ее развитие должно быть непрерывным.

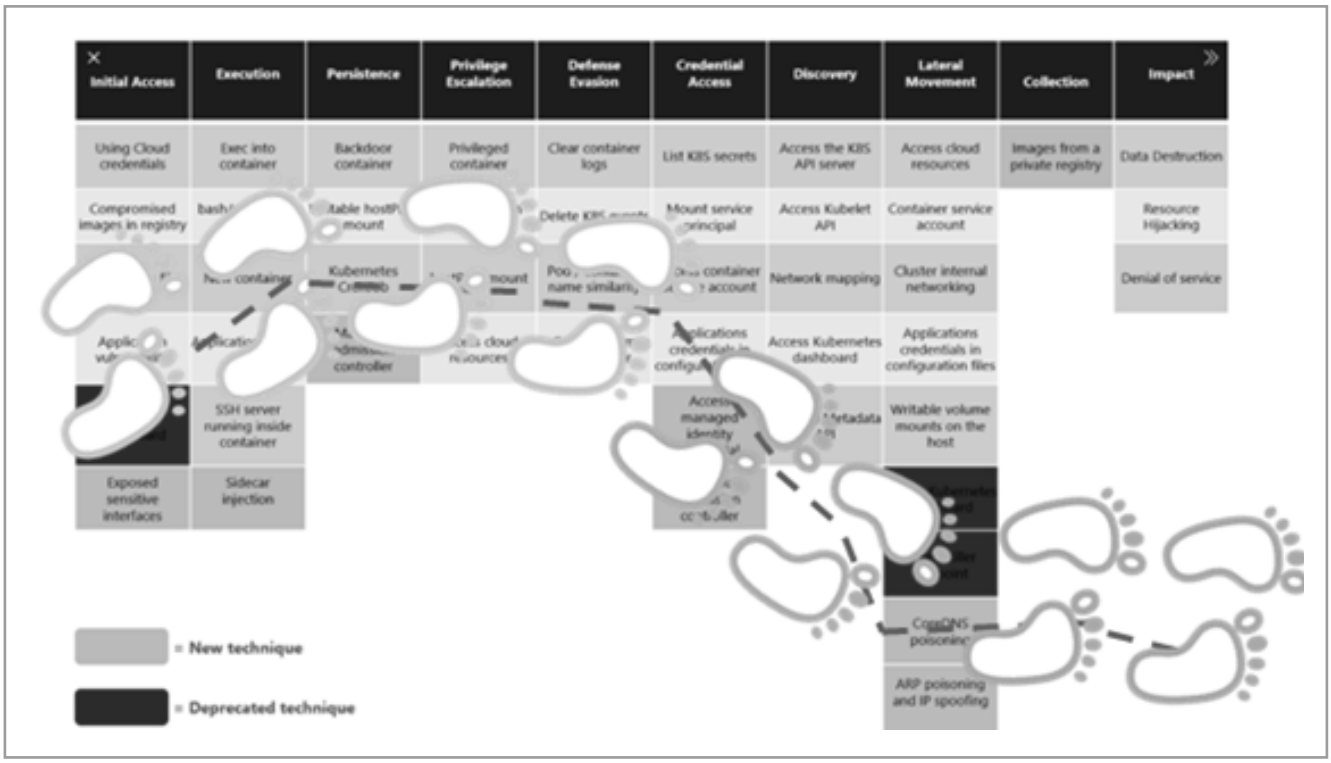
Здесь важно отметить, что по данным компании Cisco подозрительным является 1 событие из 5000, то есть 0.02% [6]. Задачу просмотра и фильтрации такого количества данных можно решить только за счет автоматизации – использования IDS и SIEM системы. Существует множество различных IDS систем и совмещенных с ними или отдельных SIEM систем – систем обработки событий безопасности.

Однако необходимо отметить, что направлены они на предупреждение атак и возможно развитие матрицы так позволяют выделять новые события безопасности. Атрибуция и главное фиксация (для доказательной базы) обнаруженных признаков уже не является их задачей, что может потребовать разработки специальных стандартов для таких средств.

Возвращаясь к теме цифровой криминалистики можно сделать вывод, что «выявлен и исследован новый криминалистический объект – «кибернетическое пространство», определяемый как среда совершения преступлений в сфере компьютерной информации и существования нового вида виртуальных следов». Но при этом: «…технико-криминалистическое и информационно-компьютерное обеспечение раскрытия, расследования и предупреждения этих преступлений находится в стадии разработки; не закончен процесс формирования криминалистических рекомендаций по тактике подготовки и производства отдельных следственных действий, связанных с обнаружением, фиксацией, изъятием и исследованием электронных следов и их материальных носителей»[7].

Но чтобы использовать признаки атак в судебном процессе они должны быть соответствующим образом зафиксированы как доказательства. И, как отмечают специалисты, этот процесс только начинается. А если необходимо, чтобы это признаки признавались как доказательства в международных организациях сама судебная экспертиза и средства обнаружения и фиксации должны быть прозрачны, понятны и соответствовать их стандартам. Это позволяет в дальнейшем исследованиях рассматривать:

- состав признанных судами, способов, методов и процедур по обнаружению, фиксации и обеспечению сохранности цифровых следов;
- возможность стандартизации средств фиксации признаков компьютерных



атак и их внедрение на объектах КИИ (например на объектах КИИ можно было бы предложить использовать специальные устройства такие как черный ящик у самолета);

- возможный состав косвенных признаков компьютерной атаки (цепочки событий безопасности) достаточный для проведения расследования состоявшегося или возможного инцидента.

Источники:

1. Семикаленова А. И. Цифровые следы: неожиданные проблемы исследования. Материалы международной научно-практической конференции. «Цифровой след как объект судебной экспертизы» материалы – Москва : РГ-Пресс, 2020. сс195-198.
2. Россинская Е.Р., Рядовский И.А. Концепция цифровых следов в криминалистике // Аубакировские чтения: материалы международной научно-практической конференции.. (19 февраля 2019 г.). Алматы, 2019. С.6–9.
3. Стало известно об атаках на системы онлайн-голосованияhttps://lenta.ru/news/2021/09/19/ddos/
4. Сервисы «Лаборатории Касперского» https://gossopka.kaspersky.ru/files/foto/1/se5fgllv1613555364.pdf
5. https://attack.mitre.org/
6. Современная ситуация по мониторингу информационной безопасности в России и Мире. https://www.securitylab.ru/blog/company/gamma/343956.php
7. Каминский А. М. Криминалистическая категория «след преступления» в анализе правонарушений в сфере компьютерной информации. Материалы международной научно-практической конференции. «Цифровой след как объект судебной экспертизы» материалы – Москва : РГ-Пресс, 2020. сс85-90.

А.С. Марков
Доктор технических наук, президент
АО «НПО «Эшелон», эксперт НАМИБ

АКТУАЛЬНЫЕ ВОПРОСЫ АТРИБУЦИИ КОМПЬЮТЕРНЫХ АТАК

Введение

Востребованность тематики атрибуции кибератак обусловлена субъективными и объективными факторами [1]. К первым следует отнести следующие:

- экспоненциальный рост атак и постоянный рост межгосударственных обвинений;
- новые факторы геополитики в сфере ИКТ (международное общественное мнение, атаки на интеллектуальную собственность и КИИ, военно-политическое прогнозирование и др.);
- атрибуция представляет собой условие существования ИКТ-отрасли как составная часть анализа угроз (Threat Intelligence), имеет техническое, юридическое и пр. значения [2, 3].

Можно предположить, что технологические и экономические возможности разных стран (например, участие в геополитических блоках, доступ к коммуникационным магистралям, доступ к международным облачным хранилищам и супервычислителям, развитие систем ИИ) создают в некоторой степени неравенство в области проведения атрибуции инцидентов в среде ИКТ. В докладе рассмотрено состояние тематики атрибуции компьютерных атак и возможные инициативы в области международной информационной безопасности.

Методологические основы атрибуции

Можно утверждать, что понятийный аппарат атрибуции находится на этапе становления. Под атрибуцией компьютерных атак обычно понимают комплекс процедур по выявлению источника атаки с целью возложения ответственности. Как известно, традиционно атрибуция включает в себя две составляющие [1, 4, 5]:

- техническую (криминалистическую), выполняющую функцию определения;
- политическую (правовую, дипломатическую), выполняющую предписывающую функцию.

Барьеры атрибуции касаются различных уровней систематизации (политический, правовой, нормативный, технический уровни) и подробно рассмотрены в литературе [2].

Кроме проблемных вопросов имеется активное противодействие проведению атрибуции кибератак, а именно:

- скрытие деятельности кибергруппировки и маскировка кибератаки (Operation Security);
- перенаправление атрибуции по ложным уликам (False Flag).

Таблица 1. Характеристики технической и политической атрибуции [2]

Тип	Функция	Достоверность	Базовые методы	Показатели, критерии
Техническая (криминалистическая)	Определения (детективная)	Высокая	Мониторинг контроль ресурсов и процессов	Количественные, качественные
Политическая (нормативная, дипломатическая)	Предписывающая	Низкая	Соблюдение норм анализ мотивации	Качественные (например, highly likely)

Рис. 1. Схема APT-атаки

В настоящее время известен ряд исследовательских проектов (DARPA, MITRE, ЕС), посвященных атрибуции, и ассоциации (attribution.news), посвященные информированию в данной области.

Объектом исследования являются, главным образом, целенаправленные атаки и APT-группы (мотивированные государством). Схема типовой кибероперации представлена ниже.

Предметом исследования являются методы атрибуции, а именно:

1. Методы моделирования процесса атрибуции и принятия решения;
2. Методы анализа признаков (выявление, оценка значимости признаков, оценка достоверности результата).

Целью первого класса методов атрибуции является правдоподобное возложение ответственности, как правило, путем проведения мозговой атаки или структурированного анализа [6] и принятия решения под углом дипломатических задач.

К основным задачам относят:

- сбор, анализ данных с целью получения идентификационных признаков;
- принятие решения о возложении ответственности;
- публикация выводов;
- постреакции.

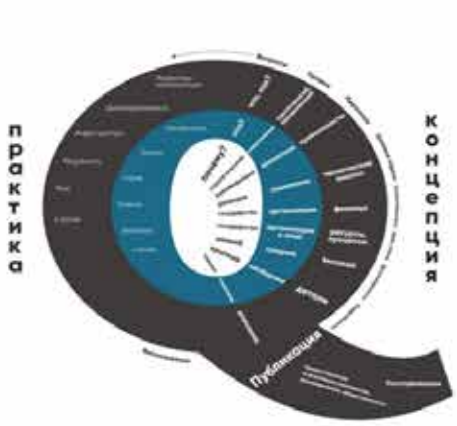
К известным концептуальным моделям данного класса относят: Q-модель, MICTIC-модель, конкурирующие гипотезы, Даймонд-модель и ее вариации, 4С – модель и пр.

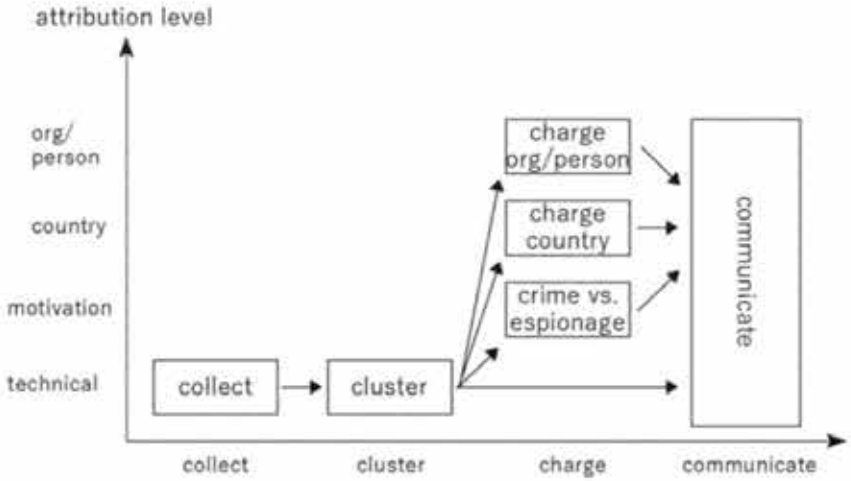
На рисунке 2 представлены схемы основных концептуальных моделей.

Представителем второго класса методов атрибуции является применение подхода учета кибератак MITRE ATT&CK, позволяющего систематизировать этапы, способы и реализации кибероперации, а, следовательно, и кибергруппировок. Данный подход на сегодня включает 14 целевых этапов (так называемых «тактик») кибероперации (рис. 3):

1. Разведка,
2. Использование ресурсов,
3. Первоначальный доступ,
4. Исполнение,
5. Настойчивость,
6. Повышение привилегий,
7. Уклонение от защиты,
8. Доступ к учетным данным,
9. Исследование сети,
10. Боковое движение,
11. Сбор данных,
12. Командование и контроль,
13. Извлечение данных,
14. Воздействие.

Надо понимать, что все представленные методы и модели отражают западные интересы, мы не видим здесь отчеты об атрибуции проамериканских или, скажем, произраильских кибергруппировок.





Evidence	Effort	H1	H2	H3	H4	H5	H6	H7
Arabian strings	Low	–	+	–	–	–	–	–
Hindi strings	Low	–	–	–	–	–	+	–
JoiterClient in PDB	Low	–	–	–	–	+	–	–
Spanish lang. rtn.	Low	–	–	+	–	–	–	–
C&C servers in SK	Med	o	o	o	+	o	o	o
code-sim RedOct	High	+	–	–	–	–	–	–
targets like RedOct	High	+	–	–	–	–	–	–
activity in UTC+2	High	+	–	–	–	–	–	–
	Score	2.7	–3.7	–3.7	–3.7	–3.7	–3.7	–4.3

	Aspect
M	Malware
I	Infrastructure
C	Control server
T	Telemetry
I	Intelligence
C	Cui bono

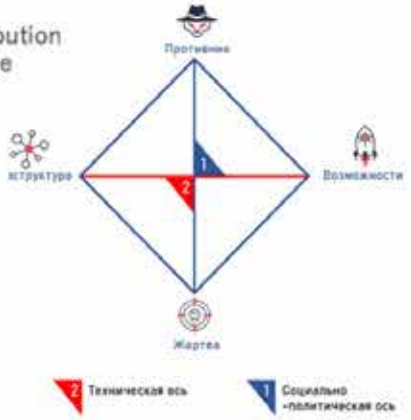


Рис. 2. Пример концептуальных моделей атрибуции

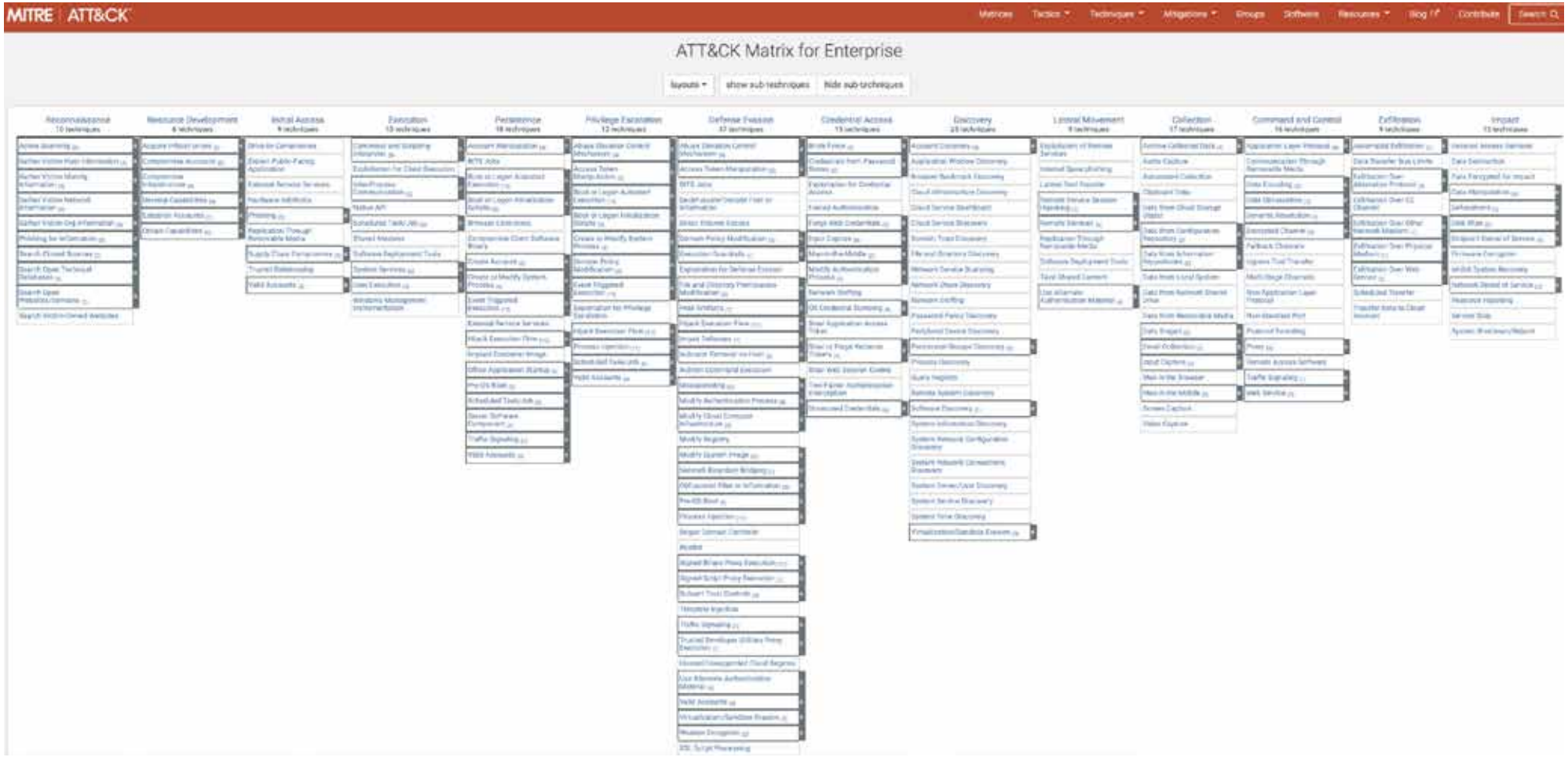


Рис. 3. Схема систематики MITRE ATT&CK

Следует отметить, что техническую атрибуцию можно обобщить путем использования многофакторного анализа, представленного в [2, 3]. Основными классами факторов здесь выступают следующие:

A. Особенности программных ресурсов (уязвимости, артефакты и пр.);
B. Особенности сетевой активности (IoC, сетевая инфраструктура);
C. Методические особенности атаки (поведенческие признаки);
D. Данные о субъектах атаки (мотивация группы, психология персонала);
E. Иная информация, полученная без использования собственно компьютерных сетей, например: техническая и агентурная разведка, аналитика по косвенным причинам, разного рода провокации и пр.

Преимущество данного подхода состоит в том, что данную концептуальную модель легко перевести к математическим (используя полиномы) для получения точных оценок.

Общие выводы

Можно констатировать ряд очевидных выводов, а именно:

1. Актуальность атрибуции кибератак возрастает в связи со смещением общественных отношений в сферу ИКТ.
2. Налицо барьеры как субъективного (политического), так и объективного (интернет, критическая сложность программ) характера.
3. В исследовании атрибуции наблюдается тенденция популизма позиции западных институтов. Свидетельством этого являются стандарты американского происхождения, исследовательские группы ЕС и США, американские группы информирования, прорывные технологии в сфере ИКТ и пр.
4. При всем этом остается актуальным вопрос о возможности регулирования международной информационной безопасности в целом и атрибуции в частности.

Можно назвать ряд общих предложений, которые могут обсуждаться в рамках дипломатических мероприятий (например, [1, 5, 7-10] и др.), как-то:

- выполнение соглашений группы правительственных экспертов ООН;
- осуществление взаимодействия между группами CERT различных стран;
- организация экспертного сообщества исследователей для совместной выработки решений на основе различных интересов и подходов;
- осуществление взаимодействия на политическом и техническом уровнях для расследования инцидентов;
- создание консультационных механизмов для повышения доверия;
- усиление защиты критически важной инфраструктуры;
- международное взаимодействие по обмену информацией об инцидентах, их характерных признаках и степени их угроз;
- соглашение о запрете кибератак на объекты критической информационной инфраструктуры и др.
- В организационно-техническом плане можно рекомендовать [2, 7, 11]:
- использование на узлах информационной инфраструктуры стран модулей, обеспечивающих механизмы подписи данных;
- подпись и децентрализованное хранение журналов;
- дополнение трафика специальной информацией, содержащей подпись наблюдателя;
- передача дополнительных подписанных сообщений о трафике;
- внесение неопределенности для злоумышленника (изменение конфигурации, использование сетевых ловушек, использование водяных знаков, раскрывающих злоумышленника);
- применение общей распространенной структуры систем обнаружения вторжений с общими актуальными международными базами правил;
- ведение реестра злоумышленников и пр.

Послесловие и неформальные инициативы

В завершение доклада можно предложить ряд инициатив по асимметричному подходу к проведению атрибуции антироссийских инцидентов в области ИКТ, например:

- создание портала для информирования по атрибуции кибергруппировок,

Рис. 4. Схема таксономии ФСТЭК России

которые направлены против ресурсов ИКТ (например, объектов КИИ) на территории России;

- ведение базы данных для учета антироссийских кибероперациий и используемых вредоносных средств, что могло бы способствовать, например, проведению киберучений (CTF-соревнований) по защите КИИ РФ и дружественных стран;
- создание отечественной методической базы атрибуции.

Что касается последнего, то в основе построения такой информационной платформы может выступить методика моделирования угроз ФСТЭК России 2021 года. Как известно, методика ФСТЭК России включает в себя 10 целевых этапов (названных авторами документа «тактиками») APT-атаки, а именно:

- Т1. Сбор информации о системах и сетях;
- Т2. Получение первоначального доступа к компонентам систем и сетей;
- Т3. Внедрение и вредоносного исполнение программного обеспечения в системах и сетях;
- Т4. Закрепление (сохранение доступа) в системе или сети;
- Т5. Управление вредоносным программным обеспечением и (или) компонентами, к которым ранее был получен доступ;
- Т6. Повышение привилегий по доступу к компонентам систем и сетей;
- Т7. Сокрытие действий и применяемых при этом средств от обнаружения;
- Т8. Получение доступа (распространение доступа) к другим компонентам систем и сетей или смежным системам и сетям;
- Т.9 Сбор и вывод из системы или сети информации, необходимой для дальнейших действий при реализации угроз безопасности информации или реализации новых угроз;
- Т10. Несанкционированный доступ и (или) воздействие.

Названные целевые этапы включают 145 способов несанкционированного воздействия на ресурсы компьютерных систем (названные авторами «техниками») (см. рис. 4).

Пример матрицы возможного соответствия («маппинга») методики ФСТЭК России и методического аппарата MITRE ATT&CK представлен на учебном тестовом веб-портале apt.etecs.ru, и может быть взят на основу при построении масштабного обучающего портала, посвященного атрибуции кибератак, имеющих антироссийский характер (российскими исследователями публично зафиксировано, что действия кибергруппировок нанесли ущерб ресурсам на территории России и ее союзников). Пример неофициального фрагмента матрицы соответствия представлен в таблице ниже.

Таблица 2. Фрагмент соотношения способов кибервторжения

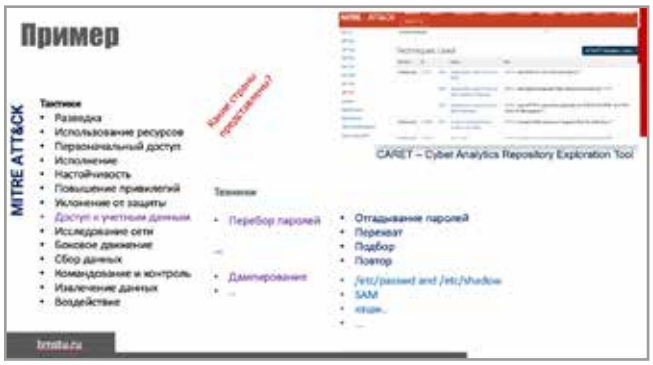
ID	MITRE ATT@CK
T4.1. Несанкционированное создание учетных записей	T1136, T1212
T4.2. Использование штатных средств удаленного доступа ОС	T1133, T1021
T4.3. Скрытая установка и запуск средств удаленного доступа ОС	T1133, T1021, T1219
T4.4. Маскирование подключенных устройств под легитимные	близко к T1036
T4.5. Внесение соответствующих записей в компоненты автозапуска	T1542, T1053, T1547, T1037
T4.6. Компрометация прошивок устройств	T1542.001, T1495
T4.7. Резервное копирование вредоносного кода в скрытые области	отсутствует

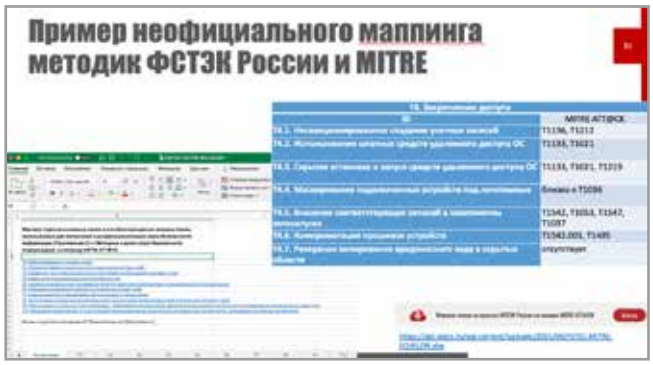
Следует повторить, что подобный учебный портал, но позволит формировать контрмеры (в том числе организовывать киберучения) для защиты, например, объектов КИИ РФ. Думается, портал будет иметь соответствующее значение для информирования и осознания (awareness) ИКТ-угроз в области международной информационной безопасности (что, напомним, является основным принципом менеджмента информационной безопасности по линии международных стандартов ISO/IEC 27xxx).

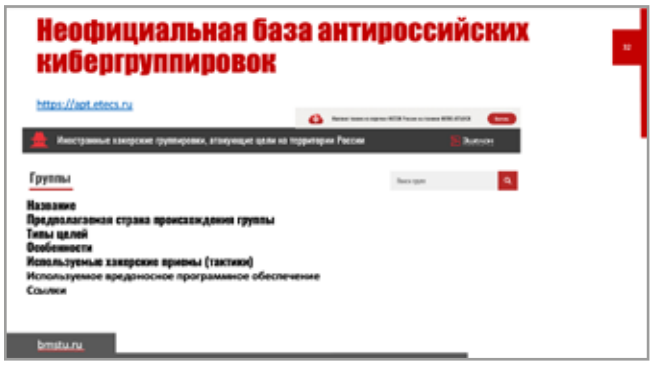
Литература

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. Марков А.С. Проблемы атрибуции и регулирования международной информационной безопасности. Сб. докл. XIV Международного форума «Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности», М.: НАМИБ, 2020. С. 88-93.
3. Ромашкина Н.П., Марков А.С., Стефанович Д.В. Международная безопасность, стратегическая стабильность и информационные технологии. М.: ИМЭМО РАН, 2020. 98с. DOI: 10.20542/978-5-9535-0581-9.
4. Комов С.А. О подходе Минобороны России к атрибуции государств, виновных в нарушении норм ответственного поведения в информационной сфере. Сб. докл. XIV Международного форума «Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности», М.: НАМИБ, 2020. С. 127-129.
5. 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.
6. Дорофеев А.В., Марков А.С. Структурированный мониторинг открытых персональных данных в сети интернет // Мониторинг правоприменения. 2016. № 1 (18). С. 41-53.

7. Марков А.С. Вопросы технического регулирования безопасности программных систем. Сб. докл. XIII Международного форума «Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности», НАМИБ, 2019 г. - С. 167-168.
8. Пилюгин П.Л. Зона ответственности государств в информационном пространстве. Сб. докл. XIV Международного форума «Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности», М.: НАМИБ, 2020. С. 127-129.
9. Ромашкина Н.П. Глобальные военно-политические проблемы международной информационной безопасности: тенденции, угрозы, перспективы // Вопросы кибербезопасности. - 2019. - No. 1 (29). - С. 2-9.
10. Стрельцов А. А. Суверенитет и юрисдикция государства в среде информационно-коммуникационных технологий в контексте международной безопасности // Международная жизнь. - 2017. - No. 2. - С. 87-106.
11. Markov A.S., Sheremet I.A. Enhancement of Confidence in Software in the Context of International Security // CEUR Workshop Proceedings. - 2019. - Vol. 2603. - P.88-92.







О.А. Мельникова
К.полит.н., начальник отдела
Департамента МИБ МИД России

КИБЕРДОВЕРИЕ В МИРЕ И ОПЫТ СОТРУДНИЧЕСТВА В ЕВРОПЕ

Уважаемые участники конференции, коллеги!

Прежде всего хочу поблагодарить организаторов XV международного форума «Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности» за приглашение принять участие в содержательных дискуссиях и поприветствовать всех, кто собрался в этом зале и тех, кто подключился онлайн.

Стремительное развитие и широкое внедрение в повседневную жизнь информационно-коммуникационных технологий (ИКТ) способствовало стиранию границ между государствами в информационном пространстве, созданию беспрецедентных практических возможностей, но также и появлению серьезных вызовов и угроз.

Возросли угрозы нарушения нормального функционирования информационных и телекоммуникационных систем, сохранности информационных ресурсов и несанкционированного доступа к ним. Возросло количество злонамеренных действий и хакерских атак на объекты критической информационной инфраструктуры государств[1], а также иных мошеннических и противоправных действий с использованием ИКТ.

В условиях формирования глобального информационного пространства информация и ИКТ все более активно стали использоваться как орудие в достижении превосходства.

Вредоносное использование ИКТ, направленное на подрыв суверенитета, нарушение территориальной целостности, безопасности и стратегической стабильности, правам человека и свободе выражения мнения становится основной угрозой современного мира.

Усиливаются попытки политизировать сферу использования ИКТ.

Проявилось новое лицо политической конфронтации, когда кибератаки и киберконфликты между крупными государствами превращаются в элемент политической реальности.

В современных условиях сохранение информационного (или цифрового) суверенитета становится не только основой развития, но и важным фактором существования самого государства.

Информационный суверенитет – это право каждого государства самостоятельно формировать информационную политику, распоряжаться информационными потоками, обеспечивать информационную безопасность независимо от внешнего влияния. Это означает, что каждая страна может самостоятельно определять параметры регулирования собственного информационного пространства и соответствующей инфраструктуры.

Однако, достижение цифрового суверенитета понимается многими государствами по-разному.

Информационный суверенитет включает в себя любые компоненты, связанные с информационной сферой государства, которые

1 В соответствии с Федеральным законом от 26 июля 2017 года №187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» к ним могут быть отнесены информационные системы и сети, а также автоматизированные системы управления, функционирующие в сфере: здравоохранения, науки, транспорта, связи, энергетики, банковской и иных сферах финансового рынка, топливно-энергетического комплекса, атомной энергии, оборонной и ракетно-космической промышленности, горнодобывающей, металлургической и химической промышленности.

можно разделить на два аспекта: *технический* (национальное программное обеспечение, собственные социальные сети, поисковики, национальная электронная платёжная система и т. д.) и *идеологический*, который подразумевает наличие официальной идеологии или национальной идеи, высокого уровня популярной массовой культуры, а также усовершенствованного законодательства в области информации.

Тема цифрового суверенитета неразрывно связана с темой международной информационной безопасности (МИБ). А МИБ в свою очередь не может быть обеспечена без решения вопросов атрибуции, т.е. установления виновного в незаконной кибератаке и, соответственно, ответственности за совершение кибернападений и за осуществление любой дугой незаконной и вредоносной деятельности в киберпространстве.

Цифровое пространство стало рассматриваться как сфера противоборства.

Киберпространство и Интернет-пространство – практически тождественны. По существу, все вредоносные события осуществляются с использованием сети Интернет. Отсюда вытекает один логический вывод – нужно не только обеспечить деанонимизацию работы Интернет, но и интернационализацию управления этой сетью. Как мне представляется, это и может стать путем для решения проблемы атрибуции.

В настоящее время Интернет бросает вызов суверенитету.

По оценкам экспертов, число подключенных к глобальному интернету электронных приборов в текущем году может превысить 25 млрд. единиц. А количество пользователей Всемирной сети составляет более половины населения мира в 150 странах.

Использование глобальной сети Интернет, связавшей все страны мира в единое целое, не только открывает широкие возможности для общения и получения информации, не только несет удобства и блага, но и способно нанести серьезный вред пользователям.

Интернет превращается в главную платформу для распространения различного рода политических манипуляций, опасного и вредоносного контента, фишинговых программ, запрещенной и экстремистской информации, различных вирусов, т.е. становится, по существу, супероружием XXI века, использование которого ни одной из стран и ООН не квалифицируется как акт вооруженного нападения. А соответственно, говоря юридически, не может быть приведена в действие статьи 51 Устава ООН о праве государств на самооборону в условиях вооруженного нападения.

Рыночные принципы функционирования сети Интернет порождают ситуацию, при которой глобальное информационное пространство может трансформироваться во вредоносную для пользователей среду.

Используют все более совершенные инструменты информационного и психологического воздействия на пользователей.

Ложная или искаженная информация, вредоносный контент и манипуляции используются ими в качестве инструментов и методов воздействия на отдельные социальные группы, прежде всего на молодежную аудиторию, а также в целях координации протестных выступлений и, в конечном счете, дестабилизации целых обществ.

Далеко не все государства имеют достаточные ресурсы для адекватного противодействия таким вызовам.

Вместе с тем регулирование этой сферы является законным и неотъемлемым суверенным правом каждого государства по защите своего информационного пространства, интересов человека и общества, а также обеспечение их безопасности.

Меры правового регулирования, которые уже приняты в России и предлагаются к принятию, ничуть не жестче, чем в других странах и дальнейшая работа в этом направлении должна создать условия, при которых надежно защищены права граждан, общества и государства в информационной сфере.

Среди новых глобальных вызовов и угроз – намерение отдельных государств милитаризировать Интернет, развязать гонку кибервооружений. На это указал Министр иностранных дел С.В.Лавров, выступая в ходе общеполитической дискуссии на 76-й сессии Генеральной Ассамблеи ООН, Нью-Йорк, 25 сентября 2021 года.

Россия последовательно выступает за интернационализацию управления Интернетом, повышение роли государств в этом процессе.

Считаем, что все страны должны равноправно участвовать в процессе управления

Интернетом, адаптации на основе норм международного права условий для безопасной и устойчивой работы глобальной Сети и сохранения суверенного права государств регулировать национальный сегмент Интернета.

Только в условиях реально демократической интернационализации управления Интернетом при доступе к этому процессу всех заинтересованных государств можно гарантировать, что атрибуция применительно к МИБ будет реально объективной и будет восприниматься всем международным сообществом с полным доверием. Без чего она будет просто фейком и станет инструментом политических интриг.

Россия предлагает согласование на площадке ООН путей обеспечения международной информационной безопасности.

В рамках системы ООН Россия последовательно настаивает на принятии целого ряда скоординированных мер, таких как повышение роли государств в процессе управления Интернетом, разработка на межгосударственном уровне глобальной политики в сфере управления Интернетом, обеспечение на основе норм международного права его стабильного и безопасного функционирования, сохранение суверенного права государств регулировать национальный сегмент Интернета.

Следует рассматривать этот и иные вопросы только на основе универсальных договоренностей, транспарентно и с опорой на достоверные факты. На это же нацелены российские инициативы о выработке единых норм ответственного поведения государств в сфере использования ИКТ и о подготовке универсальной конвенции ООН по борьбе с киберпреступностью.

Механизмы для реализации этих предложенной Россией инициатив уже созданы и запущены. Это новая Рабочая группа ООН открытого состава по вопросам безопасности в сфере использования ИКТ и самых ИКТ (РГОС) на 5-летний срок, первая субстантивная сессия которая начнет работу в декабре 2021 г. в Нью-Йорке и спецкомитет ООН по выработке универсальной конвенции ООН по борьбе с киберпреступностью, который должен приступить к работе в январе 2022 г.

Благодарю за внимание!

В.Е. Хрычев
Международный центр научной и технической информации (МЦНТИ), Эксперт, к.т.н., РМР

ПРОБЛЕМЫ ОПРЕДЕЛЕНИЯ ПУБЛИЧНОЙ АРГУМЕНТИРОВАННОЙ БАЗЫ АТРИБУЦИИ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Вот уже более 2-х десятков лет проблема объективной атрибуции инцидентов международной информационной безопасности не только не потеряла своей актуальности, но носит еще более острый характер.

Российская Федерация всегда выступала в качестве инициатора, с момента внесения в 1998 году проекта резолюции безопасности ИКТ, затем в 2004 году инициировала группу правительственных экспертов, заложившую принципиальные нормы поведения государств в кибер среде, далее в 2018 году по инициативе РФ создана группа открытого состава.

Последовательным продвижением инициатив РФ явился «Проект универсальной международной конвенции по противодействию использования ИКТ в преступных целях», внесенный РФ в ООН 27 июля 2021 года.

Однако, необходимо заметить, проблема обеспечения международной информационной безопасности расширилась до акторов государственно-частных партнёрств (ГЧП).

Соответственно расширился круг вопросов относительно атрибуции кибероперациий проводимых ГЧП и какие роли, а также ответственность будет возложена на каждую из сторон в процессе атрибуции, что также повлияет на сложившиеся международные отношения, в особенности относительно сознательно фабрикуемых обвинений в целях очернения имиджа государств, а также применения деструктивных контрмер.

При этом важность объективной атрибуции возрастает до инструмента определения фокуса глобальной политики.

Кибератаки на критическую информационную инфраструктуру могут быть не менее деструктивными, чем ядерное и другие виды оружия массового уничтожения. Цифровое пространство, по сути, становится ареной гибридной войны[1].

Особую опасность носит смещение акцента от кибершпионажа к атакам на критически важную инфраструктуру.

Как следствие возрастает ценность и острая необходимость публичной атрибуции как раскрытие стратегической, технической и оперативной информации для подтверждения/опровержения утверждений об участии государства или ГЧП в инциденте международной информационной безопасности.

Политические, технические и правовые аспекты публичной атрибуции требуют гармонизации национального и международного законодательств.

Ошибки в определении аргументированной базы и инструментов атрибуции приведут к необоснованным экономическим санкциям, уголовным обвинениям, деструктивным дипломатическим, военным или разведывательным действиям.

Особую роль в избежание данных ошибок будет носить открытый процесс в определении аргументированной базы атрибуции и, как следствие, – обмен информацией между всеми заинтересованными сторонами.

Принимая участие в международном процессе атрибуции инцидентов международной безопасности, участвуя во всех продуктивных

1 «Цифровой суверенитет оказался важен в условиях новой идеологической конфронтации» А. В. Яковенко https://www.ng.ru/vision/2021-08-01/8_8213_confrontation.html (дата обращения 23.09.2021)

институтах международной информационной безопасности, необходимо также развивать собственные инструменты в ответ принимаемых инициатив стран НАТО, таких, как создание «Транснационального института атрибуции», создание банка данных CFR Cyber Operations Tracker – Система отслеживания кибероперацийDigital and Cyberspace Policy представляет собой базу данных об общеизвестных инцидентах, произошедших с 2005 года при финансовой поддержке государств.

Трекер содержит данные в которых субъект угрозы предположительно связан с государством.

Цель трекера – определить, когда государства, либо их доверенные лица, проводят кибероперации, преследуя свои внешнеполитические интересы.

Все данные трекера опираются на открытый исходный код, который собирается из существующих репозиториев инцидентов, таких как:

- таблица APT-групп (advanced persistent threats)
- список значимых кибер-событий Центра стратегических и международных исследований
- среди отечественных источников информации необходимо выделить Лабораторию Касперского.

Данные дополняются инцидентами из средств массовой информации.

Трекер также пытается определить, какие субъекты угроз несут ответственность за конкретный инцидент.

Возможность ассоциировать инцидент является предметом давних дискуссий в сообществе кибербезопасности. Известно, что злоумышленники намеренно внедряют «ложные сигналы» в код, чтобы скрыть атрибуцию и свои следы.

Однако абсолютно недостаточно, как это реализовано в трекере, идентифицировать злоумышленника только за счет сочетания технических данных, информации из открытых источников и понимания внешнеполитических приоритетов.

Данный политизированный субъективный подход привел к тому, что по информации банка данных Россия, Китай, Иран и Северная Корея были обвинены в 75% всех поддерживаемых государством кибер инцидентов.

Субъективность данного подхода также связана с принадлежностью банка данных коалиции Five Eyes – альянсу по обмену разведданными, состоящий из США, Великобритании, Австралии, Канады и Новой Зеландии.

Сообщество поддерживает атрибуцию союзников для неоправданного обвинения РФ в кибер инцидентах.

Кроме того, с должной осмотрительностью, необходимо привлекать к атрибуции ГЧП, в этом случае к политической субъективности союзников коалиций, добавиться разнообразный набор угроз, включая, извлечение сверхприбыли, самореклама, использование отчетов атрибуции для продвижения собственных продуктов.

Однако, именно бизнес, неся существенный экономический урон от преступных действий в киберпространстве, наиболее заинтересован в действенной легитимной атрибуции.

При этом, важно не только создать условия для привлечения бизнеса к диалогу, но и придать ГЧП институциональный характер[2].

При этом основными факторами аргументированной атрибуции являются.

Точность – однозначно идентифицировать злоумышленника. Необъективная атрибуция приведет к ложной информации, что в свою очередь приведет к международной неразберихе.

Открытость – использование надежных источников идентификации и распространения для гарантии общественного признания и легитимности.

Гармонизация международного и национальных законодательств – отсутствие общепризнанных стандартов и норм приведет к политизированности и субъективности атрибуции.

Атрибуция, полученная в результате легитимного процесса, имеет большее доверие, ведет к изучению тактики и методологий, создает угрозу возмездия, позволяет применять контрмеры и устанавливать нормы этичного поведения.

Для последовательного продвижения лидирующих инициатив РФ в области меж-

2 «Глобальная киберповестка: дипломатическая победа» А.В. Крутских https://namib.online/2021/06/globalnaja-kiberpovestka-diplomaticheskaja-pobeda/ (дата обращения 23.09.2021).

дународной информационной безопасности и в частности в такой важнейшей сфере как атрибуция, необходимо и далее опираться на международные институты с участием РФ, а также создавать и развивать собственные инструменты атрибуции, продвигать открытый обмен информации, максимально вовлекая наших ближайших партнеров в совместные банки данных атрибуции, включая техническую информацию об инцидентах.

МЦНТИ – международный институт, поддерживающий деятельность в глобальном информационном пространстве, в том числе в целях предотвращения угроз международной информационной безопасности.

Обеспечивая доступность информационно-коммуникационных технологий странам участникам, способствует преодолению «цифрового разрыва» путем наращивания их потенциала в вопросах передовой практики и профессиональной подготовки.

Способствует оперативному обмену информацией о признаках, фактах, методах и средствах использования информационного пространства в преступных целях, в том числе с помощью компьютерных атак, а также взаимному информированию о правовом регулировании и организации деятельности по борьбе с этими противоправными деяниями, о накопленном опыте и практике деятельности в данной сфере.

Список литературы:

1. «Цифровой суверенитет оказался важен в условиях новой идеологической конфронтации» А. В. Яковенко https://www.ng.ru/vision/2021-08-01/8_8213_confrontation.html (дата обращения 23.09.2021).
2. «Глобальная киберповестка: дипломатическая победа» А.В. Крутских https://namib.online/2021/06/globalnaja-kiberpovestka-diplomaticheskaja-pobeda/ (дата обращения 23.09.2021).

П.У. Кузнецов
Заведующий кафедрой информационного права Уральского государственного юридического университета, д.ю.н., профессор

ПОЗИТИВНЫЕ ОБЯЗЫВАНИЯ КАК ПРАВОВОЙ МЕТОДОЛОГИЧЕСКИЙ ИНСТРУМЕНТ ОГРАНИЧЕНИЯ СВОБОДЫ В ИНТЕРНЕТ-ПРОСТРАНСТВЕ

Современное состояние международного права в части решения киберпроблем развития общества, по мнению многих ученых и специалистов в области информационной безопасности, не дает возможность реально предотвращать нанесение ущерба информационным правам и интересам человека и гражданина, а также законным интересам организаций в области информационной деятельности. С этим отчасти можно согласиться.

Действительно, ИКТ-инфраструктура существенно изменила среду жизни и деятельности человека до известных пределов, в рамках которых определение характера такой деятельности весьма затруднительно с точки зрения идентификации и фиксирования самих действий, а также их квалификации с помощью традиционных правовых средств.

Следует заметить, что право обладает своим собственным инструментальным арсеналом воздействия на объекты жизнедеятельности. Он во многом носит строгую форму (нормы права, закон и др.), которая приобретает таковую с помощью традиционного правового языка. Причем, особенности такого языка и формы права имеют историческую предопределенность, начиная со времен Древнего Рима. Но это вовсе не означает, что традиции и формы права являются строго установленными раз и навсегда. Об этом свидетельствует и византийский этап развития права (Кодекс Юстиниана), и его реформы нового времени (Кодекс Наполеона), и современный период (Гражданский кодекс РФ).

Несмотря на традиционность и догматичность формы права, все же его содержание проявляется в зависимости от складывающегося характера жизненных ситуаций. По своей природе право имеет инстинктивный характер, то есть реагирует на самые актуальные «запросы» общества. Такая реакция может не сразу наступить, она зависит от множества обстоятельств, но потенциальные возможности, заложенные в арсенале правовых средств, довольно значительны. Концептуальные позиции известного правоведа современности С.С.Алексеева, изложенные им в своих работах по теории права свидетельствуют о таких возможностях.

Начальным этапом траектории воздействия права на жизненные ситуации является возникновение острой необходимости принятия правовых решений в связи с такой ситуацией. Завершающим этапом – само принятие правового решения. Но этому предшествует выбор конкретного правового средства (или их совокупности), с помощью которого устанавливается правовой режим конкретной ситуации. Арсенал таких средств достаточно широкий. Это, прежде всего, ***запреты*** и ***дозволения, стимулы и ограничения,*** а также ***позитивные обязывания.*** Все они составляют состав «правовой материи», выбор которых используется при принятии окончательного правового решения и которые составляют его смысл и содержание: «разрешить», «запретить», «наказать» и т.д. По этой «схеме» развиваются энергия и сила закона, но в их основе в качестве оснований всегда существуют конкретные правовые средства: позитивные обязывания, запреты или дозволения; стимулы или ограничения.

Думается, что при установлении правовых режимов киберпространства на международном уровне могут применяться такие правовые средства, особенно позитивное обязывание, под которым в международном договоре возможно предусматривать обременения для субъектов международных отношений.

В связи с этим в тексте предлагаемой для обсуждения Концепции Конвенции ООН об обеспечении международной информационной безопасности раздел «Основные принципы обеспечения международной информационной безопасности» дополнить ***принципом «обременения»,*** сформулировав его следующим образом: «Обременение деятельности субъектов международных отношений с целью ограничения распространения информации в сети Интернет в интересах защиты прав и свобод других, а также удовлетворения справедливых требований морали, общественного порядка в демократическом обществе».

На основании названного принципа у стран-участников Конвенции возникает суверенное право выбора средств обеспечения собственной информационной безопасности в соответствии с международным правом.

Кроме того, пункт 4 раздела «Предотвращение конфликтов в информационном пространстве» Концепции Конвенции ООН об обеспечении международной информационной безопасности сформулировать следующим образом: «Обязывание противодействия любым действиям, угрожающим безопасности информационного пространства другого государства. На основании такого обязывания (обременения) у «другого государства» возникает возможность потребовать от субъектов информационной деятельности (в т.ч. монополий сетевого пространства) совершения активных действий, направленных на ограничение распространения противоправного информационного контента.

Строго говоря, в текстах международных документов следовало бы более активно и гибко использовать арсенал правовых средств – не только дозволения и запреты, но и стимулы и обязывания (обременения).

Например, в таких текстах устанавливать для отдельных субъектов (владельцев крупных информационных платформ в сети Интернет, владельцев крупных поисковых систем Интернет-компаний, мультисоциальных сетей Фэйсбук, Инстаграмм, ВКонтакте и др.) обременения в части обязывания осуществлять мониторинг и самостоятельно ограничивать распространение запрещенного контента вне зависимости от того, где размещен источник такого распространения, Причем такие обязывания должны носить безусловный характер (как тяжелые «гири», которые невозможно самостоятельно «сбросить»). Кроме того, в текстах международных договоров предусматривать ответственность для таких субъектов в случаях уклонения от выполнения названных обязываний (обременений). С другой стороны, в целях заинтересованности выполнения названных обременений для таких субъектов международных отношений активно использовать такое правовое средство, как стимулы. Учитывая экономические интересы бизнес-структур в сетевом пространстве, такие стимулы могут быть намного эффективнее запретов. Их отдельно можно продумать и согласовывать с крупными субъектами сетевой деятельности.

Названные гибкие правовые средства, конечно, должны включать в состав систем регулирующего воздействия и технологические средства, связывая тем самым правовые и цифровые средства в единую систему воздействия.

Как мы уже подчеркивали ранее, фиксирование таких обязываний в юридически значимых документах (международных договорах), дополненных техническими регламентами контроля за выполнением обязательных действий ключевых субъектов международных информационных отношений может стать эффективным средством правопорядка в киберпространстве. В том числе таких, которые системно определяют мировой информационный климат. Названное правовое средство в комплексе с технологическими инструментами можно использовать в правилах ответственного поведения в качестве предупреждающего злонамеренные действия субъектов распространения информации, несущей запрещенный или нежелательный контент.

Следует отметить, что действующие правила и принципы международного права

Ст. 29 Всеобщей декларации прав человека 1948 г. допускает ограничения прав и свобод с целью обеспечения уважения прав

и свобод других и удовлетворения справедливых требований морали, общественного порядка в демократическом обществе.

Кроме того, статья 30 этого же документа вводит «мягкий» запрет заниматься какой-либо деятельностью или совершать действия, направленные на уничтожение прав и свобод, изложенных в Декларации.

Следовательно, в интересах обеспечения уважения прав и свобод других, а также общественного порядка в обществе вполне допустимо вводить механизмы (обязывания и обременения) для ИТ-компаний и правила их ответственного поведения в киберпространстве, направленные на укрепление доверия и правопорядка в сети Интернет.

КРУГЛЫЙ СТОЛ № 2
ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

Модератор:
Григорьев Д.И., Директор департамента защиты информации и IT-инфраструктуры ПАО «ГМК «Норильский Никель», член Президиума НАМИБ

Э.Г. Островский
Вице-Президент группы компаний «Цитадель»

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

В современном мире наблюдается активный рост кибератак на объекты критической информационной инфраструктуры. Это связано с тем, что эти объекты играют значительную роль в экономике любой страны. Преступники используют кибератаки в качестве инструмента для экономического и политического влияния. Ущерб экономике страны, наносимый в результате кибератак на объекты критической информационной инфраструктуры исчисляется сотнями миллионов.

Сегодня с полной уверенностью можно сказать, что для осуществления кибератак злоумышленниками используется новый вид оружия – кибероружие.

Эксперты в области киберпреступности выделяют 3 типа кибероружия:

1. Низкий потенциальный конец спектра – это вредоносная программа, способная воздействовать на информационные системы извне, но не способна проникнуть в цель или создать прямой вред. К этой категории относятся инструменты и программное обеспечение для генерации мощного трафика с целью критической нагрузки информационной системы. В результате этого происходит отключение системы и требуется ее перезагрузка. Такие воздействия наносят ущерб только с временным эффектом.
2. Средний потенциальный конец спектра – это вредоносное вторжение, которое мы можем идентифицировать, но которое не может влиять на конечную цель. Оно может создать функциональный и физический ущерб. В эту категорию входит общий агент вторжения, такой как вредоносное ПО, способное быстро распространяться.
3. Высокий потенциальный конец спектра – это агент способный проникать в цель, избегая любой защиты, и создающий прямой вред жертве. Это сложная вредоносная программа, которая может нанести вред конкретной системе.

Целью самого опасного вида кибероружия является не моментальное действие, а получение «точки присутствия», то есть возможность поставить под контроль преступников управление отдельными технологическими узлами или целыми системами, находящимися на объекте критической информационной инфраструктуры.

Одним из самых опасных способов скрытного проникновения в информационные системы является возможность эксплуатации критических уязвимостей исходного кода или компонентов ПО, позволяющих обойти средства защиты информации.

Для этого преступниками разрабатывается интеллектуальный программный инструментарий. Его задача – получение скрытого доступа к критическим элементам системы управления для организации внезапных кибератак в нужный момент времени с помощью произвольных команд.

В большинстве случаев объекты КИИ не являются полностью изолированными от глобальной информационно- телекоммуникационной сети. Они имеют в своем составе большое количество информационных систем, подключенных к Интернет. Поэтому использование так называемых «защитных периметров», изолирующих атакуемые объекты от проникновения извне, не всегда решают про-

блему (например, в России доля внешних атак лишь немногим превышает 20%, остальные атаки имеют внутренний характер).

Необходимо отметить, что в основе механизма внутренних атак находится целенаправленная эксплуатация уязвимостей исходного кода программного обеспечения, используемого на объектах КИИ. После «условно дружественного» проникновения в локальную сеть защищаемого объекта хакеры исследуют информационную инфраструктуру, находят уязвимости в исходном коде ПО или его программных компонентах. Загружают на скомпрометированные узлы вредоносные программы и удаленно используют их. Во всех случаях атак зафиксирован схожий сценарий.

Появление уязвимостей и снижение уровня безопасности любого ПОЛ (неважно, состоит ли оно из заимствованных библиотек или имеет отечественное происхождение) вызвано естественным характером произвольного ухудшения качества любого ПО в процессе его эксплуатации.

Именно это, зачастую, и приводит к катастрофам на объектах КИИ.

Чтобы противодействовать новому виду кибероружия необходимо создавать такие механизмы, которые позволяют поддерживать уровень безопасности программного обеспечения на протяжении всего его жизненного цикла, начиная от разработки ПО и заканчивая его утилизацией.

В настоящее время известными крупными IT-компаниями разрабатываются и внедряются системы автоматизированного непрерывного комплексного контроля состояния безопасности эксплуатируемого программного обеспечения на предмет выявления уязвимостей. Целесообразно было бы рассмотреть возможность обмена опытом между странами по внедрению передовых практик и технологий для обеспечения безопасности объектов критической информационной инфраструктуры.

Необходимо развивать инструментарий тестирования ПО, способный выявлять уязвимости ПО при всем многообразии языков программирования, которое мы сегодня имеем. В этих целях, возможно, следует создать специальный международный фонд для финансирования разработок в этом направлении и сделать такой инструментарий доступным на межгосударственном уровне.

Считаем важными мероприятия по созданию и наполнению баз данных или, так называемых, реестров уязвимостей исходного кода и программных компонентов. Во многих странах создаются или уже существуют реестры уязвимостей исходного кода ПО. Некоторые реестры имеют свободный доступ к своим ресурсам. Представляется целесообразным проработать вопрос интеграции этих ресурсов для создания межгосударственного реестра уязвимостей программного обеспечения.

Исходя из того, что киберпреступность приобретает глобальный характер сегодня требуется консолидация усилий на международном уровне по противодействию этому виду противоправной деятельности.

В связи с этим поддерживаем предложение о принятии Конвенции об обеспечении международной информационной безопасности.

Д.И. Григорьев

Директор департамента защиты информации и IT-инфраструктуры ПАО «ГМК «Норильский Никель», член Президиума НАМИБ

Задача обеспечения безопасности критической информационной инфраструктуры (КИИ) выходит на «передовую линию» корпоративной защиты, вследствие ускоренной и повсеместной цифровизации производственных и технологических процессов, затронувшей практически все отрасли.

Для градообразующих и регионообразующих компаний, чья деятельность имеет стратегическое значение для национальной экономики, защита объектов КИИ, находящихся в их ведении, является одним из приоритетов. Бизнес в целом – это сосредоточение объектов КИИ, поэтому именно на бизнесе лежит основная ответственность по их защите.

«Норникель», будучи одним из лидеров мировой горно-металлургической индустрии и в то же время мультиотраслевым конгломератом, обеспечивает полный цикл операций, включая разведку, добычу, производство металлов, транспорт, ТЭК, логистику, сбыт и т.д.

Незаконное и злонамеренное воздействие посредством электронно-коммуникационных средств на объекты КИИ, отвечающие за бесперебойность производственных и технологических процессов, а также цепочек поставок, может, в зависимости от места и роли компании в экономике, иметь крайне негативные социально-экономические последствия для регионов присутствия и оказать ощутимое влияние на страновые макроэкономические показатели в целом.

Мировое сообщество уже давно осознало приоритет вопросов обеспечения безопасности КИИ во всем комплексе проблем международной информационной безопасности. И государство, и бизнес сталкиваются с новыми вызовами и угрозами в этой сфере.

В любой момент инцидент безопасности на объектах КИИ может стать casus belli для полномасштабного военного конфликта, особенно когда речь идет о причинении масштабного ущерба экономике и социальному благополучию страны, или, в наихудшем случае, о человеческих жертвах.

Бурное развитие и внедрение технологий искусственного интеллекта для обеспечения работы КИИ, создает новые, пока еще неочевидные и непредсказуемые риски, которые могут стать реальными уже в ближайшем будущем. Промышленные компании все больше внедряют в производственные процессы технологии Интернета вещей (Industrial IoT), больших данных (Big Data), роботизацию, системы беспроводной связи нового поколения и другие инновационные решения. Все это требует комплексной и многоуровневой защиты от воздействия злоумышленников.

Еще одна немаловажная проблема – концентрация опорных для КИИ информационно-коммуникационных технологий под юрисдикцией ограниченного числа государств. Это фактически ведет к размыванию суверенитета остальных членов международного сообщества в такой стратегически важной области. Именно поэтому на международном уровне активно обсуждается вопрос определения и закрепления границ в информационном пространстве, в том числе границ КИИ.

В целом тема обеспечения безопасности КИИ входит в повестку ключевых международных площадок: ООН, ОБСЕ, АСЕАН, ШОС и др. Россия в числе первых начала концептуально прорабатывать и фиксировать нормативно-правовой статус вопросов защиты КИИ в национальных документах стратегического уровня.

Однако процесс выстраивания эффективной системы информационной безопасности на международном и национальном уровнях, в первую очередь для КИИ, невозможен без тесного взаимодействия государства и бизнеса, в том числе посредством инструментов государственно-частного партнерства (ГЧП). В этом контексте возникает необходимость усовершенствования нормативно-правовой базы и создания дополнительных экономических стимулов для реализации проектов ГЧП в сфере обеспечения безопасности информационно-коммуникационных технологий.

«Норильский никель» постоянно работает в этом направлении. Мы развиваем инновационные технологические платформы для выявления новых угроз, в первую очередь для АСУ ТП, создаем экспертные площадки для обмена лучшими практиками обеспечения ИБ в промышленности – в 2017 году нами создан Клуб «Безопасность информации в промышленности» (БИП-Клуб), выступаем с инициативами международного уровня – в 2018 году нами был разработан и представлен проект Хартии информационной безопасности критических объектов промышленности.

Включение данной темы в повестку дня Форума позволяет поднять наиболее острые вопросы, связанные с обеспечением безопасности критической информационной инфраструктуры и получить экспертные оценки решений российского и международного бизнеса, а также инициатив, предлагаемых академическим сообществом.

А.А. Воробьев
Директор Координационного Центра доменов .RU/. РФ

СИСТЕМА БЕЗОПАСНОСТИ РОССИЙСКИХ НАЦИОНАЛЬНЫХ ДОМЕНОВ .RU И .РФ

Российский интернет – неотъемлемая часть глобального, Рунет органично вписан в Глобальную сеть. Представить, что эта связь может быть разорвана, практически невозможно. Закон о «суверенном» Рунете пугает многих именно словом «суверенный» – людям кажется, что речь идет об изоляции. На самом деле, в эти слова вкладывается другой смысл – «способный работать самостоятельно при необходимости», «стабильный, независимо от внешних факторов». Необходимо обеспечить устойчивость работы интернета в России в любых обстоятельствах, даже в случае неблагоприятных внешних воздействий: природных, техногенных или иных. А это значит, что должна работать бесперебойно вся технологическая инфраструктура, в том числе и система интернет-адресации.

Сегодня мы можем наблюдать две важных тенденции: это усиление мер по безопасности в сети, а также более пристальное внимание к Рунету со стороны государства. Так в п.1 статьи 14.2. Федерального закона от 27.07.2006 N 149-ФЗ “Об информации, информационных технологиях и о защите информации” мы увидим ответ законодателей на многие вопросы:

«Обеспечение устойчивого и безопасного использования на территории Российской Федерации доменных имен»

1. *В целях обеспечения устойчивого и безопасного использования на территории Российской Федерации доменных имен создается национальная система доменных имен, которая представляет собой совокупность взаимосвязанных программных и технических средств, предназначенных для хранения и получения информации о сетевых адресах и доменных именах.*

Приказом Роскомнадзора от 29.07.2019 N 216[1] определен перечень групп доменных имен, составляющих российскую национальную доменную зону.

Так российскую национальную доменную зону составляют доменные имена, входящие следующие группы доменных имен, имеющих единое уникальное символьное значение (далее-домен верхнего уровня):

а) домен верхнего уровня .RU;

б) домен верхнего уровня. РФ;

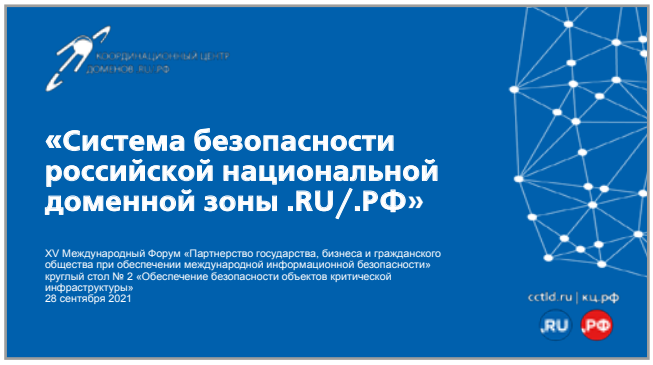
в) домен верхнего уровня .SU;

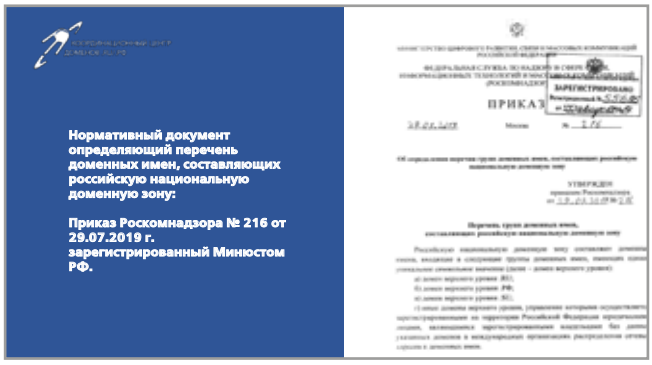
г) иные домены верхнего уровня, управление которыми осуществляется зарегистрированными на территории Российской Федерации юридическими лицами, являющиеся зарегистрированными владельцами баз данных указанных доменов в международных организациях распределения сетевых адресов и доменных имен.

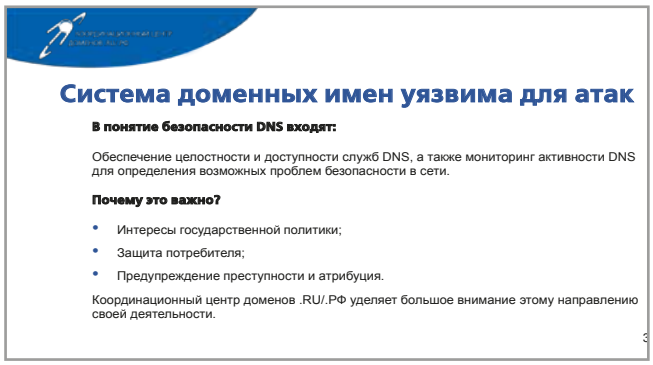
АНО «Координационный центр национального домена сети Интернет» является регистратурой доменов .RU и .РФ.

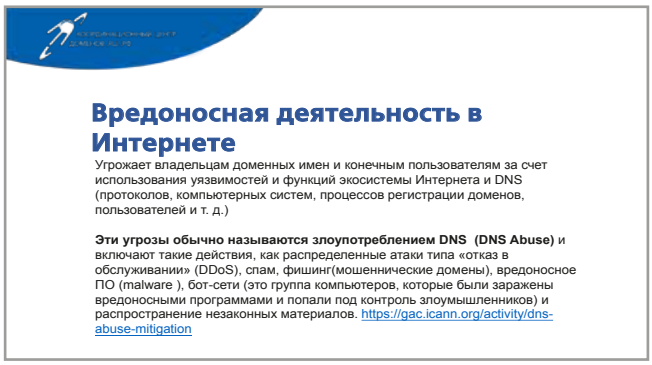
Сама технология DNS (Domain Name System – «система доменных имён») создана на заре развития Интернета в 80-х годах прошлого века. Тогда никто не думал о сетевой безопасности. DNS работает без аутентификации и шифрования, обрабатывая запросы любого пользователя. В связи с этим существует множество способов обмануть пользо-

1 Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 29.07.2019 № 216 «Об определении перечня групп доменных имен, составляющих российскую национальную доменную зону» (Зарегистрирован 20.08.2019 № 55686)









вателя и подделать информацию о том, где на самом деле осуществляется преобразование имен в IP-адреса. Таким образом, все данные DNS были доступными для каждого. Соответственно, расширения не предназначены для обеспечения конфиденциальности и это записано в RFC 4033.

В понятие безопасности DNS входят: обеспечение целостности и доступности служб DNS, а также мониторинг активности DNS для определения возможных проблем безопасности в сети.

Целостность (англ. Integrity) – избежание несанкционированной модификации информации – это гарантирование того, что информация остается неизменной, корректной и аутентичной. Обеспечение целостности предполагает предотвращение и определение неавторизованного создания, модификации или удаления информации. Примером могут являться меры, гарантирующие, что почтовое сообщение не было изменено при пересылке.

Доступность – (англ. Availability) – избежание временного или постоянного сокрытия информации от пользователей, получивших права доступа – это гарантирование того, что авторизованные пользователи могут иметь доступ и работать с информационными активами, ресурсами и системами, которые им необходимы, при этом обеспечивается требуемая производительность. Примером может являться защита доступа и обеспечение пропускной способности почтового сервиса.

Недоступность всех корневых DNS-серверов сети Интернет в течение длительного времени привела бы к невозможности разрешения имен в сети[2].

Почему это важно:

- интересы государственной политики;
- защита потребителя;
- предупреждение преступности и атрибуция.

Поэтому Координационный центр доменов .RU/.РФ уделяет большое внимание этому направлению своей деятельности.

Вредоносная деятельность в Интернете

Такая деятельность угрожает администраторам доменных имен и конечным пользователям за счет использования уязвимостей и функций экосистемы Интернета и DNS (протоколов, компьютерных систем, процессов регистрации доменов, пользователей и т.д.). В больших масштабах некоторые из этих действия могут угрожать безопасности, стабильности и отказоустойчивости инфраструктур DNS. Эти угрозы обычно называются злоупотреблением DNS (DNS Abuse) и включают такие действия, как распределенные атаки типа «отказ в обслуживании» (DDoS), спам,

2 Из книги «DNS and BIND» PaulAlbitz and Cricket Liu

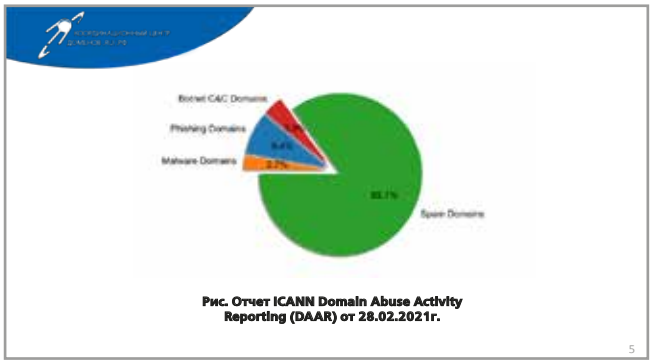


Рис. Отчет ICANN Domain Abuse Activity Reporting (DAAR) от 28.02.2021г.

фишинг, вредоносное ПО, управление бот-сетями и распространение незаконных материалов. Это определение можно прочитать на сайте ICANN https://gac.icann.org/activity/dns-abuse-mitigation

У ICANN есть проект по отчетности о случаях злоупотребления доменами Domain Abuse Activity Reporting Project (DAAR). DAAR – это платформа для изучения регистрации доменных имен и поведения, связанного с угрозами безопасности (злоупотреблениями) в регистратурах и у регистраторов доменов верхнего уровня (TLD).

Система состоит из двух основных компонентов:

1. Система сбора – собирает файлы зон каждого TLD, по которому у нас есть возможность получать данные, собирает данные о злоупотреблениях доменом из независимых источников сообщений об угрозах безопасности и соотносит угрозы безопасности с конкретными TLD.
2. Система администрирования с графическим пользовательским интерфейсом (GUI) – предоставляет табличную и графическую визуализацию регистрации доменов и злоупотреблений и отображает исторические данные. Графический интерфейс позволяет администраторам из числа персонала ICANN изучать действия, связанные с угрозами безопасности, и экспортировать данные для создания отчетов.

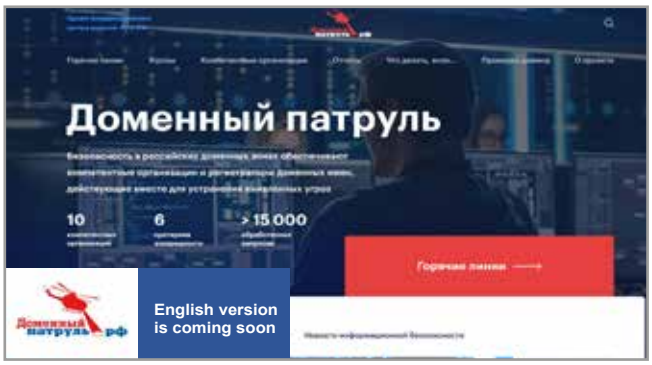
В совокупности эти две системы позволяют просматривать один или несколько дней из жизни служб регистрации доменов, включая случаи злоупотребления зарегистрированными доменными именами. Общая цель DAAR – информировать сообщество ICANN об угрозах безопасности, чтобы оно могло использовать эти данные для принятия обоснованных решений.

Так в одном из отчетов ICANN Domain Abuse Activity Reporting (DAAR) от 28.02.2021 мы найдем диаграмму распределения таких вредоносных атак.

Координационный центр доменов .RU/.РФ проводит международные конференции администраторов и регистраторов стран СНГ, Центральной и Восточной Европы с 2008 года.

15 сентября 2021 года состоялось открытие 14-й конференции администраторов и регистраторов стран СНГ, Центральной и Восточной Европы. Номинальной принимающей сторной выступил Узбекистан. Конференцию открыли Андрей Воробьев, директор Координационного центра доменов .RU/.РФ и Олег Пекось, первый заместитель министра по развитию информационных технологий и коммуникаций Республики Узбекистан.

На профильных секциях TLDCON традиционно проходит обмен опытом и мониторинг лучших практик по тематике безопасного ис-



пользования DNS. Так 16 сентября 2021 года на TLDCON 2021 на секции по безопасности в доменном пространстве были рассмотрены новые типы угроз в DNS и меры, которые разрабатываются членами доменного международного сообщества для их предотвращения. В ходе дискуссии участники рассказали насколько эффективны существующие механизмы борьбы с использованием доменов для вредоносных целей.

Грэм Бантон из DNS Abuse Institut дал определение DNS Abuse: «Это любой ущерб, который подвергает угрозе целостность DNS и совершается через DNS. Это может быть любое зловредное ПО Malwere, botnet, pharming— процедура скрытного перенаправления жертвы на ложный IP-адрес., shiching.» Не исключено, что в будущем появятся новые категории зловредов и определение может актуализироваться.

Патрик Майлс из Европейского совета регистраторов верхнего уровня (CENTR): «У нас отсутствует определение DNS Abuse потому, что общий ландшафт постоянно меняется, а у наших экспертов разные взгляды на это. Но мы все признаем, что проблема существует».

Брайан Симполич, PIR (Public Interest Registry) рассказал об алгоритме генерации доменов DGA (Domen Generation Algoritm).

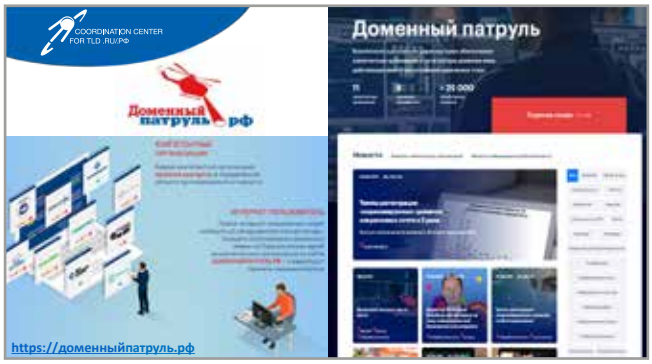
Знание принципа работы это алгоритма позволяет правоохранительным органам разных стран предупреждать правонарушения типа ботнет, который в обход традиционным методам регистрации доменов автоматически «генерит» сотни тысяч доменов. Иногда это количество превышает количество доменов, зарегистрированных национальной регистратурой. Вот почему это серьезный современный вызов.

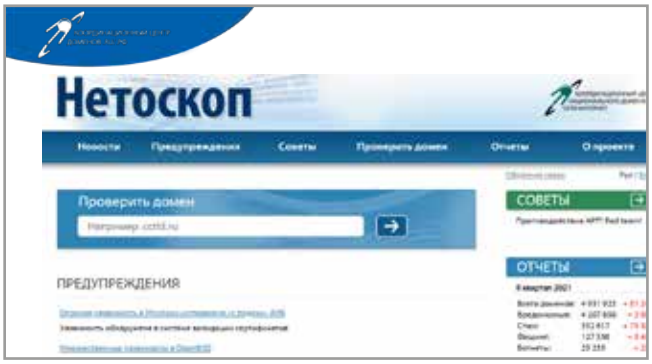
Джорди Ипаррагирре из EURID.EU рассказал о возможности использовать искусственный интеллект для того, чтобы выявлять подозрительные регистрации доменных имен.

Наши международные инициативы и мероприятия полезны для мониторинга лучших практик по этой тематике. Координационный центр имеет и собственные проекты для выявления и изучения противоправной деятельности в Интернете с использованием доменных имен. По существу, мы создали «Систему безопасности российских национальных доменов», в которую входят такие наши проекты как «Доменный патруль», «Нетоскоп», институт компетентных организаций и др.

Взаимодействие интернет-пользователей, компетентных организаций и аккредитованных регистраторов доменных имён в Рунете.

На сайте доменныйпатруль.рф размещены данные горячих линий всех компетентных организаций, сотрудничающих с Координационным центром, а также способы обрат-





ной связи с подразделением МВД России по борьбе с сетевым мошенничеством. Кроме того, здесь собраны актуальные сведения о распространении киберугроз в интернете и о ходе борьбы с вредоносными ресурсами.

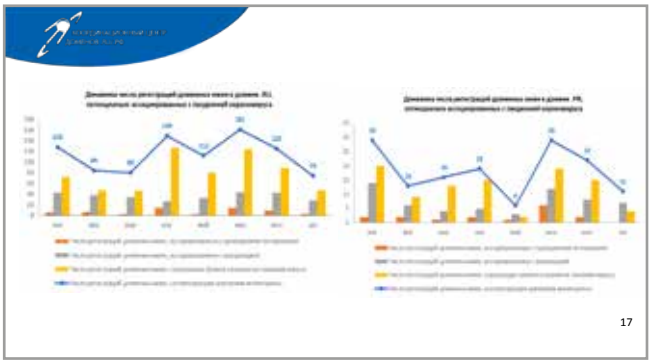
Проект «Нетоскоп» – это первый в России информационно-аналитический ресурс, посвященный информационной безопасности в доменном пространстве. На сайте публикуются информационные, справочные и аналитические материалы о распространении «зловредов» в сети Интернет и ходе борьбы с вредоносными ресурсами. Посетителям ресурса доступен онлайн-сервис по проверке доменных имен на использование в «зловредной» активности, а также формирование отчетов по типам и количеству зловредов, зафиксированных компаниями-участниками проекта.

Институт компетентных организаций

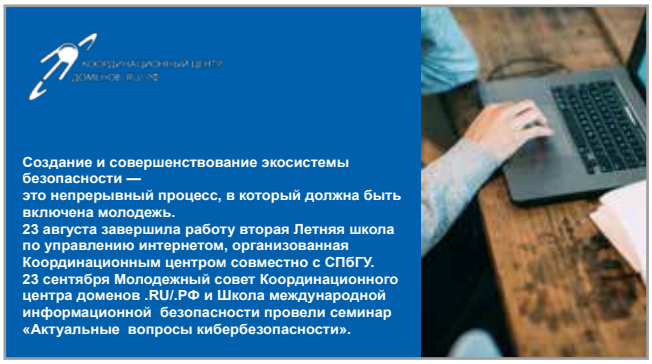
В 2012 году Координационный центр внедрил практику взаимодействия с организациями, компетентными в определении нарушений в сети Интернет. Такие организации предоставляют Координационному центру и регистраторам доменных имен информацию о ресурсах с противоправным контентом, о случаях фишинга, несанкционированного доступа к информационным системам и распространения вредоносных программ с доменных имен, находящихся в зонах .РФ и .RU. Регистраторы вправе прекратить делегирование доменных имен для подобных ресурсов. Сегодня с Координационным центром сотрудничают одиннадцать компетентных организаций – Национальный координационный центр по компьютерным инцидентам, Лига безопасного интернета, Group-IB, Лаборатория Касперского, RU-CERT, РОЦИТ, Роскомнадзор, БИЗон, Банк России и Доктор Веб. Любой пользователь сети может сообщить об обнаруженном им случае неподобающего использования доменного имени на Горячую линию одной из этих организаций – и меры будут приняты незамедлительно

Мониторинг реестра национальных доменов .RU и .РФ, проводимый, на постоянной основе Координационным центром доменов .RU/.РФ, показал, что количество регистраций, связанных с темой COVID-19, мерами по сдерживанию пандемии, а также вакциной, снижается. За первый месяц осени 2021 года в зоне .RU появилось всего 104 «коронадомена», в .РФ – 16. Общий прирост составил 120 доменных имен, что почти в два раза ниже показателей августа: в предыдущем месяце в .RU и .РФ было зарегистрировано 228 «коронавирусных» доменных имен. В среднем в сентябре каждые два дня регистрировалось 7 «коронадоменов» в .RU и 1 в .РФ.

За весь период наблюдений (с января 2020 года по сентябрь 2021 года) в список доменных имен, содержащих слова «corona», «covid», «pandemia», «ковид», «пандемия»,



17



«вакцина» и другие, было добавлено 4291 домен в .RU и 875 в .РФ; в общей сложности в российских доменных зонах насчитывается 5166 «коронадоменов».

23 августа 2021 года завершила работу вторая Летняя школа по управлению интернетом, организованная Координационным центром совместно с СПбГУ. Всего на участие в Летней школе было подано 127 заявок, на подготовительный этап был отобран 81 участник, а к основному этапу были допущены 40 лучших участников.

23 сентября 2021 года Молодежный совет Координационного центра доменов .RU/.РФ и Школа международной информационной безопасности провели семинар «Актуальные вопросы кибербезопасности». На семинар зарегистрировались порядка 150 человек из России, Турции, Украины, Пакистана, Казахстана, США, Белоруссии, Грузии и Киргизии, среди которых были представители различных международных организаций и государственных органов, в том числе Совета Европы и МИД России. Встреча прошла в гибридном формате: офлайн в Институте актуальных международных проблем Дипломатической академии МИД России и онлайн на платформе Zoom. Семинар открыли проректор по учебной работе Дипломатической академии МИД России Андрей Данельян, проректор по научной работе, директор ИАМП Олег Карпович. Ведущие эксперты Международного союза электросвязи, Лаборатории Касперского и Координационного центра доменов .RU/.РФ рассказали участникам о том, с какими вызовами приходится сталкиваться на международном и региональном уровнях.

В решение вопросов, связанных с киберпреступностью и безопасностью в интернете, несомненно, нужно вовлекать молодежь, ведь таким образом мы закладываем основу для построения безопасной информационной среды. На наших мероприятиях для молодежи выступают спикеры, представляющие разные группы профессиональных участников рынка: международные организации, крупный частный бизнес, некоммерческий сектор. И только совместная скоординированная работа всех участников гарантирует достижение прогресса в области обеспечения кибербезопасности.

А.М. Сычев
Первый заместитель директора Департамента информационной безопасности Банка России

МЕЖДУНАРОДНОЕ ИНТЕГРАЦИОННОЕ СОТРУДНИЧЕСТВО МЕЖДУ БАНКОМ РОССИИ И НАЦИОНАЛЬНЫМИ БАНКАМИ В ДОСТИЖЕНИИ КИБЕРУСТОЙЧИВОСТИ ОРГАНИЗАЦИЙ КРЕДИТНО-ФИНАНСОВОЙ СФЕРЫ

Коллеги, добрый день!

Спасибо большое за предоставленное слово. Я постараюсь тезисно сформулировать те позиции, которые Центральный банк считает крайне важным в части обеспечения устойчивого функционирования в кредитно-финансовой сфере, как одного из субъектов критически важных инфраструктур.

Первый тезис, который не вызывает никаких сомнений – это тезис, связанный с цифровизацией и трансграничностью финансовой отрасли. Это касается не только Российской Федерации, но и всего мира. Платежи и обмен финансами это та сфера, которая границ не имеет, особенно, если мы с Вами говорим про розничные платежи или про платежи для малых и средних предприятий.

Какое следствие из этого мы получаем? На сегодняшний день безопасность в финансовых организациях становится слишком многогранной, она стремится к экосистемным объединениям и не имеет четко выраженного периметра. То состояние замкнутости и контролируемого периметра, которое было 15–20 лет назад, сейчас недостижимо. Это привносит совершенно новые риски с точки зрения информационной безопасности и требует иного подхода. Не такого, как мы привыкли в информационной безопасности на объектах критически важной инфраструктуры.

Второй тезис заключается в том, что атаки, которые могут начаться на территории одного государства, на территории одной финансовой организации, могут быть дальше транслированы в третьи страны, в партнерские сети, в партнерские организации и иметь последствия для финансовых организаций разных стран одновременно. В качестве примера могу привести ситуацию, которая произошла пару лет назад с финансовой организацией Российской Федерации. Она была атакована, какое-то время ее информационные ресурсы были подконтрольны злоумышленникам и использованы в качестве плацдарма для атаки на партнеров этой организации по платежному сервису.

Третий тезис – необходимость обратить внимание на так называемые атаки цепочек поставки. Такого типа атаки могут осуществляться не на саму финансовую организацию, а на одного из партнеров и привести к ситуации, когда фактически будет атакована сама финансовая организация. Обращаю внимание, что, как правило, таки атаки имеют признаки трансграничности. Здесь отсутствует четко выраженный периметр. И это большой вызов традиционным методам обеспечения информационной безопасности и требует совершенно другой взгляд.

Кибербезопасность становится одним из ключевых моментов для обеспечения надежного функционирования финансовых организаций, то есть для обеспечения так называемой операционной надежности. Следует отметить, что большинство финансовых регуляторов, задумались о необходимости регулирования и контроля операционной надежности.

Как правило в англоязычной литературе используется термин cyber resilience, но, по сути, мы говорим об операционной надежности функционирования финансовой организации для обеспечения бесперебойного

и постоянного обслуживания клиентов вне зависимости от того, где он находится, в какой точке мира, и какие партнеры у этой финансовой организации существуют, а так же какие воздействия оказываются на информационную инфраструктуру финансовой организации.

Выводом из всех данных тезисов является необходимость тесной интеграции и сотрудничества, прежде всего финансовых регуляторов.

Такую деятельность мы, как Центральный банк, проводим на площадке БРИКС. В рамках сотрудничества были реализованы публикации нескольких документов – это доклад о цифровой финансовой доступности, сборник лучших практик по надзору и контролю в части информационной безопасности в финансовой сфере и электронный буклет о практиках информационной безопасности, применяемых в тех или иных государствах.

Почему для нас это важное событие? Мы понимаем, что, имея очень плотное взаимодействие финансовых организаций между собой, имея достаточно серьезное и тесное взаимодействие финансовых сервисов, мы должны быть уверены, что и всеми сторонами информационная безопасность понимается одинаково, меры, принимаемые в финансовых организациях, также одинаковые. И это дает уверенность в том, что сервисы, предоставляемые клиентам, будут защищены вне зависимости от того, в какой юрисдикции находится тот или иной сервис или тот или иной человек.

Меры и методы защиты не могут быть статичны и постоянно требуют корректировки. Поэтому важно понимать, какие угрозы и какие события могут повлиять на реальную защищенность и на операционную надежность. То есть важен обмен информацией о рисках, угрозах и методах их нейтрализации. В этом смысле мы плотно общаемся с коллегами из Центральных банков государств – членов ЕАЭС. Сформулированы единые правила обмена информацией об операциях без согласия клиентов, а также единые правила информационного обмена о событиях информационной безопасности. Налаженный информационный обмен имеет существенную практическую пользу.

Завершая свое выступление, я хотел бы обратить внимание, что мы, как Центральный банк, полагаем целесообразным вести широкое обсуждение вопросов информационной безопасности, потому что еще раз скажу, что безопасность в финансовых организациях – это крайне многогранная история, и она далеко не ограничивается исключительно техническими вопросами. Мы регулярно такое обсуждение проводим. В 2020 году оно проходило с широким международным участием, и у нас были представители регуляторов из большого количества стран, не только БРИКС, но и Восточной Азии. Мы считаем, что такое обсуждение – это не только хорошая площадка для обмена опытом, но и продвижение инициатив Российской Федерации в части информационной безопасности и обеспечения операционной надежности глобально в рамках финансовой отрасли.

Спасибо за внимание!

А.К. Жарова
Старший научный сотрудник Института Государства и права РАН, доктор юридических наук, доцент

НАПРАВЛЕНИЯ МЕЖДУНАРОДНОГО СОТРУДНИЧЕСТВА В ОБЛАСТИ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ

Объем информации, обрабатываемой информационными технологиями, увеличивается изо дня в день. В соответствии с анализом рынка, проведенным научно-техническим центром Главного радиочастотного центра рынок интернет вещей в России растет на 18,3% в год к концу 2021 г. его объем – промышленный и потребительский составит 49,39 млрд долларов, а в 2024-м превысит 100 млрд[1]. К концу 2022 г. на территории Российской Федерации должен быть запущен спутниковый интернет вещей[2], к концу 2023 г. пилотная сеть квантового интернета вещей[3].

Огромное количество «вещей», подключенных к Интернету для обмена данными с другими вещами не только позволяют облегчить наше существование, например, умные дома, электросети, технологии и др., но и поднимают проблемы, связанные с предотвращением возможных уязвимостей, рисков и угроз в ИКТ, с обеспечением информационной безопасности.

В связи с масштабом подключенных и взаимодействующих информационных технологий, переводом общественных отношений, включая сферу государственного управления в цифровую форму, задача обеспечения информационной безопасности значительно обострилась.

В соответствии с Основами государственной политики Российской Федерации в области международной информационной безопасности[4] к основным угрозам международной информационной безопасности относятся, в том числе «использование информационно-коммуникационных технологий для проведения компьютерных атак на информационные ресурсы государств, в том числе на критическую информационную инфраструктуру».

Основными направлениями реализации государственной политики в области международной информационной безопасности по совершенствованию межгосударственного взаимодействия, направленного на противодействие угрозе использования информационно-коммуникационных технологий для проведения компьютерных атак на информационные ресурсы государств, в том числе на критическую информационную инфраструктуру, а также межгосударственного взаимодействия в области реагирования на компьютерные инциденты являются развитие сотрудничества с иностранными государствами, международными неправительственными организациями и организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты, в целях выработки механизма обмена информацией о таких инцидентах и повышения эффективности взаимодействия уполномоченных органов.

Роль международного сотрудничества,

1 Объем рынка интернета вещей в России вырос на 18,3% // https://rg.ru/2021/07/28/obem-rynka-interneta-veshchej-v-rossii-vyrosna-183.html

2 Дорожная карта развития «сквозной» цифровой технологии «Технологии беспроводной связи» (Документ опубликован не был) // СПС «КонсультантПлюс».

3 Паспорт «дорожной карты» развития высокотехнологичной области «квантовые коммуникации» на период до 2024 года» (Документ опубликован не был) (утв. Минцифры России 27 августа 2020 г. № 17) // СПС «КонсультантПлюс».

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

направленного на предотвращение угроз и уязвимостей, недекларированных функций информационных технологий, в том числе злоупотреблений в киберпространстве нельзя переоценить. Соглашения в области определения способов верификации функций безопасности и ответственного поведения государств, связанного с взаимным информированием о новых уязвимостях являются правовыми инструментами в международном праве.

Взаимная ИКТ уязвимость государств предопределяет трансграничность рисков и угроз, свойственных для информационных технологий в связи с этим международное сотрудничество в сфере кибербезопасности, безопасности аппаратно-программных комплексов приобретает все большее значение. Комплекс правовых инструментов обеспечения кибербезопасности должен включать требования к методам и алгоритмам информационных технологий, направленные на исключение или минимизацию уязвимостей при разработке ИТ и их внедрении, а также требования к своевременному устранению уязвимостей в случае их обнаружения на протяжении всего жизненного цикла информационной системы.

Решение проблемы уязвимостей завершает один из этапов обеспечения информационной безопасности и кибербезопасности. Предложения по решению данной проблемы определены в Концепции Конвенции об обеспечении международной информационной безопасности[5] (далее, Концепции Конвенции) подготовленной Российской Федерацией в 2021 г. В Концепции Конвенции подчеркивается «важное значение информационной безопасности для реализации основных прав и свобод человека и гражданина, прежде всего права на уважение частной жизни и защиту персональных данных», а также необходимость «обеспечения глобальной стабильности в условиях нарастающей зависимости информационного общества от информационно-коммуникационных технологий»[6].

Кибербезопасность является вторым серьезным по значимости глобальным риском, который обсуждался лидерами государств на втором Всемирном экономическом форуме[7].

В предотвращении возможных рисков и угроз в области обеспечения кибербезопасности международное сотрудничество играет все более важную роль. Так, в 2015 г. всеми государствами-членами ООН принята повестка дня в области устойчивого развития на период до 2030 г., которая является планом мероприятий в целях обеспечения мира, процветания людей и планеты. Среди 17 целей, заявленных в плане мероприятий в области устойчивого развития, которые являются призывом к действиям всех стран - как развитых, так и развивающихся - в рамках глобального партнерства, определена 9 цель, направленная на создание устойчивой инфраструктуры и индустриализации, а также поощрение инноваций. Государствами признано, что расширенный доступ к ИКТ на основе безопасности и доверия является необходимым для достижения всех 17 заявленных целей.

В киберпространстве оказываются неэффективными традиционные методы и способы борьбы с преступностью, основанные на территориальном принципе, поскольку информационное пространство имеет глобальный характер. В связи с этим существующие киберриски и киберугрозы затрагивают все технологически развитые государства. Государствам необходимо объединять свои силы, создавать общие структуры для обеспечения сотрудничества в целях борьбы с киберпреступностью, поэтому решение вопроса организации взаимного доверия государств является важным для достижения эффективной борьбы с киберрисками и киберугрозами. В области обеспечения безопасности киберпространства одним из инструментов достижения такого результата является взаимодействие государств в области ответственного представления информации о факторах уязвимостей в сфере ИКТ, а также взаимный обмен соответствующей информацией о существующих методах борьбы с такими факторами уязвимости в целях ограничения, а по возможности и устранения возможных угроз для ИКТ и зависящей от ИКТ инфраструктуры.

Трансграничный характер информаци-

5 Концепция Конвенции об обеспечении международной информационной безопасности // https://namib.online/2021/07/koncepci

6 Там же

7 Global Risks Report 2020 - Reports - World Economic Forum (weforum.org) // http://reports.weforum.org/global-risks-report-2020/wild-wide-web/

онного пространства требует участие государств не только в области сотрудничества в рамках ООН, но и на уровне их двухстороннего взаимодействия.

В настоящее время кибербезопасность является основой развития цифровой эпохи и имеет решающее значение для обеспечения всеобщего, надежного и равноправного доступа к онлайновым продуктам и услугам, а также для создания надежного и устойчивого киберпространства.

Укрепление кибербезопасности и защита инфраструктуры стали неотъемлемой частью государственного стратегического планирования, поскольку происходящие инциденты ставят под угрозу доступность, целостность и конфиденциальность хранимой и передаваемой информации, а также нарушают функционирование важных информационных инфраструктур на территории различных государств[8].

Конвенция о преступности в сфере компьютерной информации[9], заключенная в г. Будапеште в 2001 г. уже не отвечает вызовам настоящего времени, связанными со стремительными темпами внедрения цифровых технологий. Многие из существующих угроз в области киберпространства не представлены в данной Конвенции. Невозможно вести эффективную борьбу с киберпреступлениями, преступлениями в информационном пространстве без определения и выработки общих юридических механизмов[10] и, соответственно криминализации деяний, связанных компьютерными преступлениями.

Группы правительственных экспертов ООН по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности признают, что на деятельность государств в ИКТ-инфраструктуре, расположенной на их территориях, распространяются принципы обеспечения суверенитета государств. Государства наряду с другими принципами международного права должны соблюдать принцип суверенного равенства, разрешение споров мирными средствами и невмешательство во внутренние дела других государств[11].

Таким образом, можно отметить, что обсуждение на уровне ООН проблем, связанных с возможными уязвимостями в ИКТ, важности ответственного представления государствами информации о них, свидетельствует об их международном значении, в решении которых заинтересованы многие информационно развитые государства. Взаимная высокая ИКТ уязвимость многих стран мира является главным источником нестабильности. Интернет-пользователи должны быть уверены в безопасности ИКТ, для этого необходимо предупреждать распространение злонамеренных программных и технических средств и использование скрытых вредоносных функций.

Литература

1. Объем рынка интернета вещей в России вырос на 18,3% // https://rg.ru/2021/07/28/obem-rynka-interneta-veshchej-v-rossii-vyros-na-183.html
2. Дорожная карта развития “сквозной” цифровой технологии “Технологии беспроводной связи” (Документ опубликован не был) // СПС «КонсультантПлюс».
3. Паспорт “дорожной карты” развития высокотехнологичной области “квантовые коммуникации” на период до 2024 года” (Документ опубликован не был) (утв. Минцифры России 27 августа 2020 г. № 17) // СПС «КонсультантПлюс».
4. Указ Президента РФ от 12 апреля 2021 г. № 213 “Об утверждении Основ государственной политики Российской Федерации в области международной информационной безопасности” //СЗ РФ 2021. № 16 (Ч. I). Ст. 2746.
5. Концепция Конвенции об обеспечении международной информационной безопасности // https://namib.online/2021/07/koncepcija-konvencii-oon-ob-obespechenii-mezhdunarodnoj-

8 Роль МСЭ в укреплении уверенности и доверия при использовании ИКТ // https://www.itu.int/ru/mediacentre/backgrounders/Pages/role-of-ITU-in-building-confidence-and-trust-in-the-use-of-ICTs.aspx

9 Конвенция о преступности в сфере компьютерной информации ETS № 185 // СПС «КонсультантПлюс».

10 Атнашев В. Р., Яхъеева С. Н. Международное сотрудничество в борьбе с киберпреступностью и кибертерроризмом // https://cyberleninka.ru/article/n/mezhdunarodnoe-sotrudnichestvo-v-borbe-s-kiberprestupnostyu-i-kiberterrorizmom

11 Красиков Д.В. Территориальный суверенитет и делимитация юрисдикций в киберпространстве // https://cyberleninka.ru/article/n/territorialnyy-suverenitet-i-delimitatsiya-yurisdiktsiy-v-kiberprostranstve

informacionnoj-bezopasnosti/
6. Global Risks Report 2020 – Reports - World Economic Forum (weforum.org) // http://reports.weforum.org/global-risks-report-2020/wild-wide-web/
7. Роль МСЭ в укреплении уверенности и доверия при использовании ИКТ // https://www.itu.int/ru/mediacentre/backgrounders/Pages/role-of-ITU-in-building-confidence-and-trust-in-the-use-of-ICTs.aspx
8. Конвенция о преступности в сфере компьютерной информации ETS № 185 // СПС «КонсультантПлюс».
9. Атнашев В. Р., Яхъеева С. Н. Международное сотрудничество в борьбе с киберпреступностью и кибертерроризмом // https://cyberleninka.ru/article/n/mezhdunarodnoe-sotrudnichestvo-v-borbe-s-kiberprestupnostyu-i-kiberterrorizmom
10. Красиков Д.В. Территориальный суверенитет и делимитация юрисдикций в киберпространстве // https://cyberleninka.ru/article/n/territorialnyy-suverenitet-i-delimitatsiya-yurisdiktsiy-v-kiberprostranstve

Андреас Кюн
Американский филиал международного Исследовательского фонда «Observer» (США)

МАРКИРОВКА КИБЕРБЕЗОПАСНОСТИ ИНТЕРНЕТА ВЕЩЕЙ И КРИТИЧЕСКИ ВАЖНАЯ ИНФОРМАЦИОННАЯ ИНФРАСТРУКТУРА

Я хотел бы поблагодарить Национальную Ассоциацию международной информационной безопасности (НАМИБ) за приглашение. Меня зовут Андреас Кюн, и я старший научный сотрудник Американского филиала международного Исследовательского фонда «Observer» (Observer Research Foundation – ORF America).

На встрече в Гармише несколько лет назад я говорил о проблемах обеспечения безопасности Интернета вещей, а также о рисках и угрозах, которые могут исходить от этой новой, полностью подключенной, постоянно работающей, глобально распределенной инфраструктуры. Коронная фраза, которая запомнилась мне тогда, была «Цунами уязвимостей, исходящих из Интернета вещей».

Теперь, спустя несколько лет и после появления еще нескольких миллиардов подключенных устройств Интернета вещей, я хочу поговорить о маркировке кибербезопасности как о новом, инновационном способе защиты потребителей и укрепления кибербезопасности.

На протяжении десятилетий государства пытались решить проблемы критической инфраструктуры, определяя критические системы и отрасли промышленности, которые заслуживают защиты и часто подвергаются жесткому или слабому надзору со стороны регулирующих органов для обеспечения безопасности и защиты. В качестве примера вы можете рассмотреть 16 важнейших секторов инфраструктуры в США[1].

Подключенные потребительские устройства не считаются критически важной инфраструктурой в традиционном смысле этого слова. Тем не менее они являются важнейшей частью цифровой трансформации, которая обещает огромные экономические и социальные выгоды. Я бы сказал, что значительное количество устройств Интернета вещей используется потребителями. Общее число, которое, по оценкам, составило 7 миллиардов в 2018 году, сегодня увеличилось до 30 миллиардов устройств Интернета вещей и, как ожидается, более чем удвоится к 2025 году. Продвигаясь вперед, нам нужно более точно подумать о том, как и где это вписывается в обсуждение защиты критически важной инфраструктуры. Но это тема для дальнейшего обсуждения. Сегодня позвольте мне углубиться в то, что есть ярлыки кибербезопасности и как они могут помочь укрепить безопасность, используя аналогию с гастрономической индустрией.

Стали бы вы сознательно есть в ресторане, который имеет сомнительные санитарные показатели?

Пищевая промышленность решила проблему плохой санитарии с помощью неанонсированных проверок и системы оценки буквенных обозначений A, B, C, о которой вы, возможно, знаете по своему опыту работы в ресторанах в Нью-Йорке или где-либо еще.

1 Агентство кибербезопасности и инфраструктуры США. Важнейшие секторы инфраструктуры, https://www.cisa.gov/critical-infrastructure-sectors; для обсуждения политики критической инфраструктуры России см. Пурсиайнен, С. Политика критической инфраструктуры России: что мы знаем об этом? Европейский журнал исследований в области безопасности 6, 21-38 (2021). https://doi.org/10.1007/s41125-020-00070-0

Чем дальше вниз по букве алфавита, тем больше вероятность расстройства желудка[2].

Действительно, этикетки являются эффективным инструментом информирования потребителей о качестве товара или услуги. Вы можете подумать об энергетических этикетках, которые рассказывают вам об энергоэффективности вашего телевизора, или об этикетке продуктов питания, которая информирует вас о пищевой ценности продуктов, которые вы покупаете в магазине.

Просто глядя на устройство Интернета вещей, как потребители, мы не очень хорошо подготовлены, чтобы определить, насколько безопасны эти подключенные устройства. Этикетка может дать потребителям возможность принимать обоснованные решения в торговой точке. На самом деле, исследования показывают, что покупатели готовы платить на 30% больше за безопасные продукты Интернета вещей. Таким образом, поставщики могли бы получать больший доход, продавая эти устройства потребителям, которые готовы больше заплатить. Это стимулировало бы столь необходимые первоначальные инвестиции в кибербезопасность.

Но если не существует ярлыка, основанного на тестировании и сертификации в соответствии с базовым уровнем безопасности или международным стандартом безопасности, асимметрия информации между продавцами и покупателями может привести к проблемам с обеспечением безопасности. Цена отсутствия безопасности становится очевидной, когда промышленности и правительствам необходимо реагировать на киберинциденты, восстанавливать атакованные компьютеры и сети, а также бороться с программами-вымогателями и похищенными конфиденциальными или чувствительными данными.

Лауреат Нобелевской премии экономист Джордж Акерлоф описал эту информационную асимметрию на рынке подержанных автомобилей, который со временем деградировал в «рынок лимонов», рынок, состоящий только из дефектных, дорогих в ремонте автомобилей. Его выводы могут быть использованы в кибербезопасности. Если нет четких показателей качества, выраженных с помощью этикетки, основанной на тестировании, мы вполне можем столкнуться с «рынком лимонов» для Интернета вещей.

В последнее время в промышленности и правительствах появились многообещающие разработки в области защитных этикеток.

Исполнительный Указ Президента США Байдена о кибербезопасности 2021 года «О повышении кибербезопасности страны (14028)» инициировал пилотный проект по маркировке. В середине сентября Национальный институт стандартов и технологий провел двухдневный семинар по маркировке кибербезопасности Интернета вещей. Записи семинара доступны на веб-сайте NIST[3].

Сингапур и Финляндия лидируют в этом процессе. Обе страны запустили этикетки для интеллектуальных, безопасных потребительских устройств и развивают эти инициативы[4].

Кроме того, частные поставщики также признали важность тестирования и сертификации устройств Интернета вещей. Underwriters Laboratories, глобальная компания по сертификации безопасности, представила рейтинг безопасности Интернета вещей на основе этикеток и подтвердила безопасность различных бытовых приборов, подключенных к Интернету. Глобальный стандарт безопасности Интернета вещей, формируемый при участии крупнейших Интернет- и технологических компаний, является еще одним примером разработки программы сертификации Интернета вещей по восьми категориям и нескольким уровням безопасности[5].

Остается ответить на ряд важных вопросов, включая следующие:

- Каков эффективный дизайн для этикеток безопасности, который передаст свойства безопасности, но не даст ложного ощущения безопасности?

2 Департамент здравоохранения и ментальной гигиены города Нью-Йорка. Инспекции предприятий Общественного питания, https://www1.nyc.gov/site/doh/services/restaurant-grades.page

3 Семинар по программам маркировки кибербезопасности для потребителей: Устройства и программное обеспечение Интернета вещей (IoT). 14-15 сентября 2021 года, https://www.nist.gov/news-events/events/2021/09/workshop-cybersecurity-labeling-programs-consumers-internet-things-iot

4 Сингапурская схема маркировки кибербезопасности (CLS): https://www.csa.gov.sg/Programmes/cybersecurity-labelling/about-cls; Ярлык кибербезопасности Финляндии: https://tietoturvamerkki.fi/en/

5 ioXt, https://www.ioxtalliance.org/certifying-your-device

- Как вы измеряете кибербезопасность и имеет ли то, что вы измеряете, отношение к безопасности?
- Как вы разрабатываете, внедряете и управляете устойчивым и масштабируемым режимом маркировки?

Я остановлюсь здесь на своем кратком обзоре, но буду рад ответить на ваши вопросы по электронной почте. Организаторы форума могут помочь вам связаться со мной.

Спасибо за внимание.

Якоб Бернтссон

Руководитель направления политики и исследований организации «Технологии против терроризма» (Великобритания)

ИСПОЛЬЗОВАНИЕ ТЕРРОРИСТАМИ ОНЛАЙН-ПЛАТФОРМ: ТЕНДЕНЦИИ И ОЦЕНКА УГРОЗ

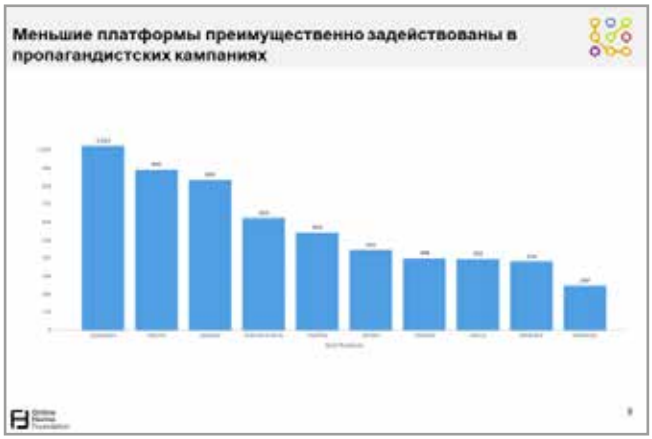
ТЕХНОЛОГИИ ПРОТИВ ТЕРРОРИЗМА» – ЭТО ГОСУДАРСТВЕННО-ЧАСТНОЕ ПАРТНЕРСТВО, ОРИЕНТИРОВАННОЕ НА ОБМЕН ЗНАНИЯМИ И ОКАЗАНИЕ ПОДДЕРЖКИ ТЕХНОЛОГИЧЕСКИМ ПЛАТФОРМАМ –

«ТЕХНОЛОГИИ ПРОТИВ ТЕРРОРИЗМА»: НАША ОПЕРАТИВНАЯ РАБОТА СОСРЕДОТОЧЕНА НА ИНФОРМАЦИОННО-ПРОПАГАНДИСТСКОЙ ДЕЯТЕЛЬНОСТИ, ОБМЕНЕ ЗНАНИЯМИ И РАЗРАБОТКЕ ТЕХНОЛОГИЙ ДЛЯ НЕБОЛЬШИХ ПЛАТФОРМ –

ЧТО ПРЕДСТАВЛЯЕТ ИЗ СЕБЯ ПЛАТФОРМА ДЛЯ АНАЛИЗА ТЕРРОРИСТИЧЕСКОГО КОНТЕНТА:

СТАТИСТИКА С МОМЕНТА ЗАПУСКА ПЛАТФОРМЫ (КОНЕЦ НОЯБРЯ 2020 ГОДА):

ТЕРРОРИСТЫ ИСПОЛЬЗУЮТ ОБШИРНУЮ И РАЗНООБРАЗНУЮ ЭКОСИСТЕМУ ОНЛАЙН-ПЛАТФОРМ ДЛЯ ВЕРБОВКИ, СБОРА СРЕДСТВ И РАСПРОСТРАНЕНИЯ ПРОПАГАНДЫ:



ТЕРРОРИСТЫ ВЫНУЖДЕНЫ ПЕРЕХОДИТЬ НА ВСЕ БОЛЬШЕЕ ЧИСЛО НИШЕВЫХ ПЛАТФОРМ, У КОТОРЫХ НЕТ ВОЗМОЖНОСТИ ИЛИ ЖЕЛАНИЯ УДАЛЯТЬ ЭКСТРЕМИСТСКИЙ КОНТЕНТ:

В 2021 ГОДУ ПРОИЗОШЕЛ ЗНАЧИТЕЛЬНЫЙ ПРОГРЕСС В ОНЛАЙН-АКТИВНОСТИ АГРЕССИВНЫХ ИСЛАМИСТСКИХ ЭКСТРЕМИСТОВ И УЛЬТРАПРАВЫХ ЭКСТРЕМИСТОВ, СКЛОННЫХ К НАСИЛИЮ:

А.Л. Козик
Региональный советник по правовым вопросам в странах Восточной Европы и Центральной Азии Международного Комитета Красного Креста

ПРАВОВЫЕ АСПЕКТЫ ЗАЩИТЫ КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ В ХОДЕ ВООРУЖЕННОГО КОНФЛИКТА

Уважаемые со-председательствующие,
Участники конференции,
Дамы и Господа!

С большой благодарностью мы в Международном Комитете Красного Креста приняли приглашение к участию в конференции. Считаем, что этот престижный форум вносит важный вклад в развитие тематики кибербезопасности. Я лично искренне рад принять в нем участие.

МККК работает в ситуации вооруженных конфликтов. Моими коллегами во всем мире движет, по большому счету, только один тезис. Мы верим, что каким бы ни был вооруженный конфликт, Комитет и воюющие стороны могут приложить усилия для того, чтобы спасти жизни гражданских лиц. МГП подчинено только одной задаче – сократить количество жертв, предотвратить излишние страдания.

Мне особенно приятно говорить об этом в России. Стране, внесшей огромный вклад в развитие МГП. Родине и соавтору важнейших инициатив, таких как Санкт-Петербургская декларация 1868 года, Гаагские конференции мира, Женевские конвенции 1949 года.

МГП для Международного Комитета Красного Креста – не пустой звук, не просто отрасль права. Зачастую это единственная защита для жертв войны и для персонала самого Красного Креста. Сотрудники МККК не носят оружия, не используют бронежилеты при этом работая часто там, куда другие не могут получить доступ. Каждый день мы видим тысячи жертв войны участь которых зависит от того – применяется ли сторонами МГП или нет.

И поэтому вопрос о применимости МГП к кибернападениям является для нас принципиальным. Здесь есть три аспекта на которые я хотел бы сегодня обратить внимание.

Во-первых, это смешение МГП и других отраслей международного права. МГП применяется только во время вооруженного конфликта. Оно не имеет ничего общего с определением статуса применяющего силу – агрессор или жертва. Не имеет ничего общего с ответственностью за развязывание войны. Никак не регулирует право на самооборону. Перенос в МГП политизированных умозаключений из других отраслей международного права вредит ему как никогда. МГП это про улучшение участи раненых и больных, про средства и методы ведения вооруженных конфликтов. Именно этому посвящены Женевские Конвенции и Дополнительные протоколы к ним.

Во-вторых, применимости МГП мешает миф о том, что поскольку атрибуция в ИКТ среде затруднительна (или даже невозможна) – применение норм права становится также невозможным поскольку непонятно к кому их применять, кто нарушитель. Этот миф основан на чрезвычайно узком понимании функции права. Право в меньшей степени задумано как мера ответственности нарушителя. Его основная функция – предписывать правомерное поведение. Отделять плохое от хорошего, допустимое от недопустимого. Факты нарушения права, равно как и случаи ухода от ответственности не ставят под сомнение саму норму. Следуя указанной ошибочной логике, можно смело отменять правила дорожного движения поскольку «многие нарушители уходят от ответственности». Кроме того, необходимо вспомнить, что международное право не

знает сроков давности. То, что нельзя атрибутировать сейчас – может стать возможным атрибутировать через пять, десять или двадцать лет.

В-третьих, еще один миф – это утверждение о том, что поскольку в ИКТ среде объекты нападения неразличимы, выполнение основополагающих норм технически невозможно – например принципа различия. И здесь, кроме приведенных выше аргументов следует сказать, что это утверждение не является новым. Именно так нацистская германия обосновывала убийство гражданского населения – «их невозможно отличить от партизан», полагали они. Абсурдность этого подхода очевидна. В качестве одного из примеров усиления принципа различия в ИКТ среде я могу привести проект по разработке цифровой эмблемы который активно поддерживается МККК. Мы призываем государства искать другие возможности соблюдения норм МГП, а не причины его несоблюдения.

Мы всячески приветствуем желание государств развивать нормы поведения в киберпространстве, дискутировать об интерпретации уже существующих норм. Но для нас является принципиально важным, чтобы на всех форумах, однозначно и определенно звучал тезис о применимости МГП.

Я думаю, в этом зале нет никого, кто бы возражал, что, например, госпитали и медицинские учреждения не должны становиться объектом нападения – будь то кинетическими средствами или посредством кибернападений.

В 2015 году благодаря Группе правительственных экспертов появляются нормы ответственного поведения государств. Эта инициатива идет много дальше требований МГП резервируя за государствами право на защиту своей критической инфраструктуры (норма g) и постулируя запрет на такие нападения (норма f). И здесь снова вклад российской делегации трудно переоценить.

Мандат МККК включает статус хранителя МГП. В 2019 году мы сформулировали институциональную позицию по вопросу применения международного гуманитарного права к кибероперациям в ходе вооруженного конфликта. В виде документа она доступна на нашем сайте и переведена на все основные языки. Использование в названии документа фразы «в ходе вооруженного конфликта» умышленно подчеркивает, хоть и избыточно, что МГП применяется только в ходе уже существующего вооруженного конфликта.

Если вернуться к нормам ответственного поведения (в частности нормам g и f), то, принимая во внимание что они охватывают и ситуации вооруженных конфликтов, можно привести несколько примеров их взаимодейтсвия с существующими нормами МГП. Во-первых, МГП налагает абсолютный запрет на нападения на гражданские объекты. Критическая гражданская инфраструктура – такая, например, как электрические сети питающие жилые зоны, в терминах МГП являются гражданским объектом. Во-вторых, МГП предоставляет особую защиту медицинским учреждениям и медицинскому персоналу. В соответствии с МГП стороны в вооруженном конфликте обязаны в любое время уважать и защищать медицинские учреждения. Это означает, что в дополнение к требованию воздерживаться от создания препятствий к их функционированию, государства должны предпринимать все возможные меры для организации их работы и предотвращать ущерб в отношении их, включая причинённый путем кибероперацийй. В-третьих, некоторые типы критической инфраструктуры квалифицируемые как необходимые для выживания гражданского населения, такие, например, как установки обеспечивающие питьевую воду, в соответствии с МГП, также подлежат особой защите. Они защищены против любых кибероперацийй, включая те, которые приостанавливают их функционирование.

Завершая свое выступление, я хочу еще раз подчеркнуть, что МГП применяется исключительно в ходе вооруженного конфликта и посвящено исключительно вопросу защиты жертв войны. Мы призываем государства приступить к активным консультациям по вопросу интерпретации и усиления конкретных норм и готовы поделиться своей экспертизой в вопросах МГП и гуманитарной деятельности

Благодарю за внимание.

Такахиро Сасаки,
Хироюки Фуджимаки
Научно-исследовательский институт стратегического мира и международных отношений, Университет Токай (Япония)

ПРИМЕНЕНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА (ИИ) В КИБЕРПРОСТРАНСТВЕ

«ПРИМЕНЕНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В КИБЕРПРОСТРАНСТВЕ»

Такахиро Сасаки (Приглашенный профессор)
Хироюки Фуджимаки (Доцент)
Научно-исследовательский институт стратегического мира и международных отношений
Университет Токай
28 сентября 2021

СОДЕРЖАНИЕ ДОКЛАДА:

Содержание

1. **Взаимосвязь между многофункциональностью / единичной функцией и высокой / низкой автономностью в ИИ**
2. **Возможность использования ИИ в военной сфере**
3. **Киберзащита с использованием ИИ**
4. **Кибератаки с использованием ИИ**
5. **Использование ИИ для операций влияния**
6. **Атаки на ИИ в киберпространстве**

ВЗАИМОСВЯЗЬ МЕЖДУ МНОГОФУНКЦИОНАЛЬНОСТЬЮ / ЕДИНИЧНОЙ ФУНКЦИЕЙ И ВЫСОКОЙ / НИЗКОЙ АВТОНОМНОСТЬЮ В ИИ:

ВОЗМОЖНОСТЬ ИСПОЛЬЗОВАНИЯ ИИ В ВОЕННОЙ СФЕРЕ:

Возможность использования ИИ в военной сфере

- Интеллектуализация оружия, подобного системам беспилотных летательных аппаратов
- Защита, атака и накопление информации в кибервойне
- Злоумышленная информация: операции влияния с использованием дезинформации и утечки стратегической информации
- Обработка и анализ информации
- Подтверждение цели и ситуативная осведомленность
- Образование/подготовка сотрудников: Военные игры, моделирование сражений
- Система принятия решений и командного управления
- Система поддержки логистики и транспорта

КИБЕРЗАЩИТА С ИСПОЛЬЗОВАНИЕМ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА:

Киберзащита с использованием Искусственного Интеллекта

1. Сбор информации о вредоносных программах, циркулирующих в Интернете, и ее анализ с помощью машинного обучения позволяют заранее понять методы атаки, которые могут быть применены в будущем.

2. ИИ использует глубокое обучение для мониторинга большого объема коммуникаций в режиме реального времени, а также анализирует информацию, общую для кибератак, и информацию об источниках атак, обнаруживает в ней отклонения и прогнозирует новые угрозы.

В будущем также ожидается разработка системы, которая способна обнаруживать передовые кибератаки, автоматически отслеживать их и автоматически принимать защитные меры. Кроме того, ИИ может работать 24 часа в отличие от людей, и появляется возможность автоматизировать то, что может быть определено с помощью машинного обучения, и снизить нагрузку на администраторов.

АТАКИ ПРОТИВ ИИ В КИБЕРПРОСТРАНСТВЕ:

Атаки против ИИ в киберпространстве

1. Уязвимости: сам Искусственный Интеллект легко обмануть. Это особенно актуально для "контролируемого ИИ". Если злоумышленник обработает ложные данные, алгоритм ИИ предоставит ответ, который будет полностью отличаться от ожидаемого результата.

2. Типичным примером является "тест, в котором к изображению панды добавляются помехи".

2. Тест, проведенный Microsoft (март 2016 г.): Microsoft провел тест на самообучение из диалога с Искусственным Интеллектом в Twitter.

Знание определенных шаблонов ввода, которые могут обмануть ИИ, может привести к ошибкам в действиях и решениях, которые принимает ИИ.

КИБЕРАТАКИ С ПРИМЕНЕНИЕМ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА (ИИ):

Кибератаки с применением Искусственного Интеллекта (ИИ)

1. Система атак на базе ИИ способна собирать большой объем информации о целях, используемых в кибератаках, формировать базу данных, предоставлять злоумышленникам подробную информацию и выполнять атаки быстрее и точнее.

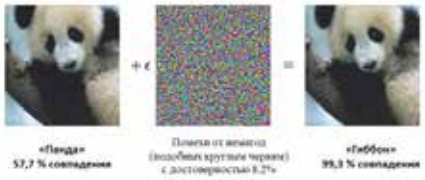
2. Машинное обучение также может быть использовано для разрушения фильтров нежелательной почты, используемых системами кибербезопасности. Кроме того, можно имитировать поведение пользователя в сети и избегать обнаружения нетипичного поведения.

3. Используя ИИ, можно усовершенствовать различные методы, главным образом применяемые в кибератаках, таких как использование информации, DDoS-атаки и взлом паролей, а сложные атаки могут быть быстро и эффективно реализованы от имени хакеров-людей.

Уже были зафиксированы многочисленные случаи кибератак с использованием "ИИ, который может решать только узкоспециализированные задачи", так называемого "слабого ИИ".

ПРИМЕРЫ КИБЕРАТАК НА ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ:

Примеры кибератак на Искусственный Интеллект



Конкурентный ввод, накладываемый на типичное изображение, может привести к тому, что классификатор ошибочно определит панду как гиббона

Знание определенных шаблонов ввода, которые могут обмануть ИИ, может привести к ошибкам в действиях и решениях, которые принимает ИИ.

КИБЕРАТАКИ С ИСПОЛЬЗОВАНИЕМ СЛАБОГО ИИ (СЛАБЫЙ ИИ: ЕДИНИЧНАЯ ФУНКЦИЯ, НИЗКАЯ АВТОНОМНОСТЬ):

Кибератаки с использованием слабого ИИ (слабый ИИ: единичная функция, низкая автономность)

Наименование атаки	Как применяется ИИ	Детали / примеры
DeepExploit	· Выбор наилучших возможностей атаки	Пример использования глубокого обучения для тестирования на проникновение.
DeepLocker	· Идентификация цели · Сокрытие вредоносного ПО	Пример использования глубокого обучения для целенаправленных атак.
tAIchi	· Автоматически генерирует вредоносное ПО	Пример использования усиленного обучения для генерации вредоносных программ.
Deepfake	· Замена лица · Воспроизведение выражения	Пример использования программного обеспечения автокодера для создания поддельных видео.

ПРИМЕРЫ КИБЕРАТАК НА ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ (ПРОДОЛЖЕНИЕ):

Примеры кибератак на Искусственный Интеллект (ИИ)

Тип атаки	Категория	Детали / примеры
Атака уклонения	· Атака на прозрачность · Атака с подменой	Атака, которая вызывает различное распознавание между людьми и механизмами машинного обучения путем ввода данных, содержащих помехи, которые не могут быть распознаны человеком (Panda case).
Атака зависимости	· Атака на доступность · Атака с обратной стороны	Атака, которая каким-либо образом сдвигает границы модели обучения путем «целенаправленного ввода данных" в обучающие данные (случай Microsoft).
Атака перемещения	· Атака конфиденциальности · Атака на выведение из членства	Атака, которая извлекает конфиденциальную информацию, подобную исходным данным, с помощью команды машинного обучения "ввод/вывод или ответ данных на механизм вывода".

ИСПОЛЬЗОВАНИЕ ИИ ДЛЯ ОПЕРАЦИЙ ВЛИЯНИЯ:

Использование ИИ для операций влияния

1. Искусственный Интеллект обладает потенциалом дальнейшего усиления операций влияния с использованием "Дезинформации".
2. Машинное обучение используется для осуществления влияния, такого как вмешательство в выборы, путем сбора, анализа и микро-таргетирования всех доступных данных, таких как раса, этническая принадлежность, идеология, демографические и географические условия.

Для распространения информации используются поддельные синтетические учетные записи, созданные ИИ, а также учетные записи, украденные в результате кибератак, и, таким образом, становится возможным распространять ложную информацию ускоренными темпами.

ЗАКЛЮЧЕНИЕ И БУДУЩАЯ ПОВЕСТКА ДНЯ:

Заключение и будущая повестка дня

- **Слияние искусственного интеллекта и кибероружия неизбежно**

→ Реализация более нацеленной дезинформации / злоумышленно-информационных атак

- **Оружие на базе искусственного интеллекта** может быть захвачено через киберпространство

- **Кибероружие, от которого нельзя ожидать сдерживания**

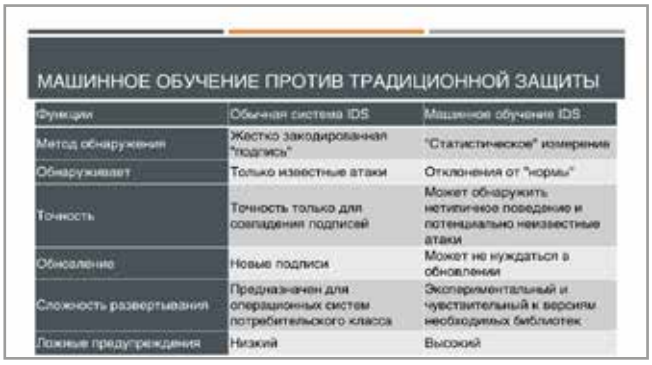
→ Трудно измерить физический ущерб в отношении военных, социальных, административных систем

Станислав Абаимов
Сеть «Ландау», Фонд им. Алессандро Вольта, Комо, Италия

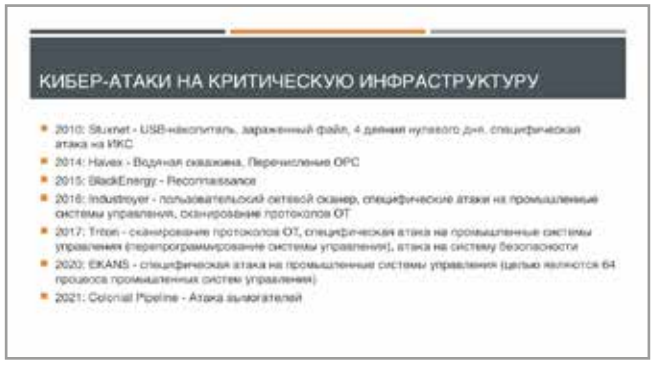
МАШИННОЕ ОБУЧЕНИЕ ДЛЯ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ В КРИТИЧЕСКИ ВАЖНЫХ ИНФРАСТРУКТУРАХ

ВСТУПЛЕНИЕ

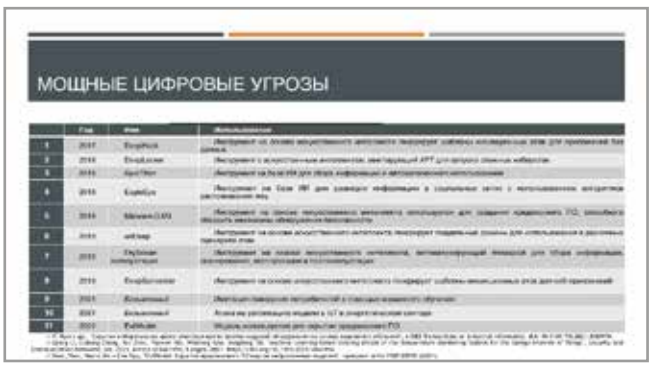
МАШИННОЕ ОБУЧЕНИЕ ПРОТИВ ТРАДИЦИОННОЙ ЗАЩИТЫ



КИБЕР-АТАКИ НА КРИТИЧЕСКУЮ ИНФРАСТРУКТУРУ



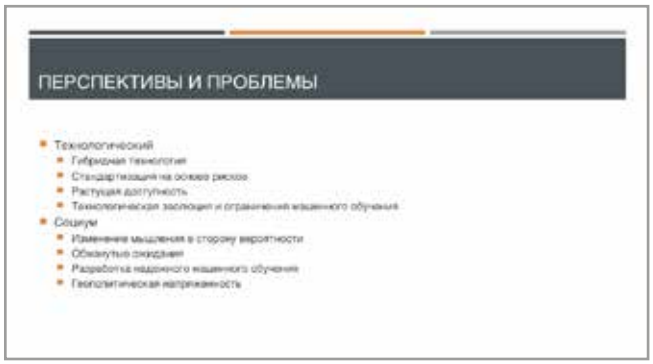
МОЩНЫЕ ЦИФРОВЫЕ УГРОЗЫ



КИБЕР-АТАКИ НА КРИТИЧЕСКУЮ ИНФОРМАЦИОННУЮ ИНФРАСТРУКТУРУ

МАШИННОЕ ОБУЧЕНИЕ ДЛЯ КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ

ПЕРСПЕКТИВЫ И ПРОБЛЕМЫ



СПАСИБО!

Жу Ликсин
Директор Института верховенства права в области кибербезопасности Академии развития науки и образования (КНР)

ПРАВОВОЕ МЫШЛЕНИЕ О МЕЖДУНАРОДНОМ СОТРУДНИЧЕСТВЕ В ОБЛАСТИ ЗАЩИТЫ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

1. ОСНОВА СОТРУДНИЧЕСТВА

Многие международные организации и многие страны уже уделили внимание построению национальных стратегий, законодательства и систем организованной защиты критической инфраструктуры и критической информационной инфраструктуры. Страны имеют схожие стратегические намерения по защите критической информационной инфраструктуры, и все они подчеркивают важность защиты критической инфраструктуры посредством международного сотрудничества. В то же время, основные страны создали систему приоритетной защиты критической инфраструктуры в законодательстве и приняли приоритетные меры защиты.

Например, в КОНВЕНЦИИ О МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ, инициатором которой стала Россия, в статье 5 “Основные принципы обеспечения международной информационной безопасности” и статье 6 “Основные меры по предотвращению военных конфликтов в информационном пространстве” упоминается защита информационной инфраструктуры.

В 2011 году Россия, Китай и другие страны ШОС (Шанхайской организации сотрудничества) совместно предложили Организации Объединенных Наций Международный кодекс поведения по информационной безопасности, в котором говорится, что каждая страна несет ответственность и имеет право на защиту информационного пространства и критической инфраструктуры от угроз, вмешательства и ущерба от атак.

Парижский призыв от 12 ноября 2018 года о доверии и безопасности в киберпространстве, защита отдельных лиц и инфраструктуры:

Принцип 1. Предотвращение и восстановление после злонамеренных кибердействий, которые угрожают или причиняют значительный, беспорядочный или системный вред отдельным лицам и критически важной инфраструктуре.

8 сентября 2020 года Китай также выдвинул Глобальную инициативу по безопасности данных, выступив за то, чтобы все страны выступили против использования информационных технологий для разрушения критической инфраструктуры других стран или кражи важных данных, а также против их использования для совершения действий, угрожающих национальной безопасности и общественным интересам других стран.

Что касается США, то политика и стратегия США сосредоточены на соглашениях между союзниками для защиты КИИ, возможно, против других стран и их критики.

2. ПРИОРИТЕТНЫЕ НАПРАВЛЕНИЯ МЕЖДУНАРОДНОГО СОТРУДНИЧЕСТВА В ОБЛАСТИ ЗАЩИТЫ КИИ

По этому вопросу я соглашаюсь с “КОНВЕНЦИЕЙ О МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ”, **Статья 5, пятый пункт:** каждое государство-участник имеет право устанавливать суверенные нормы и управлять своим информационным пространством в соответствии со своими национальными законами. Его суверенитет и законы распространяются на информационную инфраструктуру, расположенную на территории государства-участника или иным образом подпадающую под его юрисдикцию.

И статья 6, второй пункт: государства-участники предпринимают все необходимые шаги для предотвращения любых деструктивных информационных действий, исходящих с их собственной территории или использующих информационную инфраструктуру, находящуюся под их юрисдикцией.

Как правило, КИИ, расположенные на территории государства, в основном находятся в сфере действия суверенитета страны, их защита находится под ее юрисдикцией.

Итак, на мой взгляд, приоритетные направления международного сотрудничества в области защиты КИИ лежат в двух плоскостях:

2.1.КИИ в глобальном сообществе

2.1.1. В открытом море

В начале апреля 2018 года подводный кабель “Африканское побережье - Европа” был перерезан, что нарушило доступ к части сетей Сьерра-Леоне и национальной сети Мавритании, которая перешла в “офлайн” на два полных дня.

КИИ, находящаяся в открытом море, не подпадает под суверенную юрисдикцию государства, с другой стороны, она связана с информационной безопасностью нескольких стран.

2.1.2. Через космическое пространство

КИИ космического базирования является растущей частью КИИ государства. Международное воздушное пространство определяется как воздушное пространство за пределами территории и территориальных вод (обычно 12 морских миль) государств. Оно не простирается над государствами.

2.2. Данные КИИ

Исходя из ускоряющегося сближения физической критической инфраструктуры и информационных систем, а также скрытой способности аналитики больших данных к обеспечению безопасности и развитию, работа с данными в критической инфраструктуре становится главным приоритетом в защите безопасности киберпространства.

Сегодня, с ростом цифровой экономики, данные КИИ часто становятся важной целью для атак на КИИ. Защита данных критической инфраструктуры, особенно тех данных, которые пересекают границы, также должна стать приоритетом для международного сотрудничества КИИ.

2.2.1 Трансграничные финансовые данные

Для решения проблем соблюдения данных, с которыми сталкивается финансовая индустрия в условиях информатизации: во-первых, необходимо осуществлять международное сотрудничество, внедрять международные правила трансграничной передачи личной информации, уточнять требования и исключения для трансграничной передачи между собой, вести международный диалог по трансграничному поиску данных, уточнять правила экстерриториального поиска и сбора доказательств регуляторами. Во-вторых, исходя из предпосылки совершенствования правовой системы управления данными в отечественной финансовой отрасли, следует содействовать соблюдению требований глобального бизнеса на основе отечественной защиты персональной информации.

2.2.2. Данные о трансграничном трафике

1) Данные системы слежения за судами Автоматической идентификационной системы (AIS).
2) Данные GPS-подобных систем
3) Данные управления воздушным движением в международном воздушном пространстве (обычно за пределами 12 морских миль от национальных границ и над международными водами).

Многие страны зависят от этих систем и данных для выполнения таких функций, как определение местоположения и времени для критически важных общественных услуг – от торговли до аварийных служб и национальной безопасности.

2.2.3 Данные о трансграничном здравоохранении

С медицинской точки зрения, с одной стороны, медицинские данные людей связаны с общей безопасностью страны и здоровьем людей, поэтому их необходимо защищать. С другой стороны, цифровая медицинская экосистема, онлайн-консультации по медицинской информации, Интернет + больница, телемедицина, носимые устройства и другие приложения для управления здоровьем позволили человечеству вступить в эпоху медицинского лечения с использованием больших данных, а хранение и использование медицинских данных стало

более гибким. Защита этих данных также важна и сложна. Пандемия COVID-19 иллюстрирует важность международного сотрудничества в области лечения, которое также требует защиты важных трансграничных медицинских данных.

3. КАК ДЕЙСТВОВАТЬ ДАЛЬШЕ

На высоком уровне я предлагаю как можно скорее создать Международную комиссию по защите КИИ в рамках ООН. Определить международную критическую информационную инфраструктуру и связанные с ней данные, которые должны быть совместно защищены международным сообществом. И обеспечить безопасные и надежные стандарты для перемещения этих данных через границы, четкую и определенную совместную ответственность международного сообщества за защиту этих данных.

Джон К. Мэллори
Массачусетский технологический университет (США)

КИБЕРНОРМЫ И МЕРЫ УКРЕПЛЕНИЯ ДОВЕРИЯ ДЛЯ БИОБЕЗОПАСНОСТИ

ОБЗОР

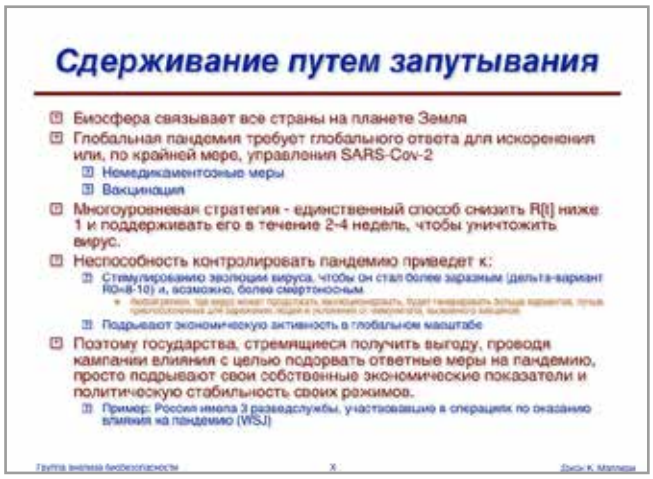
ВВЕДЕНИЕ

СООБРАЖЕНИЯ ПО ПОВОДУ МИРОВОГО ПОРЯДКА

РАЗВОРАЧИВАНИЕ МНОГОСТОРОННИХ ДИЛЕММ КИБЕРБЕЗОПАСНОСТИ: КИБЕРНЕТИЧЕСКОЕ ИЗМЕРЕНИЕ БОЛЕЕ ШИРОКОГО БАЛАНСА СИЛ

МЕЖДУНАРОДНЫЙ КОНТЕКСТ

СДЕРЖИВАНИЕ ПУТЕМ ЗАПУТЫВАНИЯ



Комментарий: Майкл Р. Гордон и Дастин Фольц, «Российская кампания дезинформации направлена на подрыв доверия к вакцинам Pfizer, другим вакцинам Covid-19, говорят американские чиновники», Wallstreet Journal, 7 марта 2021 года.

МЕЖДУНАРОДНОЕ ПРАВО

ЗАЩИТА ПО МЕЖДУНАРОДНОМУ ПРАВУ

ОПРЕДЕЛЕНИЕ НАЦИОНАЛЬНОЙ КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ БИОБЕЗОПАСНОСТИ

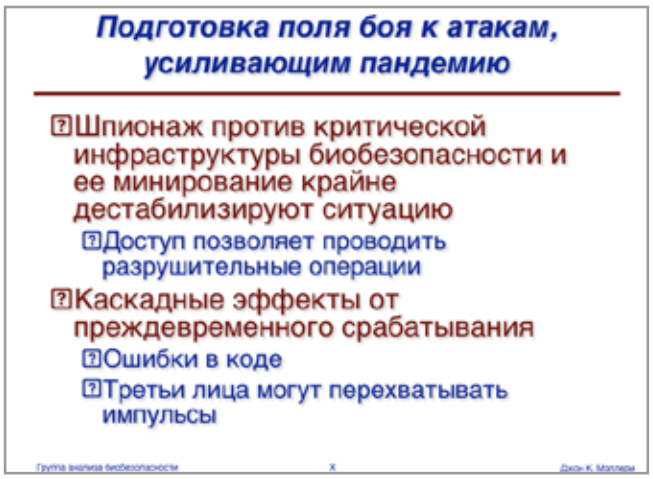
Комментарий: Ключевое различие заключается в том, являются ли они исключительно гражданскими, исключительно военными или промежуточными (гражданскими, которые могут быть актуальной инфраструктурой поддержки войны в случае вооруженного конфликта). Конечно, почти все это будет относиться к первой категории.

ОПРЕДЕЛЕНИЕ МЕЖДУНАРОДНОЙ КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ БИОБЕЗОПАСНОСТИ

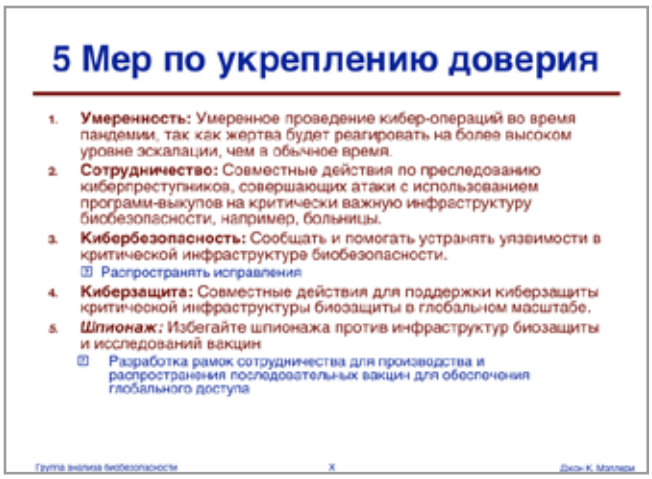
КЛАССЫ КИБЕРОПЕРАЦИЙ ПРОТИВ КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ БИОБЕЗОПАСНОСТИ

10 БИО-КИБЕР НОРМ

ПОДГОТОВКА ПОЛЯ БОЯ К АТАКАМ, УСИЛИВАЮЩИМ ПАНДЕМИЮ

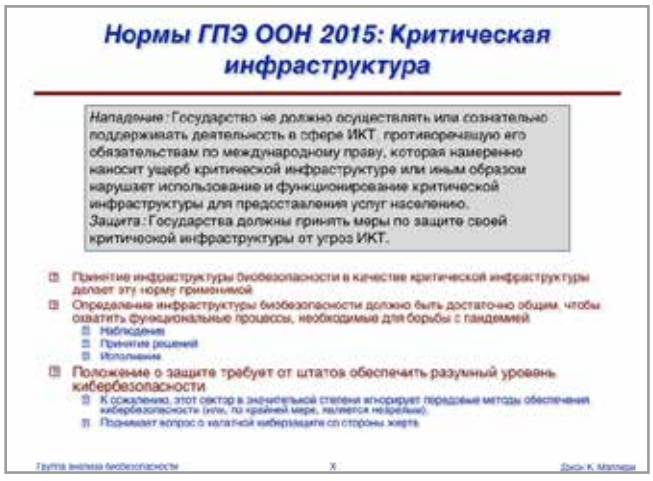


5 МЕР ПО УКРЕПЛЕНИЮ ДОВЕРИЯ

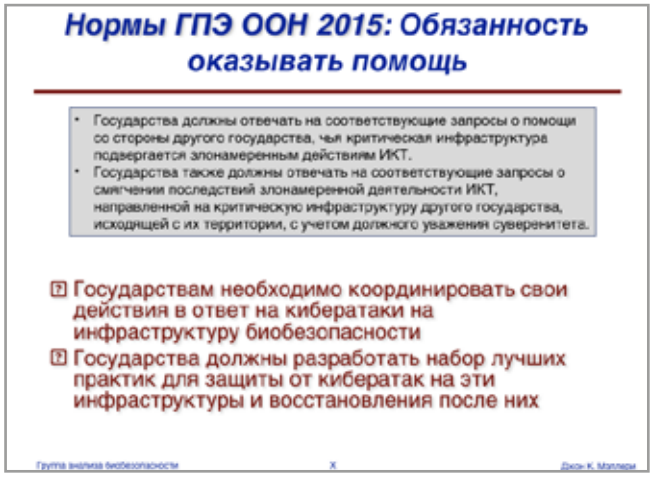


ЗАПРЕТИТЬ ПРЕКУРСОРНЫЕ ЭТАПЫ ЖИЗНЕННОГО ЦИКЛА АТАКИ НА КРИТИЧЕСКИ ВАЖНУЮ ИНФРАСТРУКТУРУ БИОБЕЗОПАСНОСТИ

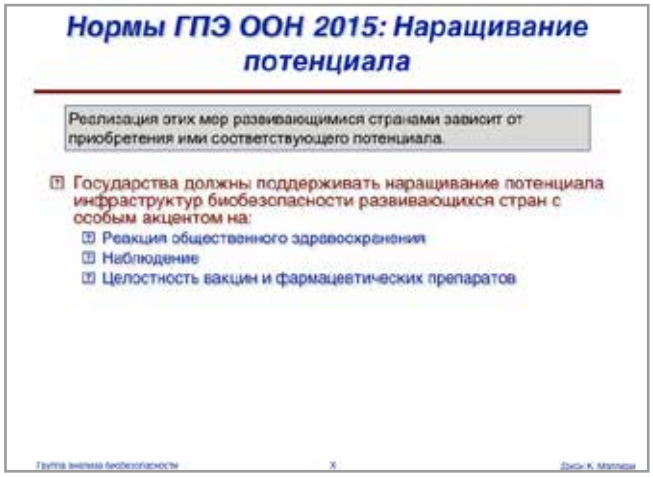
НОРМЫ ГПЭ ООН 2015: КРИТИЧЕСКАЯ ИНФРАСТРУКТУРА



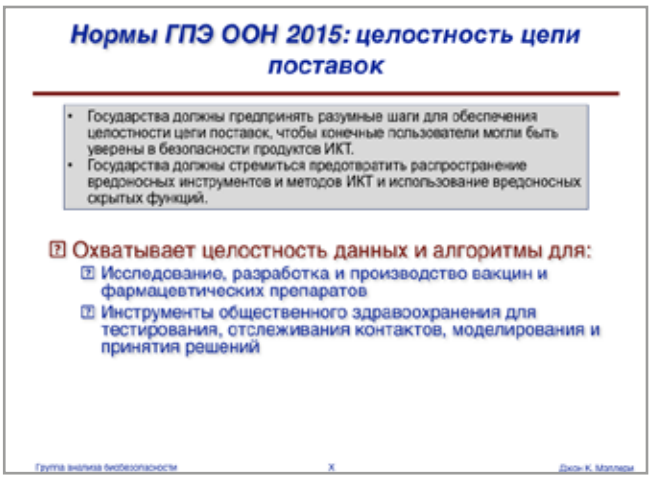
НОРМЫ ГПЭ ООН 2015: ОБЯЗАННОСТЬ ОКАЗЫВАТЬ ПОМОЩЬ



НОРМЫ ГПЭ ООН 2015: НАРАЩИВАНИЕ ПОТЕНЦИАЛА

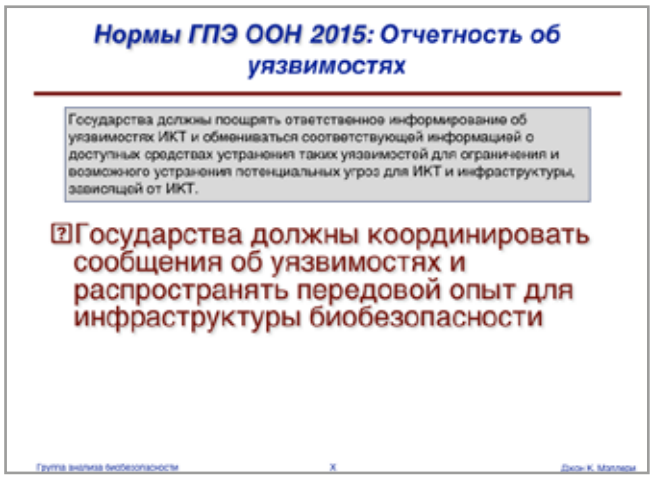


НОРМЫ ГПЭ ООН 2015: ЦЕЛОСТНОСТЬ ЦЕПИ ПОСТАВОК



ВЛИЯНИЕ НА ОПЕРАЦИИ ПРОТИВ РЕАГИРОВАНИЯ НА ПАНДЕМИИ

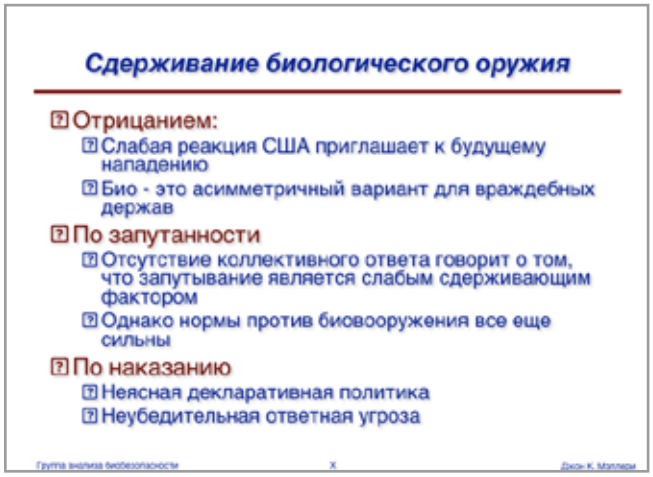
НОРМЫ ГПЭ ООН 2015: ОТЧЕТНОСТЬ ОБ УЯЗВИМОСТЯХ



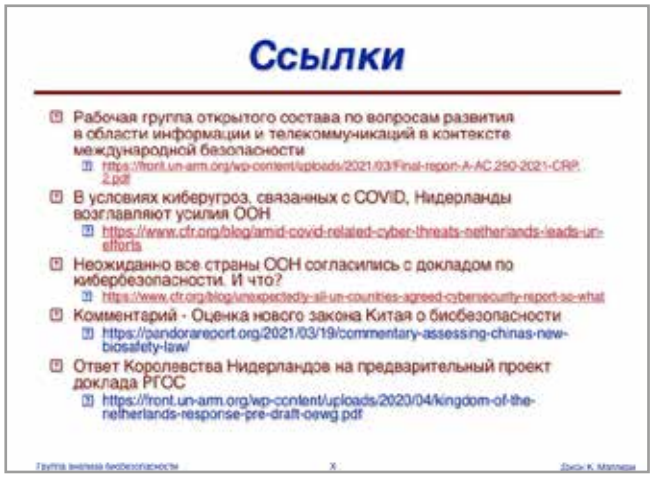
Комментарий: Джонатан Б. Такер и Эрин Р. Махан, Решение президента Никсона отказаться от американской программы наступательного биологического оружия, Вашингтон, округ Колумбия: Центр по изучению оружия массового уничтожения, Национальный университет обороны, октябрь 2009 года.

ВЫВОДЫ

СДЕРЖИВАНИЕ БИОЛОГИЧЕСКОГО ОРУЖИЯ

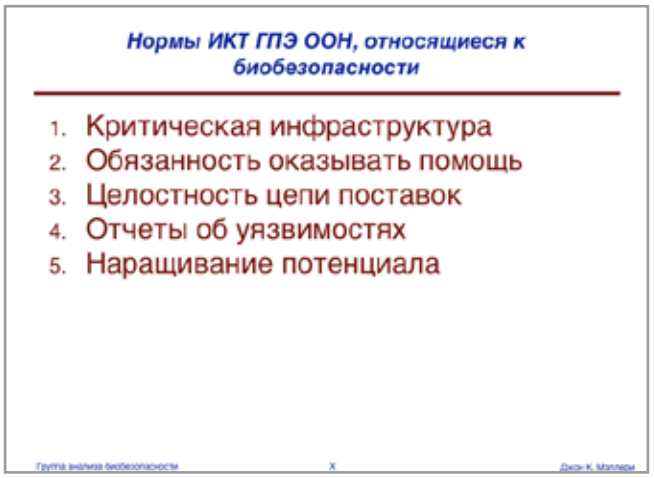


РЕЗЕРВНЫЕ СЛАЙДЫ: ССЫЛКИ



ИНФОРМАЦИОННЫЕ ОПЕРАЦИИ В ОБЛАСТИ БИОВООРУЖЕНИЙ ПРИЛОЖЕНИЕ:

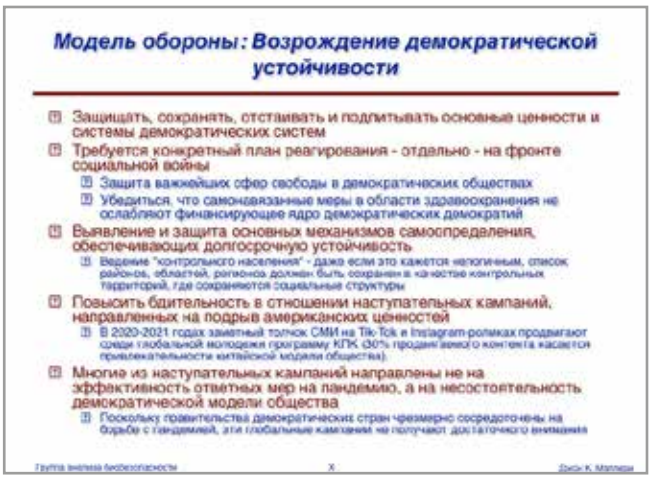
НОРМЫ ИКТ ГПЭ ООН, ОТНОСЯЩИЕСЯ К БИОБЕЗОПАСНОСТИ



ДВЕ КОГНИТИВНЫЕ ВОЙНЫ

МОДЕЛЬ УГРОЗЫ: ОБОЮДООСТРАЯ НАПРЯЖЕННОСТЬ

МОДЕЛЬ ОБОРОНЫ: ВОЗРОЖДЕНИЕ ДЕМОКРАТИЧЕСКОЙ УСТОЙЧИВОСТИ



10 КОГНИТИВНЫХ НОРМ

КРУГЛЫЙ СТОЛ № 3
МЕЖДУНАРОДНОЕ СОТРУДНИЧЕСТВО В ОБЛАСТИ ПРОТИВОДЕЙСТВИЯ ИНФОРМАЦИОННОЙ ПРЕСТУПНОСТИ

Модератор:
Мирошников Б.Н., к.ю.н., вице-президент ГК «Цитадель»,
член Президиума НАМИБ

Б.Н. Мирошников

К.ю.н., вице-президент ГК «Цитадель», член Президиума НАМИБ

Тема, которую предлагается обсудить на данном круглом столе, называется «Международное сотрудничество в области противодействия информационной преступности».

Тема как никогда актуальная и важная. Тысячу раз говорилось, что природа Интернета такова, что в нем большинство процессов могут носить трансграничный характер. К сожалению, и криминальная активность тоже. Прекрасно осознавая этот факт и успешно им пользуясь, (а также понимая разобщенность спецслужб и правоохранительных органов), преступники намеренно свое каждое преступление практически любой сложности делают трансграничным. То есть используют территории разных стран. Таким образом, преступление не может быть раскрыто самостоятельно или в одиночку без привлечения помощи коллег из стран, территория или сетевое пространство было использовано при совершении преступления. Таким образом, правоохранительные органы обречены на взаимодействие.

Это давно уже не открытие. Однако… МВД сообщило летом, что за январь-май 2021 года преступность в сфере информационных технологий выросла на 25% по сравнению с аналогичным периодом прошлого года. Количество зарегистрированных преступлений в ИКТ за полгода составило 271 тысячу. Доля киберпреступлений в общем объеме преступлений выросла до 26,8%, а год назад она составляла 21,7%. На 48,4% выросло количество преступлений, совершенных при помощи Интернета. На 40,1% увеличилось число преступлений с использованием компьютерной техники. По данным Банка России потери россиян от действий кибермошенников в 2020 году выросли в 1.5 раза по сравнению с 2019 годом и составили 9,8 миллиарда рублей.

Тот факт, что статистика киберпреступности ежегодно драматически растет и растет количество жертв и размер наносимого ущерба, говорит о том, что, похоже, предпринимаемых усилий недостаточно. А анализ причин, способствующих росту количества компьютерных преступлений, говорит о том, что одной таких причин является недостаточный уровень международного взаимодействия.

Именно эту тему, мы считаем, что надо активно обсуждать и вырабатывать меры преодоления этих недостатков. И я очень рад сообщить участникам форума, что обсудить эту проблему мы пригласили, а они согласились, опытных, компетентных специалистов из разных стран, и поэтому надеемся, что результаты круглого стола будут интересны и полезны.

Нельзя сказать, что до сих пор ничего не делалось на направлении противодействия криминальному использованию информационно-телекоммуникационных сетей и налаживания международного взаимодействия. Сегодня, в год проведения нашего с вами форума, мы можем вспомнить, что многим событиям и процессам отмечено 20 и более лет.

Давайте вспомним.

- 22 июля 2000 года главами государств и правительств «Группы восьми» была принята «Окинавская хартия Глобального информационного общества».
- А в России 9 сентября того же года была принята Доктрина информационной безопасности страны.
- 24 года назад в Уголовный кодекс России была введена Глава 28 «О компьютерных преступлениях»
- 23 года назад в структурах МВД России были созданы подразделения по борь-

бе с преступлениями в сфере высоких технологий (УБПСВТ МВД России, сокращенно Управление «Р»).

Международное сотрудничество правоохранительных органов с начала двухтысячных начала координировать подгруппа по киберпреступности Римско-Лионской группы. Римско-Лионская группа – это рабочий орган «G8», который изначально специализировался на проблематике противодействия терроризму и транснациональной организованной преступности. А оперативный обмен информацией для противодействия преступлениям в сфере информационных технологий стал осуществляться посредством международной сети национальных контактных пунктов, также созданной решением Восьмерки. Около 60 стран присоединились к этой сети, включая Россию. В России уполномоченным органом для обеспечения работы национального контактного пункта было определено Министерство внутренних дел, а внутри министерства – вновь созданное Управление по борьбе с преступлениями в сфере высоких технологий (УБПСВТ). Соответствующие подразделения по координации борьбы с киберпреступностью были образованы и активно заработали в структурах Интерпола и ОБСЕ.

А в ноябре 2001, совсем ровно двадцать лет назад, в Будапеште была принята Европейская конвенция по борьбе с киберпреступностью. Напомню, что Россия к ней не присоединилась. Хотя время от времени приходится сталкиваться с так называемыми «западниками», которые пытаются высказать упрек в адрес властей за неприсоединение к Конвенции. Или еще хуже: объяснить трудности в борьбе с киберпреступностью именно фактом неприсоединения – отсутствием нашей подписи под Конвенцией. Очевидно, они повторяют доводы сторонников Конвенции, которые были обрушены на мудрую и осторожную Россию. Надо сказать, что сама по себе Конвенция – неплохой и нужный в то время документ. Однако это для тех стран, у которых еще не было соответствующего законодательства, которые только приступали к организации борьбы с компьютерной преступностью. Для России, которая к 2001 году уже прошла эти этапы, присоединение к Конвенции явилось бы шагом назад. Кроме того, и главное, о чем не раз было заявлено на всех площадках, существование в тексте Конвенции статьи 32 Б делало ее совершенно неприемлемой для России, так как этот пункт содержал угрозу национальной безопасности.

При этом надо понимать, что Россия, как и многие другие страны, давно является участником двух и многосторонних соглашений о взаимной правовой помощи в борьбе с преступностью. А киберпреступность это же лишь частный случай преступности. События последующих лет, а именно – совместные расследования с правоохранительными органами разных стран, показали возможность такого эффективного взаимодействия и получения результатов.

В апреле 2006 года МВД России провело первую международную конференцию по борьбе с киберпреступностью и кибертерроризмом. Около 40 стран приняло в ней участие – страны СНГ, Великобритания, ФРГ, Франция, США, Китай и многие другие. Такое широкое представительство было признанием опыта и достижений российских киберполицейских в борьбе с высокотехнологичной преступностью.

Десятки аналогичных мероприятий регулярно стали проходить по всему миру, образовывая прекрасные тематические площадки для обмена опытом и налаживания контактов и взаимодействия. Огромный вклад в развитие международного сотрудничества внес ежегодный форум в Гармиш-Партенкирхене «Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности», на разнообразных площадках которого традиционно много внимания уделялось теме борьбы с киберпреступнности. На ее базе образовался международный Консорциум, объединивший авторитетные научные и учебные заведения разных стран, что является отличным инструментом для продвижения вперед лучшего опыта и научных идей. Наш сегодняшний форум – продолжение этой важной и замечательной традиции на Московской земле.

К сожалению, приходится констатировать, что к настоящему времени международные контакты и взаимодействие между уполномоченными структурами ослабли. Причин тому много – от коронавируса до политиче-

ских. В любом случае это на руку преступным группировкам и отдельным киберпреступникам, а криминогенная ситуация от этого продолжает ухудшаться.

Технический прогресс идет вперед огромными темпами, чаще всего предоставляя новые услуги гражданам, причем именно в глобальном масштабе. Это, прежде всего, услуги в области коммуникаций и в области финансов. Удаленное банковское обслуживание, развитие платежных систем, «умные и безопасные города» и так далее – все эти достижения прогресса таят в себе много возможностей для преступного мира, и мы видим, как развивается преступность в телекоммуникационной сфере и финансовом секторе. Одни шифровальщики и кибермошенники чего стоят! Плюс добавьте к этому еще массовые утечки персональных данных во всем мире.

Поэтому возвращаюсь к мысли, которую уже высказал несколько выше – мы обречены на взаимодействие. Нам нужны не только заверения в благих намерениях, а конкретные механизмы, обеспечивающие обмен информацией о преступлениях, совместные действия по расследованию и пресечению правонарушений, розыск и задержание преступников, криминалистические исследования, добывание и закрепление улик, а также подготовка и обучение специалистов, способных противостоять современному киберпреступнику. Причем отмечу, что качественное взаимодействие правоохранительных органов в области противодействия киберпреступности имеет идущие последствия, помимо собственно сдерживания преступников. Эти процедуры и инструменты взаимодействия в силу их способности раскрывать различные процессы, события, делать прозрачной телекоммуникационную среду, видеть или выявлять участников всевозможных инцидентов на самом деле могут служить еще и сдерживанию развязывания информационных операций во всем мире и в целом обеспечению международной информационной безопасности. Ведь хорошо известно, что информационные акции и операции, гибридные войны и разные злонамеренные происшествия зачастую выдаются за проделки хулиганов или действия индивидуальных преступников. Так что работа на этом направлении имеет огромное значение для формирования глобальных механизмов обеспечения международной информационной безопасности.

Спасибо за внимание.

Успехов вам!

Чарльз Барри
Независимый консультант по кибербезопасности, США

МОГУТ ЛИ ГОСУДАРСТВА УСМИРИТЬ КИБЕРПРЕСТУПНОСТЬ?

Приветствие и введение

Господин председатель, спасибо за ваше представление. Я также искренне благодарю профессора Владислава Шерстюка, президента Национальной Ассоциации международной информационной безопасности, и саму Ассоциацию за приглашение выступить сегодня виртуально на этом важном мероприятии. Я сожалею лишь о том, что не могу лично присутствовать вместе с вами во впечатляющем Актовом зале Дипломатической академии Министерства иностранных дел Российской Федерации. Тем не менее, для меня действительно большая честь принять участие в Круглом столе 3 по сотрудничеству в борьбе с киберпреступностью в рамках XV Международного форума.

Мои сегодняшние выступления на Форуме, как всегда, являются лишь отражением моего личного анализа состояния международных усилий по противодействию киберпреступности. Таким образом, мои оценки по этой теме не связаны с каким-либо учреждением, организацией или агентством, государственным или частным, в США или где-либо еще.

Давайте начнем с того, что должно быть очевидным: все мы, занимающиеся серьезным делом борьбы с киберпреступностью, должны отвергать такие преступные действия не меньше, чем любое другое беззаконие. Мы признаем, что киберпреступность причиняет боль всем нам, и эта боль становится все глубже почти ежедневно. Кибербеззаконие подрывает информационную безопасность. Оно подрывает доверие бизнеса и правительств к полезности сетей. Оно обходится международному сообществу во многие триллионы долларов США ежегодно в виде потерь производительности, выкупа, защиты систем безопасности и правоохранительных органов. Это подрывает доверие общества к Интернету, который стал самостоятельной товарной услугой мирового масштаба. Доступ к интернету стал необходимым для понимания столь многих аспектов нашей жизни, что некоторые утверждают, что он стал одним из основных прав.

Конечно, киберпреступность не возникает из воздуха. Она совершается лицами вне закона, действующими с территории одного или нескольких суверенных государств, да, включая те самые государства, которые участвуют в этом Форуме. Каждое суверенное государство имеет конечную власть привлекать к ответственности преступников, находящихся под его юрисдикцией. Государство может пресекать все виды преступлений в пределах своих границ, включая киберпреступность. Тем не менее киберпреступность практически полностью захватила эту новую и перспективную область. Сегодня каждая новостная лента информационного домена предоставляет нам постоянный поток сообщений о киберпреступлениях – преступлениях, инициированных с территории кого-то из нас. Сложность, отчасти, заключается в том, что отслеживание киберпреступлений требует международного сотрудничества. Киберпреступность не признает физических границ и почти незаметно пересекает национальные юрисдикции.

Что мы, участники Форума, можем сделать или предложить нашим правительствам сделать, чтобы остановить эту разлагающую, дорогостоящую волну преступлений? Будем ли мы только еще раз пересказывать последнюю версию длинного списка киберпреступлений? Будем ли мы, образно говоря,

еще раз «срывать маски» в насмешливом гневе по поводу ущерба, который киберпреступники наносят рынкам и обществам, расходов, которые они налагают на всех нас? Разве мы еще не достаточно написали и сказали о вышедшей из-под контроля эпидемии киберпреступности? Разве мы уже не знаем эту проблему достаточно хорошо, чтобы еще раз сказать себе: хватит?

Нет, мы собрались здесь не для того, чтобы перечислять недавние атаки с использованием программ-выкупов, такие, как последняя атака REvil на американскую компанию Kaseya (июль 2021 года)[1], атака Conti на японскую компанию JVC Kenwood (сентябрь 2021 года)[2] или любые другие киберпреступления. Мы должны взять на себя обязательство решительно двигаться вперед. Вопросов, на которые мы должны ответить, три. Во-первых, почему государства, из которых совершаются такие атаки, не могут или не хотят усмирить киберпреступность в пределах своих границ? Во-вторых, почему государства-жертвы и государства, потенциально укрывающие киберпреступников, так неохотно работают вместе и обмениваются информацией, чтобы привлечь киберпреступников к ответственности? И, наконец, почему государства так не решаются договориться и внедрить более сильные международные нормы для борьбы с киберпреступностью на глобальном уровне? Это те действия, которые все государства должны предпринять с истинной целью, чтобы мы смогли укротить киберпреступность. Тем не менее, существуют существенные и реальные препятствия на пути к существенному прогрессу. Мы должны не только говорить об этих проблемах. Мы должны взять на себя обязательство предпринять внутренние и коллективные действия, необходимые для того, чтобы остановить постоянную, нарастающую волну киберпреступности.

Обсуждение основных моментов

Другие докладчики затронут важные темы военной кибердеятельности и шпионажа. Здесь мы хотим сосредоточиться на преступных атаках, которые наносят прямой ущерб людям и коммерции, то есть сетям и системам, которые непосредственно влияют на наших граждан и национальный образ жизни. В последние годы по всему миру прокатилось цунами атак с использованием вымогательского ПО, направленного на мясокомбинаты, сети продуктовых магазинов, сети здравоохранения, больницы, электросети, транспортные системы, органы власти небольших городов и многие другие объекты и учреждения, критически важные для повседневной жизни[3]. Масштабы и изощренность киберпреступлений в каждой из этих областей растут угрожающими темпами.

По каким причинам государствам не удается привлечь преступников к ответственности на своей территории? Конечно, может быть так, что у государства не хватает разведывательных или следственных возможностей для выявления киберпреступников. В таких случаях государства прибегают к помощи международных организаций, таких как МСЭ; частных охранных компаний, таких как Kaspersky (Россия), SecDev (Канада) или Mandiant (США); или обращаются за помощью к странам-партнерам. Государства также могут принять решение о защите, то есть намеренно защищать киберпреступников в пределах своих границ, поскольку такие преступники обеспечивают предполагаемые асимметричные преимущества, включая финансовую или политическую выгоду для принимающего государства. По-

1 Атака на американского поставщика программного обеспечения Kaseya, осуществленная в июле 2021 года печально известной связанной с Россией группой разработчиков программ-вымогателей REvil, по оценкам, затронула до 2 000 глобальных организаций. REvil использовала уязвимость в инструменте удаленного управления компьютерами Kaseya для проведения атаки, последствия которой продолжались несколько недель. См. Атака Kaseya ransomware: Хронология I CSO Online.

2 Японский производитель электроники JVCKenwood сообщил, что 22 сентября серверы его торговых компаний в Европе были взломаны программой Conti ransomware, в результате чего было похищено 1,7 Тб данных, а сумма выкупа составила 7 миллионов долларов (США). Conti - это русскоязычная группа вымогателей, жертвами которой, по сообщениям, стали более 400 организаций по всему миру, из которых 290 находятся в США. Conti атакуют, проникая в сети через жертв фишинговых электронных писем (вредоносные ссылки или вложения) или украденные/взломанные учетные данные протокола удаленного рабочего стола. См. Сообщается, что группа вымогателей Conti похитила 1,5 ТБ данных у компании JVCKenwood(eccouncil.org)

3 См. объяснение вирусов Peyya/NotPetya, давно распространяющихся с 2016 года, на странице What Is Petya and Not Petya Ransomware? I McAfee. Другой пример – обнаружение компанией FireEye в декабре 2020 года атаки на Solarwinds с помощью вредоносного ПО, предположительно российского

следнее обоснование может быть особенно привлекательным для принимающей стороны, если киберпреступники успешно нарушают экономику или промышленность противника. В этих случаях таким государствам будет трудно внести свой вклад в укрощение киберпреступности.

По каким причинам государства не хотят действовать совместно в борьбе с киберпреступностью? Возможно, одна из причин заключается в том, что стоимость киберпреступлений для экономики большинства государств еще не настолько возросла, чтобы преодолеть их недоверие к совместным действиям. По прогнозам Cybersecurity Ventures, в 2021 году стоимость киберпреступлений во всем мире составит 6 триллионов долларов США[4]. Это много, но этого может быть еще недостаточно, чтобы побудить государства преодолеть свое нежелание сотрудничать в борьбе с киберпреступностью. Хотя затраты на борьбу с киберпреступностью сегодня по любым меркам астрономические, похоже, что они еще не достигли уровня, достаточного для того, чтобы подтолкнуть государства к более глубокому сотрудничеству. Это должно измениться, поскольку стоимость этих преступлений продолжает расти.

Отвечая на вопрос, государства действительно пытались договориться о международных нормах киберповедения в отношении киберпреступности, а также других проблемных областей, включая применение законов вооруженных конфликтов (ЗВК) к деятельности в киберпространстве. Соглашения (более подробно рассмотренные ниже) позволили добиться определенного прогресса. Однако потребность в них велика, а результаты слишком незначительны. Страны соглашаются лишь рекомендовать всем государствам соблюдать общие нормы. Впоследствии лишь немногие государства проводят внутреннюю политику для обеспечения соблюдения рекомендованных норм. Иногда соглашения со временем ослабевают, поскольку ключевые государства впоследствии возражают против определенных положений. В целом, нормы, которые были согласованы коллективно, представляют собой результат "наименьшего общего знаменателя", который не способен уменьшить воздействие киберпреступников. Такие усилия ни в коем случае не должны быть прекращены. Однако, если они не смогут выработать более сильные нормы, которые будут применяться странами, международные соглашения будут все больше отставать в гонке по пресечению киберпреступности.

Более широкий контекст межгосударственных отношений также может влиять на заинтересованность государств в сотрудничестве по вопросам киберпреступности. Незаконный захват Крыма и военное вторжение в суверенную Украину в 2014 году завели в тупик российско-американские отношения и многие другие сферы. Многие другие внутренние и внешние факторы, включая торговлю, дипломатию санкций, энергию как оружие, и даже отношения между лидерами влияют на потенциал достижения новых или более глубоких договоренностей по совместной борьбе с преступностью. Есть ли потенциал для того, чтобы борьба с преступностью была отгорожена кольцом от других напряженных ситуаций? До сих пор этого не удалось достичь на низком уровне.

Еще одной важной проблемой является деликатная тема государственного суверенитета. Государства всегда настороженно относятся к любому намеку на посягательство на их суверенитет, особенно при рассмотрении вопроса о присоединении к международным соглашениям. Будапештская конвенция о киберпреступности 2001 года[5] является хорошим примером. Сегодня Конвенцию ратифицировали 65 государств. Однако Россия, Индия и другие крупные державы последовательно отказываются от ее принятия на том основании, что ее положения будут ущемлять их национальный суверенитет. Аналогичным образом, некоторые державы отказываются присоединяться к соглашениям, в разработке которых они не принимали участия.

В августе 2021 года Россия предложила ООН «Конвенцию ООН о противодействии использованию информационно-коммуникационных технологий в преступных целях». США неофициально заявили, что они могут[6] быть настроены на переговоры по россий-

4 Глобальный ущерб от киберпреступлений к 2021 году достигнет $6 трлн в год (cybersecurityventures.com)

5 См. раздел "Действия против киберпреступности" (coe.int)

6 Резолюция была принята в мае 2021 года единогласно после интенсивного обсуждения и трех одобренных поправок, две из

скому предложению, наряду с другими инициативами, когда речь пойдет о повестке дня ООН в 2022 году. Новая конвенция по киберпреступности будет включать в себя положения существующих соглашений, в том числе Будапештского. Такое начинание стало бы позитивным событием и приоритетом для международного сотрудничества в противодействии информационной преступности.

Государства могут и должны изучить возможность расширения сотрудничества в борьбе с киберпреступностью посредством двусторонних и многосторонних отношений в области правоохранительной деятельности, технической помощи и обучения технических экспертов. В дополнение к межгосударственным режимам существуют агентства по координации правоохранительной деятельности в Европе (Европол) и на глобальном уровне через Интерпол. Эти хорошо зарекомендовавшие себя организации недавно были реорганизованы и теперь имеют центры по борьбе с киберпреступностью и обмену киберинформацией. Эти агентства и программы могут оказывать взаимную помощь в расследовании информационных преступлений. Аналогичным образом региональные организации, такие как ЕС, ОАГ, АСЕАН, ОБСЕ и ШОС, также помогают своим членам реагировать на угрозы киберпреступности.

Отсутствие полезного международного доверия, стремление спрятаться за национальный суверенитет, когда приходится идти на компромисс, рассеянная реальность бремени расходов, связанных с преступностью, политическая завеса сопротивления всему, что «создано не здесь», политическое влияние реляционных трений, не связанных с рассматриваемым вопросом, и вполне реальный факт, что некоторые государства прямо или косвенно занимаются киберпреступностью – все эти факторы препятствуют углублению международных соглашений по контролю над киберпреступностью. Предсказуемым результатом стали лишь добровольные, необязательные и, откровенно говоря, довольно мягкие нормы. Напротив, все государства сталкиваются с неумолимой и нарастающей волной международной киберпреступности. Некоторые государства устанавливают так называемые «горячие линии» между агентствами кибербезопасности друг друга, но потом эта линия редко используется. Государства вкладывают значительное время и ресурсы в соглашения ООН, которые постоянно оказываются слабыми или невыполнимыми.

Основные международные усилия по борьбе с (*среди прочего)* киберпреступностью на сегодняшний день

С признательностью послу Андрею Крутских[7] и нашим российским коллегам ООН с 2004 года реализует концепцию Группы правительственных экспертов (ГПЭ) по информационной безопасности. Эти группы – первоначально 15, а затем 25 членов ООН – подготовили несколько докладов для Генеральной Ассамблеи, последний из которых был представлен в мае этого года. Эти отчеты включали ряд «добровольных, необязательных норм», которым государствам рекомендуется следовать в отношении информационной безопасности. Некоторые из них затрагивают аспекты киберпреступности, например, нормы 13 (a) – 13 (d)[8].

Новая рабочая группа ООН открытого состава (РГОС) также завершает свою работу в 2021 году. РГОС – это еще одна российская инициатива, направленная на достижение консенсуса в отношении добровольных норм поведения государств в киберпространстве. Разница в том, что РГОС открыта для всех членов ГА ООН, а не только для 25, а также приглашает заинтересованный международный и частный сектор. И ГЭП ООН, и РГОС предназначены для продолжения работы, поэтому остается надежда на дальнейший прогресс в области норм[9].

которых требовали занесения в протокол голосования. Генеральная Ассамблея принимает резолюцию, определяющую условия для переговоров по договору о киберпреступности, на фоне опасений по поводу "поспешного" голосования в ущерб дальнейшим консультациям I Освещение заседаний и пресс-релизы (un.org)

7 См. Андрей Крутских назначен специальным представителем Президента РФ по вопросам международного сотрудничества в области информационной безопасности – Президент России (kremlin.ru). Я знаю посла Крутских более 10 лет по форуму NAIIS Garmisch и считаю его проницательным, дипломатичным профессионалом в области информационной безопасности и другом.

8 См. документ 76-й сессии ГА ООН A/76/135 от 14 июля 2021 года (на английском языке). Раздел III "Нормы, правила и принципы ответственного поведения государств", подпункты III a – III d включительно.

9 Хорошее описание и резюме процессов ГПЭ ООН и РГОС см. в разделе ГПЭ ООН и РГОС I GIP Digital Watch Наблюдение за управлением интернетом и цифровой политикой

Некоторые государства, включая США, также разработали стимулирующие методы выявления и пресечения источников растущей волны дезинформирующих веб-сайтов и сообщений. Дезинформация часто направлена на элементы избирательных процессов в демократических обществах. В свою очередь, доверие общественности к результатам выборов может быть подорвано. За последние пять лет дезинформация стала серьезной проблемой не только в США, но и во всей Европе, включая Россию. Виновниками злонамеренных кампаний по дезинформации являются как внутренние, так и внешние источники, связанные с затрагиваемой страной. Международное сообщество не может мириться ни с тем, ни с другим.

Резюме основных положений и рекомендаций для совместных действий

Только страны, действующие сообща, могут найти решение для нынешнего неприемлемого уровня киберпреступности. Тем не менее, публичные свидетельства часто говорят о том, что государства сами причастны к этому, что они сопротивляются соглашениям, которые запрещают использование кибертехнологий для дестабилизации державы-противника. Другие свидетельства говорят о том, что государства используют марионеточные преступные предприятия для подрыва других держав. Видя выгоду в деятельности киберпреступников, они не склонны арестовывать лиц, совершающих такие преступления на своей территории.

Все члены ГА ООН во главе с пятью постоянными членами Совета Безопасности должны резко усилить реализацию согласованных норм ГПЭ ООН и РГОС, связанных с борьбой с киберпреступностью. В частности, давайте одобрим:

- Агрессивное задержание и преследование киберпреступников, действующих на территории каждого из наших штатов.
- Более интенсивный обмен информацией о киберпреступниках. Это требует регулярного использования каналов связи.
- Незамедлительное внедрение рекомендованных норм, связанных с киберпреступностью
- Инвестиции в новые соглашения, которые действительно остановят киберпреступность, включая правоприменение и последствия для преступников. Это одобрение должно начаться прозрачно и без предварительных условий для любого государства в январе 2022 года, как это единогласно согласовано в резолюции ГА ООН A75/L.87/Rev.1 «Противодействие использованию информационно-коммуникационных технологий в преступных целях».

Предлагаемые новые переговоры по резолюции A75/L.87/Rev.1 плюс продолжающиеся более широкие обязательства РГОС и ГПЭ ООН должны быть направлены на значительное улучшение слабых соглашений, которые были достигнуты за последние 15 с лишним лет. Мы знаем, чего необходимо достичь. Страны должны стремиться к повышению взаимного доверия. Новая конвенция может стать возможной, если государства смогут вести переговоры с общим глобальным благом в качестве цели. В любом случае, если они хотят остановить стремительный рост киберпреступности, им придется принять вызов сотрудничества. Если они намерены укротить киберпреступность, время для активизации международного сотрудничества настало.

Н.М. Гудков
Генеральная прокуратура Российской Федерации

ИНФОРМАЦИОННО-СПРАВОЧНЫЕ МАТЕРИАЛЫ ПО ВОПРОСУ ОБЕСПЕЧЕНИЯ КООРДИНАЦИИ ДЕЙСТВИЙ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ В СФЕРЕ ПРОТИВОДЕЙСТВИЯ ИКТ ПРЕСТУПНОСТИ

Развитие информационно-коммуникационных технологий сопряжено не только с прогрессом, что обусловило их повсеместное проникновение во все сферы общественной жизни, но и с активной противоправной деятельностью злоумышленников в целях личного обогащения, дискредитации граждан и государства, незаконного оборота запрещенных к обороту средств и нелегальной информации.

Распространенность преступлений в данной среде, число которых в 2020 году достигло 510 тыс., увеличившись на 70% (а в первом полугодии 2021 года – на 20%, превысив 270 тыс.), вызывает серьезную обеспокоенность.

Учитывая трансформацию способов шифрования данных, максимально повышающих анонимность злоумышленников, новые технологии, дающие доступ к неограниченным ресурсам, всё чаще выступают средством совершения самого широкого круга преступлений, превращая любую криминальную деятельность в сверхдоходную.

Прирост отмечается в отношении вымогательств, оборота наркотиков, распространения сведений составляющих охраняемую законом тайну, порнографии, актуальны посягательства на неприкосновенность частной жизни, подделка документов. По-прежнему, с использованием ИКТ совершается большое количество преступлений экстремистской и террористической направленности. Очень часто ИКТ используется злоумышленниками в отношении несовершеннолетних.

Однако основной массив преступлений данной категории составляют дистанционные хищения, совершенные с банковских карт, в частности в сети «Интернет» и при помощи средств мобильной связи.

Значительное количество преступлений продолжает совершаться с использованием различных интернет-сервисов для размещения объявлений (Avito и др.), социальных сетей, а также «фишинга». В большинстве случаев при этом, используя методы социальной инженерии, преступники становятся владельцами идентификационных данных потерпевшего или получают доступ к их личным кабинетам в различных мобильных сервисах.

Например, только за один квартал отдельными центрами реагирования на компьютерные инциденты блокируется более 5 тыс. фишинговых ресурсов и это далеко не предел. Обобщение подобных лже-сайтов свидетельствует о том, что преступники умело встраиваются в новостную повестку.

Многие такие ресурсы связаны с торговлей лекарствами, вакцинацией, выплатами социальных пособий. Также осуществлялась активная рассылка фишинговых писем от имени авторитетных международных организаций, или предлагающих простой и быстрый способ заработка, в том числе связанного с оборотом криптовалюты. Отмечен прирост числа сайтов-клонов известных торговых площадок, мошеннических предложений при онлайн-продажах. Сами вредоносные рассылки стали более таргетированными и потому чаще вызывали доверие у получателей.

Изложенное диктует необходимость повышения эффективности противодействия

ИКТ преступности, что бесспорно относится к стратегическим направлениям деятельности правоохранительных органов. И одной из важнейших задач в этом случае является совершенствование законодательства в целях усиления защиты граждан и общества от преступных посягательств.

Уголовно-правовые запреты должны отвечать существующим реалиям и в полной мере обеспечивать соразмерную ответственность за совершение того или иного преступления. При этом в случае динамично развивающихся видов преступности, что особенно актуально для цифрового пространства, конструкция уголовно-правовых норм должна не просто учитывать складывающуюся криминогенную обстановку, но и, в идеале, заглядывать в будущее, предсказывая в своей фабуле возможные опасные варианты развития методов и средств применения информационно-коммуникационных технологий в противоправных целях.

Подобный подход взят за основу при подготовке представленного Российской Федерацией проекта Конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях.

При этом, что касается национальных уголовно-правовых запретов, то ими в настоящее время охватываются основные варианты правонарушений в рассматриваемой сфере.

Уголовным кодексом Российской Федерации предусмотрена ответственность за ряд специальных составов, криминализирующих такие деяния как: мошенничество в сфере компьютерной информации; неправомерный доступ к компьютерной информации во всех его проявлениях; создание, использование и распространение вредоносных программ; посягательства на критическую информационную инфраструктуру, а также нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.

Кроме того, совершение преступления с использованием такой информации и сетей рассматривается в целом ряде составов преступлений в качестве квалифицирующего или отягчающего наказание признака, в частности в сфере незаконного оборота наркотиков, сведений о частной жизни и иных охраняемых законом данных, экстремизма, терроризма и других.

Озвученные данные не оставляют сомнений в том, что преступность очень быстро приспосабливается к меняющимся условиям. И очевидно, что злоумышленники будут расширять свою деятельность в рамках глобальной виртуальной криминальной сети, не знающей ни границ, ни юрисдикции, для чего собственно и была принята Резолюция Генассамблеи ООН 74/247.

Необходимо подчеркнуть, что в Российской Федерации борьба с преступностью рассматривается как комплексное явление, включающее в себя не только поиск виновных, привлечение их к ответственности, но и меры, направленные на предупреждение преступлений

С учетом изложенного перед органами прокуратуры, как перед главным координатором всей правоохранительной системы, поставлена задача по оперативному противодействию угрозам в цифровом пространстве, использованию современных технологий для противодействия рассматриваемым преступлениям.

В июле прошлого года в рамках Координационного совещания руководителей правоохранительных органов страны выработан комплекс мероприятий, направленных на совершенствование методов и способов выявления, раскрытия и расследования ИКТ преступлений, а также их предупреждения.

Внимание акцентировано на внедрении компьютерно-криминалистических инструментов в области информационной безопасности.

Прорабатывается вопрос совершенствования автоматизированных поисковых систем, в том числе интеграции с существующими базами на основе искусственного интеллекта, а также расширения их функционала.

Такие системы позволяют выявлять серийные преступления, совершенные в разных регионах страны в отношении различных потерпевших, а также выявлять всех задействованных в мошеннических схемах злоумышленников.

Например, по одному из раскрытых УМВД по Московской области преступлений в сфере банковского мошенничества с помощью такой системы была установлена причаст-

ность лица, его совершившего, к аналогичным действиям в отношении более 400 человек на территории 44 субъектов Российской Федерации, выявлены соучастники преступной деятельности, также проживающие в разных регионах.

В других случаях, следователями МВД по Удмуртской Республике в 2020 г. соединены в одном производстве имеющие признаки серийности 240 уголовных дел, 13 дел на 166 преступных эпизодов в отношении 30 обвиняемых направлены в суд. В ноябре 2020 г. следственными органами МВД по Пермскому краю завершено производством уголовное дело по обвинению К. и Г. в совершении 40 преступлений в отношении жителей различных регионов России. Обвиняемые обзванивали потерпевших, представлялись сотрудниками службы безопасности банка, сообщая ложную информацию о проблемах с банковской картой, похищали денежные средства со счетов данных лиц.

Прорабатываются механизмы фильтрации подменных телефонных номеров, оперативной блокировки номеров, с использованием которых осуществлялись мошеннические действия, а также формирование соответствующих черных списков абонентских данных для смартфонов.

Кроме того, в развитие обозначенных ранее целей созданы и продолжают формироваться на региональном уровне специализированные подразделения правоохранительных органов по выявлению и расследованию преступлений в сфере ИКТ, не раз доказавшие свою эффективность в борьбе с рассматриваемыми противоправными деяниями.

Подобным положительным примером является реализованный комплекс скоординированных правоохранителями мероприятий в 11 субъектах Российской Федерации, итогом которых стало задержание 30 активных членов и руководителей хакерской ОПГ, а также прекращение функционирования более 90 интернет магазинов, объединенных в единую информационную систему, предназначенную для оборота запрещенных предметов.

Итогом такой деятельности служит увеличение раскрытия обозначенных преступлений. В частности в отчетном периоде, как и прежде, зафиксирована положительная динамика (рост в 2 раза) по направлению уголовных дел в суд.

В качестве положительного примера можно привести расследование уголовного дела, возбужденного по признакам преступления, предусмотренного ч. 2 ст. 273 УК РФ.

В ходе расследования уголовного дела установлено, что 7 участниками организованной группы, в период с 2017 по 2018 создали и распространили неопределенному кругу лиц на территории различных регионов России более 2 тыс. экземпляров компьютерных программ «HEUR:Trojan», заведомо предназначенных для несанкционированных модификации и копирования компьютерной информации, при этом извлекли доход на общую сумму не менее 4 млн рублей.

В течение полутора лет проводилась объемная компьютерно-техническая судебная экспертиза в связи со многочисленными объектами, в ходе которой установлено наличие экземпляров компьютерных программ, их исходных кодов, сведений о получении и распределении доходов от преступной деятельности, а также история переписки между членами организованной группы.

С целью обеспечения гражданского иска и возможной конфискации имущества и по обеспечению исполнения наказания в виде штрафа на имущество обвиняемых наложен арест. Уголовное дело с утвержденным обвинительным заключением в ноябре 2020 года направлено для рассмотрения по существу в суд.

Одновременно, расширяется деятельность иных специализированных институтов, также доказавших свою компетенцию в рамках противодействия правонарушениям в информационном пространстве.

В активном взаимодействии с Росфинмониторингом Генпрокуратурой реализованы имеющиеся полномочия по удалению и блокированию запрещенной информации с более чем 300 тыс. интернет-ресурсов. Среди них материалы экстремистского и террористического толка, суицидальной направленности, детской порнографии, а также ресурсы пронаркотического характера.

В настоящее время в рамках расширения указанных полномочий нами обеспечивается блокировка «фишиноговых» ресурсов, а также сайтов «финансовых пирамид».

Немалую роль в пресечении рассматриваемых преступлений занимает ФСИН России, которой в целях упреждающего воздействия прорабатываются механизмы принудительной блокировки мобильных сигналов на территории исправительных учреждений.

Ведется работа по активизации государственно-частного партнерства, поскольку ключевое значение для эффективного противодействия ИКТ преступлениям имеют качество взаимодействия с организациями, располагающими оперативно значимой информацией.

Примером такой системной работы служит созданный на базе Банка России Центр реагирования на компьютерные инциденты в кредитно-финансовой сфере. В годы его существования удалось предотвратить многомиллиардные хищения из российских банков, а также совместно с правоохранительными органами пресечь деятельность многих преступных групп.

По сообщениям иных центров реагирования отрабатывается информация о посягательствах в сфере использования компьютерной информации, во взаимодействии с операторами связи и провайдерами Интернет ресурсов блокируются мошеннические ресурсы и абонентские номера.

Безусловно, ведется работа и по совершенствованию действующего законодательства, в целях обеспечения защиты новых объектов посягательств в киберпространстве, появление которых обусловлено стремительным развитием информационных технологий.

Основное внимание при этом акцентировано на внедрении новых электронных форматов осуществления судопроизводства. Кроме того, не так давно принят закон, регулирующий оборот цифровых финансовых активов, что позволит в будущем предотвратить криминальное использование криптовалют. Совершенствуется законодательство в области оборота персональных данных, в том числе в целях предупреждения утечек соответствующих баз.

Также принятыми мерами активизированы мероприятия по повышению квалификации всех категорий лиц, осуществляющих функции по противодействию IT преступлениям, а также комплексному развитию системы экспертного сопровождения данных действий. Организовано формирование и внедрение в профильные учебные заведения соответствующих программ обучения.

Активное участие принимается в процессах профилактики рассматриваемых преступлений. В первую очередь, через официальные сайты государственных органов и иных учреждений. Например, через аккаунт Генпрокуратуры в социальных сетях, имеющий среднемесячную посещаемость в несколько сотен тысяч человек.

Подводя итоги, можно отметить, что нами активно прорабатываются и внедряются в практику современные инструменты и механизмы противодействия киберпреступности, однако для решения всего комплекса проблем, в том числе связанных с высокой степенью анонимности злоумышленников и трансграничностью таких действий, одним из ключевых направлений является объединение в рамках деятельности спецкомитета усилий по работе над проектом всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях.

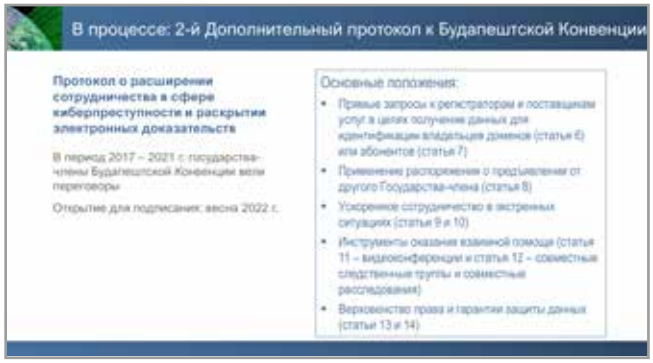
В условиях появления новых вызовов криминального сообщества, без малейшего сомнения использующего отсутствие границ в виртуальном пространстве, мы должны быть на шаг впереди в части международного взаимодействия и прилагать максимально возможные усилия к его совершенствованию. При этом позволю себе выразить уверенность в том, что реализация мероприятий, предусмотренных Резолюции Генассомблеи ООН 74/247, даст возможность если устранить преступную деятельность в цифровом пространстве, то, самое меньшее, не позволить злоумышленникам избежать установленной ответственности за свои действия.

Александр Зегер
Отдел по борьбе с киберпреступностью Совета Европы; Исполнительный секретарь Комитета по Конвенции о киберпреступности (Франция)

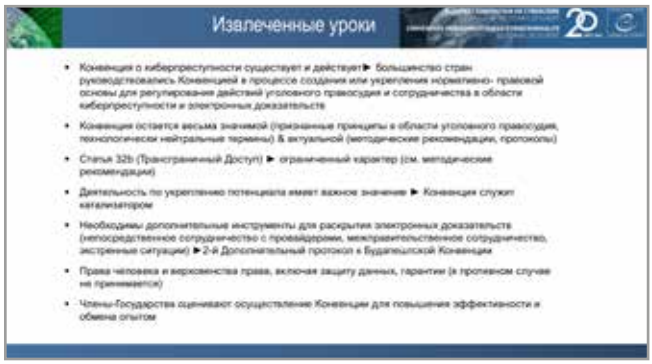
МЕЖДУНАРОДНОЕ СОТРУДНИЧЕСТВО В ОБЛАСТИ КИБЕРПРЕСТУПНОСТИ И ЭЛЕКТРОННЫХ ДОКАЗАТЕЛЬСТВ: ОПЫТ СОВЕТА ЕВРОПЫ

ИНСТРУМЕНТЫ БУДАПЕШТСКОЙ КОНВЕНЦИИ ПО БОРЬБЕ С КИБЕРПРЕСТУПНОСТЬЮ

В ПРОЦЕССЕ: 2-Й ДОПОЛНИТЕЛЬНЫЙ ПРОТОКОЛ К БУДАПЕШТСКОЙ КОНВЕНЦИИ



ИЗВЛЕЧЕННЫЕ УРОКИ



К.Ю. Хмелевский
Сотрудник технико-криминалистического управления Главного управления криминалистики (Криминалистического центра) Следственного комитета Российской Федерации

РАССЛЕДОВАНИЕ ПРЕСТУПЛЕНИЙ С ПОМОЩЬЮ ОТКРЫТЫХ ИСТОЧНИКОВ СЕТИ ИНТЕРНЕТ

Добрый день уважаемые участники конференции! Мне чрезвычайно приятно и почетно принимать участие в этом высоком мероприятии призванном объединить усилия государства, бизнеса и гражданского общества в целях обеспечения международной информационной безопасности и противодействия информационной преступности!

Я являюсь сотрудником одного из самых цифровых подразделений Следственного комитета России. Мы достаточно молодая, по правоохранительным меркам, команда киберкриминалистов. Состоим в технико-криминалистическом управлении Главного управления криминалистики. Должен отметить, что руководство Следственного комитета уделяет повышенное внимание цифровой криминалистике и киберпреступлениям. С 2019 года в структуре СК России появились отдельные подразделения по расследованию киберпреступлений и преступлений в сфере высоких технологий. На сегодняшний день такие обособленные подразделения есть в каждом следственном управлении. Нашей рутиной является оказание помощи следователям в сборе криминалистической информации в сети Интернет, оказание помощи во взаимодействии с другими схожими подразделениями правоохранительных органов, консультации, аналитика, обработка больших массивов данных, что и есть моя персональная зона ответственности.

Как и иные правоохранительные органы, Следственный комитет сталкивается с отдельными противоправными проявлениями использования информационно-коммуникационных технологий.

Стремительное развитие общества и информационных технологий, повсеместное внедрение инноваций приводят к видоизменению преступной деятельности, распространению киберпреступности, создающей для нас новые нарастающие вызовы. Чаще всего это указанные на слайде виды деятельности, такие как различные проявления экстремизма и терроризма, нелегальные оборот оружия и наркотиков, изготовление и распространение детской порнографии, пропаганда терроризма и иные преступления и деяния направленные против человечества.

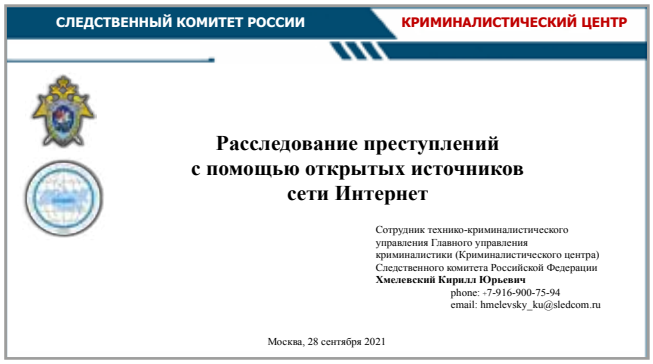
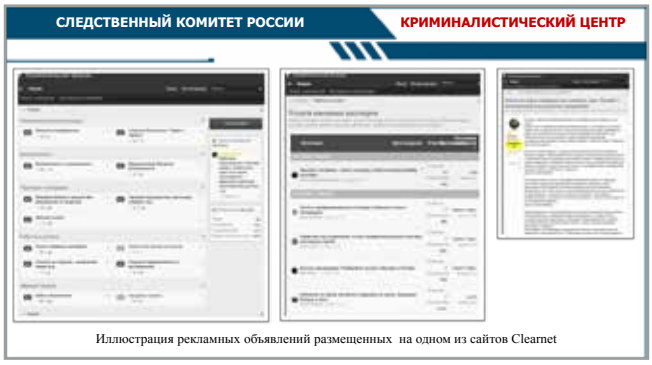
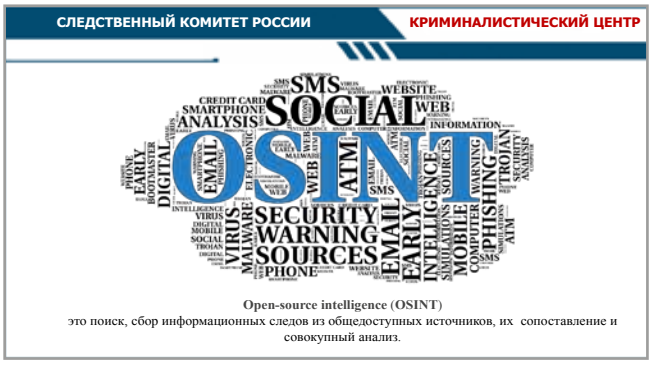


Иллюстрация некоторых видов оружия и боеприпасов, размещенных к продаже в сети TOR.

Иллюстрация некоторых видов наркотических средств размещенных для продажи в сети TOR





Говоря о рынке нелегальных товаров, можно отметить три массово используемые для этого технологии – TOR, ассиметричное шифрование, применяемое для общения, и криптовалюту, чаще всего – биткоин.

Как это работает? Продавец договаривается с администрацией форума, сайтом-площадкой в сети Тор о продаже, например – оружия. Создает тему с описанием товара, ценой, фото, способами связи и публичным ключом для шифрования. Заинтересованные клиенты списываются с продавцом, и если договорились, то на сцене появляется еще один важный участник – «гарант», который является посредником, гарантирующим, что никто никого не обманет. Гарантом является, как правило «проверенный» пользователь форума, либо сайта. Покупатель переводит всю сумму в биткоинах гаранту, который сообщает об этом продавцу. Он, в свою очередь, производит закладку оружия в тайник, и сообщает место покупателю. Если покупатель доволен товаром и не имеет претензий, он сообщает это гаранту, гарант переводит деньги продавцу за вычетом своей доли (3-7%) и доли сайта (3–5%).

В результате довольны все участники этого процесса — продавец продал, покупатель купил, при этом никто никого не видел и не слышал.

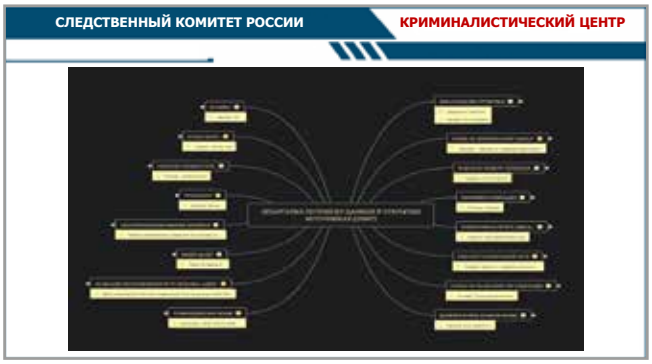
Так же, как и с оружием, используя аналогичные методы реализуются наркотические средства, которые вы можете видеть на слайдах.

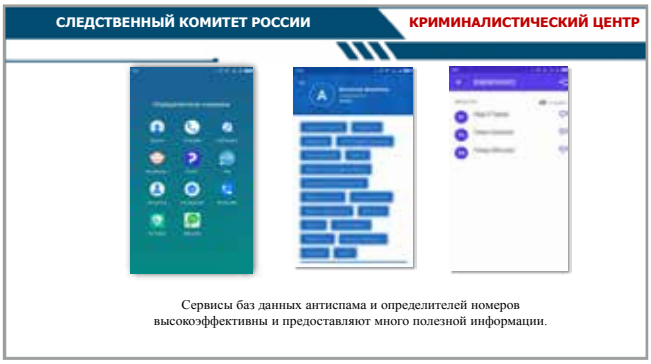
На этих слайдах вы видите примеры оказываемых услуг, в том числе таких, как совершение убийства, поджог зданий и автомобилей, слежка, продажа поддельных документов и т.д. Данная информация размещается на специализированных форумах в сети Интернет. Чем больше участников, тем более известная становится площадка и тем шире комплекс видов оказываемых услуг.

В свою очередь мне хотелось осветить пока ещё новую для правоохранителей сферу сбора информации – это OSINT.

OSINT – разведывательная дисциплина, включающая в себя поиск, выбор и сбор разведывательной информации из общедоступных источников, а также её анализ.

OSINT под тем или иным названием существует уже сотни лет. История OSINT начинается с формирования в декабре 1941 года Службы мониторинга зарубежных трансляций (Foreign Broadcast Monitoring Service, FBMS) в Соединённых Штатах Америки для изучения иностранных трансляций. Сотрудники службы записывали коротковолновые передачи на пластиковые диски, после чего отдельные материалы переписывались и переводились, а затем отправлялись в военные ведомства и подавались в формате еженедельных докладов. Классическим примером работы FBMS является по-





лучение информации об успешности проведения бомбардировок на вражеские мосты путём получения и анализа изменения цен на апельсины в Париже.

В своей деятельности мы также встречаемся с использованием, например, средств анонимизации, при совершении обычных преступлений, которые нельзя отнести к киберпреступлениям.

Отдельные инструменты из сферы информационно-коммуникационных технологий используются массово.

Часто препятствием является применение: шифрованных и анонимных мессенджеров, почтовых сервисов, технологий voice over internet (VOIP), использование систем прокси, vpn, tor, иных пиринговых систем, зарубежных ресурсов (поставщики услуг связи), указание недостоверных сведений о себе, использование для верификации СИМ-карт, оформленных на подставные лица и т.д.

Мы уже говорили о том, что Интернет полон различных данных. В нем можно найти данные с мест происшествий, катастроф, терактов и иных происшествий, привлекающих внимание людей. Он полон различных данных, которые могут послужить доказательством или опровержением тех или иных событий. Нужно лишь научиться с этим работать. И мы в Следственном комитете России принимаем меры к развитию направления по поиску данных в открытых источниках сети Интернет.

Как правило, осуществляется поиск информации о событиях, либо о людях. С поиском сведений о событиях меньше сложностей, а вот найти человека, особенно если он этого не очень хочет, сложнее. Тем не менее, если человек является активным пользователем сети, использует социальные сети, мессенджеры, интернет-банкинг и иные доступные удобства, то о нем можно узнать сведения, представленные на слайде.

Для получения таких сведений используются различные методы OSINT, о которых, с некоторыми упрощениями, я сейчас расскажу.

OSINT начинается с установления поисковой задачи, понимания источников информации. Для структурирования и накопления собственных знаний, а также для фиксации данных в ходе какого-либо сложного поиска, мы применяем подобную памятку.

Сервисы баз данных антиспама и определителей номеров высокоэффективны и предоставляют много полезной информации о владельце или владельцах телефонного номера. Полезнее всего, что данные являются историческими и показывают истинного владельца телефона, то каким образом он записан у других людей.

В завершении своей презентации хотел бы отметить, что у нас есть положительный опыт взаимодействия с другими странами с целью раскрытия неочевидных и сложных преступлений, в которых жертвами стали дети. В подобных делах счет идет на часы, поэтому так важно продумать механизм взаимодействия, который позволял бы обмениваться информацией с зарубежными коллегами по электронным каналам связи, избегая возможные бюрократические издержки и т.д. В идеале данный алгоритм должен позволять держать связь правоохранителям разных стран и обмениваться информацией в режиме онлайн, ответ от одного исполнителя должен доходить до другого исполнителя с минимальной задержкой и минимальным количеством посредников. При этом любой подобный запрос должен быть прозрачен для надзирающих и контролирующих органов. Информация должна быть максимально доступна.

Цичао Жу
Заместитель директора и профессор Института оборонных технологий и стратегических исследований Национального университета оборонных технологий (КНР)

ВЛИЯНИЕ РАЗВИТИЯ ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА НА КИБЕРБЕЗОПАСНОСТЬ

Для меня большая честь участвовать в VX Международном информационном форуме. Сегодня мы обсудим тему «Международное сотрудничество в области борьбы с информационной преступностью». Как мы видим, информационные технологии бурно развивались в течение десятилетий во всем мире, но еще слишком рано делать вывод о том, что тенденция их развития и инноваций достигнет стабильного или зрелого состояния, особенно когда появляется множество новых информационных технологий, таких как ИИ, глубокое обучение, глубокая подделка, автономный алгоритм, большие данные, облако, интернет вещей (物联网, интернет тел (身联网), мета-вселенная (元宇宙) и т.д., все еще быстро развиваются. Я хотел бы кратко рассказать о том, как новые технологии, особенно связанные с искусственным интеллектом, создадут новые проблемы для информационной безопасности, ставят перед нами дилемму управления в этой области и даже станут причиной преступлений.

Как мы все знаем, ИИ – это несколько запутанное понятие, которое содержит множество подчиненных технологий или отраслей, поэтому если мы не сможем дать точное определение упомянутого здесь ИИ, мы не сможем прийти к единому мнению относительно его значения, его происхождения или его фактического влияния. По сравнению с ядерными технологиями, космическими технологиями или квантовыми технологиями, ИИ имеет некоторые очевидные особенности: (1) Порог или стоимость разработки одной технологии ИИ не очень высока, за исключением некоторых ключевых технологий, таких как производство микрочипов ИИ, разработка сложных алгоритмов ИИ и т. д. Именно поэтому небольшие компании-стартапы ИИ или отдельные разработчики игр ИИ процветают в Китае и за рубежом. (2) Разработка и применение продуктов ИИ распространяются легко. Особенно, когда выходят некоторые привлекательные приложения ИИ, количество пользователей будет расти в геометрической прогрессии. Пользователями могут быть как гражданские лица, так и военные. (3) Технология ИИ, конечно, повысит киберзащиту и военный потенциал в области разведки, наблюдения и исследования, командования и управления, принятия решений, логистики, обучения и подготовки. Многие страны ищут технологии ИИ для реорганизации своей гражданской инфраструктуры и военного потенциала.

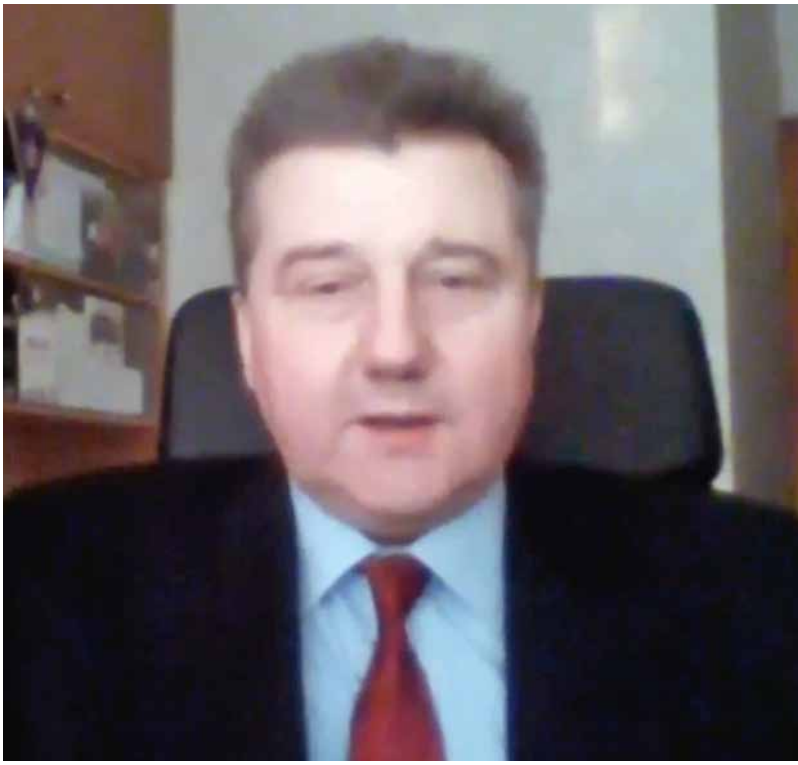
Это практическое применение ИИ, но оно также вызовет проблемы в управлении глобальной информационной безопасностью. Во-первых, вызовы исходят от самой технологии ИИ. Несмотря на быструю эволюцию и развитие, ИИ, о котором мы говорим сегодня, все еще находится на слабой стадии. Поэтому они могут привести к техническим сбоям или катастрофам из-за неправильного использования, особенно когда «черный ящик» алгоритмов выходит из-под контроля. Трудно установить одинаковые стандарты или ввести одинаковое регулирование для всех проблем, связанных с ИИ. Если ключевые технологии или ноу-хау ИИ будут злостно использоваться отдельными хакерами или террористами, обладающими техническими навыками, это может вызвать серьезные проблемы безопасности инфра-

структур, систем финансового и фондового рынка, нефтяных систем, электросетей, космических информационных систем или ядерных систем каждой страны. Такое глобальное управление ИИ будет вызывать все большее беспокойство во всем мире.

Во-вторых, проблема заключается в том, можно ли создать механизм взаимного доверия между крупными державами. Необходимо, чтобы страны, особенно крупные державы, обладающие наиболее сложными информационными технологиями, связанными с ИИ, объединили свои усилия и взяли на себя ответственность за управление глобальной информационной безопасностью. Видно, что ГПЭ при ООН и все большее число аналитических центров активно обсуждают принципы и кодексы поведения для ответственного использования, но построение механизма взаимного доверия пока находится на слабой стадии. Если страна с наиболее сложными технологиями попытается получить монополию за счет своих преимуществ передовых информационных технологий или будет стремиться развязать инновационную экосистему информационных технологий ИИ для сдерживания или санкций в отношении других стран в политических целях, то она подаст плохой пример для установления взаимного доверия.

В-третьих, управление глобальной информационной безопасностью должно продвигаться вперед неуклонно и с достаточным консенсусом. Например, осуществление эффективного глобального управления ИИ является обязанностью не только крупных держав, но и малых стран, развивающихся стран с развитыми информационными технологиями. Все больше и больше государств заинтересованы в укреплении своей экономики, социальной службы и национальной безопасности, поэтому при продвижении инициативы по управлению международной информационной безопасностью необходимо учитывать различия в развитии, цифровые пробелы и диверсифицированную среду правоприменения. Будет несправедливо применять стандарты одной большой державы, и ничего не получится, если в рамках управления глобальной информационной безопасностью будут игнорироваться существующие международные законы и нормы, основанные на человеческой справедливости и честности. В связи с этим было бы безответственно продвигать управление глобальной информационной безопасностью слишком медленно или слишком поспешно. Всего год назад Ван И, министр иностранных дел Китая, выдвинул Глобальную инициативу по безопасности данных (全球数据安全倡议). Это было хорошее начало для обмена позициями и опытом китайского правительства по поддержанию открытой, безопасной и стабильной цепи поставок глобальных продуктов и услуг ИКТ.

А.В. Морозов
Д.ю.н., профессор, заведующий кафедрой информационного права, информатики и математики ВГУЮ (РПА Минюста России)



ПОДГОТОВКА ЮРИДИЧЕСКИХ КАДРОВ ВЫСШЕЙ КВАЛИФИКАЦИИ В ОБЛАСТИ ПРОТИВОДЕЙСТВИЯ ИНФОРМАЦИОННОЙ ПРЕСТУПНОСТИ

Автор является руководителем магистерской программы, реализуемой кафедрой компьютерного права и информационной безопасности МГУ. Заведующий кафедрой – летчик-космонавт, герой России, доктор юридических наук, член-корреспондент РАН, действительный государственный советник РФ I класса Батурин Юрий Михайлович.

Программа направлена на обучение студентов, имеющих высшее образование по юридическим и неюридическим специальностям, претендующих на замещение высоких позиций в государственных органах и учреждениях, крупных и специализированных корпорациях, и предназначена для получения профессиональных знаний в сфере применения информационного законодательства, построения информационного общества и цифровой экономики (создание информационных систем и ресурсов, расследование компьютерных правонарушений и электронное правосудие), ведения электронного бизнеса (финансы, торговля, реклама, СМИ и т.д.) и обеспечения надежной информационной безопасности своей сферы деятельности.

Защитить магистерскую диссертацию и получить степень магистра юриспруденции по предлагаемой программе могут не только лица, уже имеющие юридическое образование, но также и лица, имеющие дипломы бакалавров, специалистов, магистров иных направлений, желающие развить свой образовательный потенциал, стать более конкурентоспособным на рынке труда, повысить свой общественный статус.

Учебные, практические и научно-исследовательские занятия ведут как преподаватели МГУ, обладающие, как правило, и техническим, и юридическим образованием, имеющие огромный практический и научный опыт, так и специалисты-практики – представители органов государственной власти, практикующие юристы и эксперты российских и зарубежных компаний.

Всем обучающимся в магистратуре предоставляется возможность прохождения практики в Государственной Думе и Совете Федерации Федерального собрания РФ, Верховном Суде РФ, Следственном комитете РФ, Минфине РФ, Минюсте РФ, Федеральной антимонопольной службе РФ, а также целом ряде других государственных и коммерческих организаций, с которыми МГУ имеет соответствующие партнерские отношения.

Выпускники магистерской программы востребованы в сфере юридического сопровождения электронного бизнеса, в юридических службах министерств и ведомств (организация электронного взаимодействия и электронных государственных услуг), в спецслужбах и правоохранительных органах, службах безопасности крупных компаний, адвокатуре и нотариате.

Имеется возможность самостоятельно сформировать свой индивидуальный план обучения в магистратуре, выбрав необходимые курсы профессионального цикла подготовки, в частности, такие, как «Актуальные проблемы информационного права», «Правовое регулирование отношений в сети Интернет», «Правовое регулирование отношений в сфере электронной коммерции и банковской тайны», «Форенсика (исследование до-

казательств по компьютерным инцидентам)», «Виртуальная разведка», «Компьютерная этика», «Правонарушения в онлайновых вселенных (мирах) и традиционные правовые системы» и ряд других авторских спецкурсов

Магистерскую программу отличает высочайший уровень профессорско-преподавательского состава и целевая установка на углубленную подготовку профессионалов для работы в юридической и смежных сферах деятельности.

Развитие информационного общества в России в настоящее время происходит в соответствии с Указом Президента Российской Федерации № 203 от 9 мая 2017 года, утвердившим новую Стратегия развития информационного общества России на период до 2030 года[1], которая предусматривает развитие цифровой экономики и создание цифровой среды как основы ее функционирования. Второе, в свою очередь, базируется на национальном проекте «Цифровая экономика Российской Федерации», который продолжает и развивает идеи, заложенные в соответствующей правительственной программе[2]. И, наконец, современные вызовы, угрозы и средства обеспечения безопасности личности, общества и государства отражены новой Доктрине информационной безопасности Российской Федерации[3].

Информационное общество в своей основе формирует особого рода информационные отношения, которые представляют интерес для научных исследований и подготовки кадров в ведущих вузах страны. В условиях развития информационного общества в Российской Федерации информационные правоотношения определяются объективными экономическими отношениями, основанными на многообразии форм собственности, в том числе и на объектах интеллектуальной собственности, и представляют собой общественные отношения граждан, предприятий, органов власти, иных субъектов права. Они являются средством решения задач в области формирования единого информационно-правового пространства страны, защиты конституционных прав на информацию, осуществления информационного обмена, обеспечения информационной безопасности.

Все вместе предполагает ведение в информационном обществе электронного бизнеса, включая такие направления как электронные финансы, торговля, смарт контракты, рынок криптовалют, реклама, СМИ и т.д. и обеспечение надежной информационной безопасности этой сферы деятельности.

При преподавании закрепленных за кафедрой дисциплин производится подробный анализ результатов правоприменения Федеральных законов «Об информации, информационных технологиях и о защите информации»[4], «О персональных данных»[5], «Об электронной подписи»[6], «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления»[7], «Об организации предоставления государственных и муниципальных услуг»[8], «О защите детей от информации, причиняющей вред их здоровью и развитию»[9], «О связи»[10],

1 См.: СЗ РФ. 1996. № 28. Ст. 3347. Указ Президента Российской Федерации от 09.05.2017 № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы» // «Собрание законодательства РФ», 15.05.2017, № 20, ст. 2901.

2 Распоряжение Правительства РФ от 28.07.2017 № 1632-р «Об утверждении программы «Цифровая экономика Российской Федерации» // «Собрание законодательства РФ», 07.08.2017, № 32, ст. 5138.

3 Указ Президента РФ от 05.12.2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // Официальный интернет-портал правовой информации pravo.gov.ru.

4 Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // «Собрание законодательства РФ», 31.07.2006, № 31 (1 ч.), ст. 3448.

5 Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» // «Собрание законодательства РФ», 31.07.2006, № 31 (1 ч.), ст. 3451.

6 Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи» // «Собрание законодательства РФ», 11.04.2011, № 15, ст. 2036.

7 Федеральный закон от 09.02.2009 № 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления». Официальный интернет-портал правовой информации pravo.gov.ru.

8 Федеральный закон от 27.07.2010 № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг». Официальный интернет-портал правовой информации pravo.gov.ru.

9 Федеральный закон от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию». Официальный интернет-портал правовой информации pravo.gov.ru.

10 Федеральный закон от 07.07.2003 г. № 126-ФЗ «О связи» // «Собрание законодательства РФ». 2003. № 28, ст. 2895.

«О коммерческой тайне»[11], «Об обеспечении доступа к информации о деятельности судов в Российской Федерации»[12], «О безопасности критической информационной инфраструктуры Российской Федерации»[13] и других, анализ которых показывает, что идет бурное развитие информационного законодательства, реализующего информационные права и свободы граждан.

Главнейшей составляющей указанного процесса является развитие четвертой части Гражданского кодекса Российской Федерации[14], в направлении правового регулирования цифровой экономики, оборота объектов интеллектуальной собственности, защиты авторских прав на указанные объекты, особенно такие, как программы для ЭВМ и базы данных, сообщения в эфир или по кабелю радио- или телепередач, идущих сегодня, прежде всего в сети Интернет, изобретения и полезные модели, промышленные образцы, топологии интегральных микросхем, секреты производства (ноу-хау), фирменные наименования, товарные знаки и знаки обслуживания, которые сегодня практически тесно связаны с доменными именами как средствами индивидуализации. Автор имеет 10 патентов (авторских свидетельств) на изобретения и программные продукты, включая базы данных правовой информации, и делиться с учащимися своими соображениями по поводу их создания, использования и защиты в рамках требований информационной безопасности.

Также идет изучение процессов противодействия компьютерным преступлениям, предусмотренным главой 28 Уголовного кодекса Российской Федерации[15] «Преступления в сфере компьютерной информации», в которую недавно добавлен новый состав – статья 274.1. «Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации».

В настоящее время происходит разработка и совершенствование новых терминов правового регулирования процессов становления информационного общества. Первый тип терминов связан с понятиями, определяющими применение вычислительной техники (аппаратно-программных средств) и телекоммуникационных сетей передачи данных при реализации государственных задач и ведении бизнеса, таких как «информационный», «компьютерный», «цифровой», «электронный» и т.д. У каждого определения есть свои преимущества и недостатки. Я думаю, что время расставит все по своим местам. Главная особенность стыка веков – развитие информационно-коммуникационных технологий (характеристики компьютеров удваиваются каждые 3–5 лет) и катастрофическая нехватка точных законодательно закрепленных терминов и правовых норм, регулирующих правоотношения в глобальном информационном обществе.

Очень много споров ученые правоведы ведут в настоящее время по поводу терминологических особенностей понятий «информационная безопасность», «кибербезопасность» и «безопасность информации». Последний термин, как и «защита информации» как правило, используется классическими «технорями» в погонах, помнящими еще закон 1995 года «Об информации, информатизации и защите информации». Молодежи нравится все иностранное (например IT – информационные технологии) и особенно все, что начинается и таит в себе что-то магическое с приставки «кибер». Скажу без рассуждений, я приверженец глобального понятия «информационная безопасность» и буду использовать его в дальнейшем. По моему мнению, у информации не может быть безопасности – это универсальная категория, такая же, как материя или энергия, а термин «кибер» изначально обозначал «железяку» (робот, ком-

11 Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне» // «Собрание законодательства РФ», 09.08.2004, № 32, ст. 3283.

12 Федеральный закон от 22.12.2008 № 262-ФЗ «Об обеспечении доступа к информации о деятельности судов в Российской Федерации» // «Собрание законодательства РФ», 29.12.2008, № 52 (ч. 1), ст. 6217.

13 Федеральный закон от 26.07.2017 № 187 «О безопасности критической информационной инфраструктуры Российской Федерации». Официальный интернет-портал правовой информации pravo.gov.ru.

14 Гражданский кодекс Российской Федерации: федер. закон от 18 декабря 2006 г. № 230-ФЗ, часть четвертая // Российская газета. – М. 2006. - 22 декабря.

15 Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ // «Собрание законодательства РФ», 17.06.1996, № 25, ст. 2954.

пьютер и т.д.) и слишком узко определяет правоотношения в глобальном информационном обществе.

Объединяющими элементами общественных отношений в условиях построения информационного общества являются[16], в первую очередь, информация и информационные объекты (элементная база, программные продукты, ресурсы, системы, сети, технологии и т.д.), обладающие спецификой при осуществлении прав, исполнении обязанностей и установлении ответственности по поводу их использования в цифровой среде. Однородность и особенности информационных отношений определяются особенностями и юридическими свойствами этих объектов. К таким объектам, помимо информации, информационных технологий, ресурсов и систем, относятся также средства обеспечения информационной безопасности.

Распространение и активное развитие информационно-коммуникационных технологий (далее - ИКТ), создание на их основе высокопроизводительных компьютерных систем и баз данных большой размерности характеризует нынешний этап построения информационного общества. Государства стали активно использовать ИКТ во всех сферах деятельности, что привело к значительному повышению качества жизни населения и повышению эффективности государственного управления. Но вместе с этими преимуществами государство столкнулось с проблемой обеспечения безопасности в данной сфере, такие как безопасность объектов инфраструктуры, защиты объектов авторских прав, граждан от информационно-психологического воздействия и т.д.

После распада СССР, Россия активно вступила в процесс информатизации и глобализации. В 1994 году в стране был зарегистрирован первый домен в зоне «.ru»[17] (автор руководил созданием первого сайта Минюста России scli.ru в 1996 году), а Интернет начал бурно развиваться и распространяться среди граждан и организаций и стал основой развития информационного общества. В тоже время в информационной сфере деятельности стали появляться и первые правонарушители (хакеры). Тогда Россия столкнулась с фактом того, что если деятельность в цифровой среде не регулировать правовыми средствами, то это может явиться угрозой безопасности как государства, так и личности и общества. Первым делом опасность бесконтрольного использования ИКТ может привести к возможности влияния на российское общество извне, поскольку сеть Интернет практически безконтрольно дает возможность общаться и контактировать с представителями зарубежных государств и с их помощью влиять на политические взгляды и предпочтения.

Сфера ИКТ постоянно эволюционирует и следует за техническим прогрессом. Очевидно, что многие угрозы исходящие из данного вида деятельности человечества, только приобретают свои очертания и государства находятся еще на стадии выработки механизмов противодействия данного вида угрозам. Для противостояния и успешного преодоления проблем в данной сфере нужно объединить усилия между техническими, политическими и юридическими институтами. Только объединенная работа этих институтов и общества в целом позволит преодолеть угрозы развитию современного информационного общества.

Доктрина информационной безопасности Российской Федерации называет национальными интересами России в информационной сфере объективно значимые потребности личности, общества и государства в обеспечении их защищённости и устойчивого развития в части, касающейся информационной сферы. Немаловажно, что указанное определение основано на определении национальных интересов в Стратегии национальной безопасности. То есть, законодательное определение ключевых понятий в информационной безопасности может основываться на регулировании понятийного аппарата национальной безопасности. Это естественно, поскольку

16 Информационное право и информационная безопасность : учебник для магистров и аспирантов : в 2 ч. / Морозов А.В., Полякова Т.А., Филатова Л.В. - [Электрон. Изд.]. ВГУЮ (РПА Минюста России). – М. : : ВГУЮ (РПА Минюста России), 2017. – Ч. 1. - 365 с. – экз. – ISBN 978-5-00094-295-6.- ISBN 978-5-00094-295-3 (Ч. 1) и ВГУЮ (РПА Минюста России). – Москва - Саратов: ВГУЮ (РПА Минюста России), 2017. – Ч. 2. - 412 с. – экз. – ISBN 978-5-00094-295-6.- ISBN 978-5-00094-297 (Ч.2).

17 Демкина И. Когда появился Интернет в России и мире // См.: [Электронный ресурс] // URL: // И. Демкина // SYL.ru. – 19.02.2015. – Режим доступа: https://www.syl.ru/article/170038/new_kogda-poyavilsya-internet-v-mire-i-v-rossii, свободный (дата обращения: 31.08.2018).

информационная безопасность – неотъемлемая составляющая национальной безопасности РФ[18].

Следует отметить, что законодательное определение информационной безопасности, закреплённое Доктриной, учитывает как пассивный её аспект (состояние защищённости объективно значимых потребностей личности, общества и государства в информационной сфере), так и активный аспект (устойчивое развитие). Однако активный аспект информационной безопасности был бы закреплён полнее, если бы информационная безопасность определялась Доктриной не только как состояние защищённости национальных интересов РФ (интересов личности, общества и государства) в информационной сфере, но и как определённый уровень информационного развития, позволяющий предупреждать, устранять и противодействовать основным угрозам в информационной сфере[19].

Немаловажно, что информационные возможности используются в террористических и экстремистских целях, одной из основных угроз в этом случае выступает пропаганда терроризма и экстремизма. Доктрина в целом характеризует и состояние информационной безопасности в отдельных сферах общественной жизни. Так, отдельные государства стремятся использовать своё технологическое превосходство для доминирования в информационном пространстве, подрыва стратегической стабильности и равноправного стратегического партнёрства[20].

Состояние правового регулирования основ информационной безопасности, несомненно, обусловлено и необходимостью соблюдения государственной и иной охраняемой законом тайны в РФ, ограничения и запрета доступа к определённой информации. Проблемами обеспечения информационной безопасности занимаются федеральные органы безопасности и защита информации с ограниченным доступом является важной составляющей их работы.

Для минимизации масштабов угроз в отношении, прежде всего государственных информационных систем и ресурсов, был принят Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»[21], который устанавливает организационно-правовые основы обеспечения безопасности критической инфраструктуры в целях ее устойчивого функционирования, определяет права и обязанности ее владельцев, а также полномочия госорганов в указанной сфере.

Под безопасностью критической информационной инфраструктуры (далее КИИ) понимается состояние защищенности критической информационной инфраструктуры, обеспечивающее ее устойчивое функционирование при проведении в отношении ее компьютерных атак.

Актуальность и приоритетность направления совершенствования нормативной правовой базы в области обеспечения информационной безопасности, с учетом соответствующих предложений и рекомендаций Совета Безопасности Российской Федерации, подтверждаются необходимостью создания структурно единой и функционально взаимосвязанной системы обеспечения информационной безопасности на федеральном, региональном и муниципальном уровнях, что, в свою очередь, подчеркивает важность стратегического планирования и правового обеспечения в данной области, а главное, что именно право призвано не допустить состояния информационного хаоса.

Как известно, для успешного окончания магистратуры учащийся должен подготовить и защитить выпускную квалификационную работу (магистерскую диссертацию). Вот некоторые направления проведения научных исследований:

1. Правовые основы развития информационного общества.
2. Институт информационного права и его развитие в 21 веке.

18 Доктрина информационной безопасности Российской Федерации от 5 декабря 2016 г. (утверждённая Указом Президента Российской Федерации от 5 декабря 2016 г. № 646) [Электронный ресурс] // Режим доступа: https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html.

19 Там же

20 Ковлагина Д.А. Информационный терроризм: понятие, уголовно-правовые и иные меры противодействия: монография / Д.А. Ковлагина; под редакцией доктора юридических наук, профессора Н.А. Лопашенко. – Москва: Юрлитинформ, 2017. – С. 84.

21 Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» // Собрание законодательства РФ. 2017. № 31 (Часть I). Ст. 4736.

3. Формирование и развитие единого информационного пространства в исследуемой сфере.
4. Правовое обеспечение доступа к информации.
5. Информационные технологии в деятельности органов государственной власти.
6. Мониторинг правоприменения и система правовой информации Российской Федерации.
7. Государственные услуги, осуществляемые с использованием информационных технологий в электронном виде.
8. Информационные технологии как объект правового регулирования
9. Информационные ресурсы как объект правового регулирования
10. Информационные системы как объект правового регулирования
11. Особенности правоотношений, возникающих при производстве, распространении и потреблении информации в сети Интернет.
12. Деятельность средств массовой информации (далее – СМИ) в сети Интернет.
13. Развитие правовых информационно-справочных систем.
14. Нормативное правовое регулирование оказания государственных услуг через Интернет.
15. Электронный документооборот в деятельности органов государственной власти.
16. Использование электронной подписи при оказании государственных и муниципальных услуг.
17. Организация деятельности по выпуску, выдаче и обслуживанию универсальных электронных документов.
18. Ответственность за нарушения в сфере компьютерной информации.
19. Юридические проблемы идентификации личности в сети Интернет.
20. Защита персональных данных при осуществлении деятельности в сети Интернет.
21. Система межведомственного электронного документооборота.
22. Национальные интересы России в информационной сфере.
23. Доктрина информационной безопасности Российской Федерации.
24. Стратегия развития информационного общества.
25. Развитие цифровой экономики при построении информационного общества.
26. Криптовалюты и цифровые финансовые активы
27. Национальная стратегия развития систем искусственного интеллекта.
28. Развитие и совершенствование законодательства об информации, информатизации и защите информации.
29. Развитие и совершенствование законодательства о персональных данных.
30. Развитие и совершенствование законодательства об электронной подписи.
31. Развитие и совершенствование законодательства по противодействию преступлениям в сфере компьютерной информации.
32. Организационно-правовые основы дистанционного обучения.
33. Обеспечение информационной безопасности деятельности государственных органов.
34. Основы и перспективы развития международной информационной безопасности.

В этом году 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 нас находить новые возможности в этой важнейшей сфере деятельности.

Михаил Анисимов
Корпорация по управлению доменными именами и IP-адресами (ICANN)

ИССЛЕДОВАТЕЛЬСКИЕ ПРОЕКТЫ ICANN В ОБЛАСТИ БЕЗОПАСНОСТИ ДОМЕННЫХ ИМЕН

ПРОЕКТ DAAR:

Проект DAAR

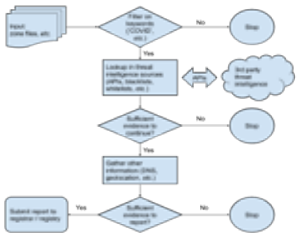
- DAAR (domain abuse activity reporting) – это система отчетов о зловредной активности в доменных именах.
- Анализируются данные по следующим категориям: фишинг, распространение зловредного ПО, управление бот-сетями.
- Источники данных: регистратуры доменов верхнего уровня, партнеры по кибербезопасности

- SURBL lists (только доменные имена)
- Spamhaus Domain Block List
- Anti-Phishing Working Group
- Malware Patrol (Composite list)
- Phishtank
- Ransomware Tracker

| 2

Пример работы DAAR в условиях COVID-19

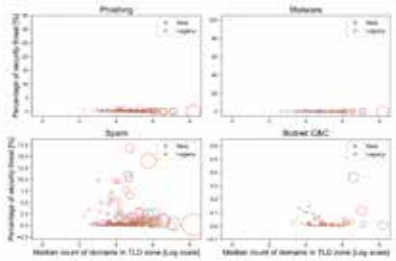
- Анализ списков доменов на ключевые слова
- Проверка у сторонних экспертов
- Проверка "поведения" домена
- Если замечено нарушение – информация передается администратору



| 3

Некоторые результаты проекта DAAR:

Корреляция угроз и размера доменных зон



| 5

НЕКОТОРЫЕ РЕЗУЛЬТАТЫ ПРОЕКТА DAAR:

Некоторые результаты проекта DAAR:

Распределение доменов по типам угроз

| 4

СОВМЕСТНАЯ РАБОТА НАД ПРАВИЛАМИ:

Совместная работа над правилами

DNS Abuse Framework

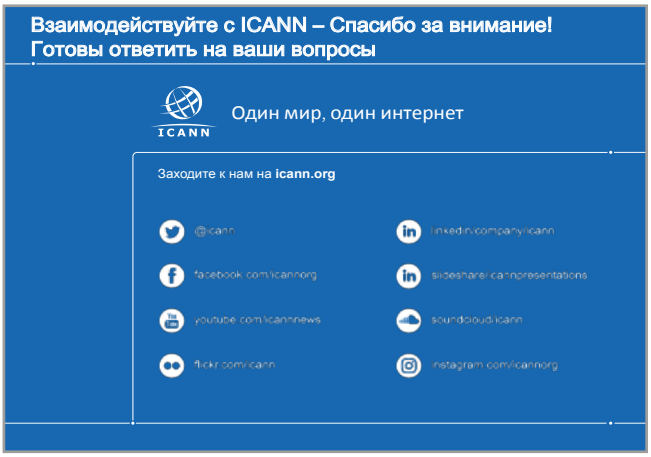
документ, определяющий классификацию угроз

- Фишинг
- Распространение вредоносного ПО
- Управление бот-сетями
- Фарминг
- Спам

DGA Framework

документ, описывающий действия с доменами, которые регистрируются автоматически.

| 6


Взаимодействуйте с ICANN – Спасибо за внимание!
Готовы ответить на ваши вопросы
ICANN
Один мир, один интернет
Заходите к нам на icann.org
@icann
linkedin.com/company/icann
facebook.com/icannorg
slideshare/icannpresentations
youtube.com/icannnews
soundcloud/icann
flickr.com/icann
instagram.com/icannorg

Ю.А. Юдина
Центр международной информационной безопасности МГИМО МИД России

ПРОБЛЕМЫ РАССЛЕДОВАНИЯ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ ПРЕСТУПНОСТИ

Коллеги, благодарю за предоставленное слово!

При подготовке к выступлению мною было выявлено несколько блоков проблем, которые встают перед нашим государством и международным сообществом при расследовании международных преступлений, совершенных с использованием ИКТ.

По прошествии двух дней Форума я дополнила перечень еще некоторыми проблемными вопросами, о которых говорили докладчики.

И так, ключевыми проблемами в области расследования и предупреждения международной информационной преступности являются:

1. Правовые;
2. Организационно-управленческие;
3. Технические;
4. Образовательные.

Необходимо начать с глобального блока – с правового.

Несмотря на наличие в законодательстве практически каждого государства спектра нормативно-правовых актов (преимущественно, соответствующих глав Уголовного кодекса), полностью весь спектр злонамеренных действий, возможно, имеющих конструкцию, аналогичную составу преступления, не охватывается обозначенными нормами. Так, в отечественном уголовном законодательстве имеет место глава 28 “Преступления в сфере компьютерной информации”, что нисколько не исключает применение для классификации преступления статей из других глав, разделов, как например, ст. 159.3 УК РФ, ст. 159.6 УК РФ.

Что касается регионального и глобального уровня, мы все так же наблюдаем отягченные политической повесткой договоренности в рамках международного сообщества. В первую очередь, даже в условиях действующих, принятых практически единогласно итоговых докладов РГОС, и впоследствии принятых на их основе Резолюций ГА ООН, государствам все еще трудно прийти к единогласию по ряду значимых вопросов, например, касающихся применимости принципов международного права к процессу реализации и обеспечения международной информационной безопасности.

Так, наблюдаются разногласия по поводу понимания принципа соблюдения суверенитета (невмешательства во внутренние дела суверенных государств). Что это – правило или принцип? Представители российского научно-исследовательского сообщества, а кроме того и практики в области обеспечения МИБ настаивают на соблюдении указанного «условия» как принципа. Западные коллеги претендуют на закрепление трактовки – правило. Разница семантическая: принцип – это базис, нерушимая основа, несоблюдение которых может повлечь за собой наказание, применение санкций, если говорить более точным терминологическим языком. Правила же всегда могут иметь те или иные исключения, возможность поиска лакун и blackhole.

Исходя из того на какой правовой основе выстроится система обеспечения международной информационной безопасности – soft law или hard law, будет зависеть и степень ответственности государств в рамках реализации своей внутренней и внешней политики в ИКТ-среде.

Вторым важным блоком вопросов, требующих разрешения для успешной деятельно-

сти в области расследования преступлений с применением ИКТ, является организационно-управленческий.

Как на заседании 1 Круглого стола Форума отметил Бабекин Дмитрий Владимирович, заместитель директора Департамента международного права и сотрудничества Министерства юстиции России, для эффективной реализации политики в сфере обеспечения международной информационной безопасности в России необходимо выстроить единую вертикаль власти, самостоятельную, обособленную структуру, в ведении которой будет находиться процесс создания единой универсальной методики расследования информационных преступлений. Представитель Министерства Юстиции России выдвинул действительно прекрасную инициативу. Однако, в отличие от него я бы не рекомендовала создание структуры по типу Федерального Агентства, ввиду того, что согласно действующему национальному законодательству Федеральные Агентства и схожие с ними по статусу государственные федеральные органы исполнительной власти, подчиняются федеральным Министерствам. Дабы исключить конфликт интересов, а равно создать по-настоящему независимую структуру, я настаиваю на разработке плана создания государственного органа, напрямую подчиняющегося Президенту России. В состав такого органа следует ввести лучших специалистов из различных структур власти, как правоохранительных – МВД России, ФСБ России, СК России, Прокуратуры России, но кроме того, и самых сильных светочей научной мысли.

Третьим блоком проблем выступает недостаточность технического оснащения, необходимого для расследования преступлений рассматриваемого толка. Так, исходя из личного опыта, я могу отметить, явную нехватку в регионах, малых населенных пунктах современного оборудования, мощных ПК и иных технических устройств, что напрямую сокращает возможность эффективности проведения оперативно-розыскных, следственных и иных мероприятий, представляющих процесс расследования информационных преступлений или как в последние годы принято говорить – проводить атрибуцию таких преступлений. Яркий пример, подтверждающий данную проблему – не самый высокий уровень раскрытия некоторых преступлений финансового толка с применением ИКТ, т.е. фишинга.

Четвертым блоком вопросов выступает катастрофический кадровый голод. Как молодой специалист, за спиной которого еще виднеется студенческая скамья, с болью отмечу недостаток часов для полноценного введения студентов в курс уголовного-процессуального права, криминалистики и криминологии. Безусловно, можно наблюдать как сильных преподавателей и студентов, работа совместная работа которых проходит в унисон, но имеет место и нерадивость самих студентов, а также неспособность или нежелание отдельных представителей преподавательского корпуса заинтересовать обучающихся, равно как и объяснить им сложные вопросы простым языком. Кроме того, наблюдается нехватка специализированных дисциплин, включающих обширный спектр правовых и технических аспектов обеспечения международной и национальной информационной безопасности в юридических вузах, в частности, в региональных вузах. Разумеется, в качестве исключения можно выделить отдельные высшие школы, в течение долгого времени сфокусированные на обучении студентов, как юридическим аспектам обеспечения международной информационной безопасности, так и техническим. Отмечу, что меня особо заинтересовало выступление одного из докладчиков 2 Круглого стола, рассказавшего о программе магистратуры, реализуемой уже порядка двадцати лет. Однако у меня возник и ряд вопросов к данной программе: 1) как можно принимать к обучению на специализации в области цифрового общества и информационной безопасности лиц, не имеющих базы юридической или в области государственного и муниципального управления, или не обучавшихся в вузах при Министерстве обороны России, и т.д.; 2) меня озадачило малое число часов, отведенных на изучение forensic science, т.е криминалистики.

В заключении отмечу, что не хочу заканчивать свое выступление на негативной ноте, поэтому выражу свою глубокую убежденность и сильную веру в то, что рано или поздно будет достигнут консенсус по решению обозначенных проблем как в рамках реализации внутренней политики Российской Федерации, так и внешней в области заключения договоренностей по МИБ.

Единственное, что я еще хотела бы отметить, подводя итог своему выступлению: нам необходимо поторопиться. Догонять преступников, отставать от них на шаг или идти в ногу, неэффективно и грозит чрезмерно опасными последствиями. Выражая надежду на то, что в течение ближайших пяти лет Россия и международное сообщество совместными найдут выход из сложившейся ситуации.

П.У. Кузнецов
Заведующий кафедрой информационного права Уральского государственного юридического университета, д.ю.н., профессор

ПРАВОВЫЕ ПРОБЛЕМЫ БОРЬБЫ С КИБЕРПРЕСТУПНОСТЬЮ

Как известно, информационные преступления представляют собой угрозу безопасности развития информационного общества, так как имеют устойчивую тенденцию к увеличению их распространенности и, следуя в русле технического прогресса, способы совершения киберпреступлений постоянно обновляются и развиваются.

Как известно, в криминологии существует общепризнанное мнение о том, что лучший способ борьбы с этим наиболее опасным видом преступлений являются меры их предупреждения. Это правильно.

Но все же на современном этапе в сложных условиях зарождения начал цифровой экономики на первое место выдвигается именно борьба с киберпреступностью, весьти которую весьма и весьма затруднительно.

Наиболее характерные проблемы борьбы с информационными преступлениями можно представить следующие.

Сложность терминов, понятий и их определений

Конечно, эта сложность является отражением технологической сложности окружающей человека информационной среды.

Практически почти все понятия и термины, которые употребляются в текстах соответствующих нормативных правовых актов, имеют физическую и математическую природу. Это обстоятельство существенно влияет на формирование языка уголовного закона.

Например, понятие «компьютерная информация» как предмет совершения преступления в прежней редакции УК РФ определялось как «информация, обработанная на машинном носителе, и содержащаяся в ЭВМ, в системе ЭВМ или в их сети». В действующей редакции

Кодекса приводится уже другое определение – «сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи». Вместе с тем, в п. 11.1 ст. 2 Закона «Об информации, информационных технологиях и о защите информации» приводится определение понятия «электронный документ» – «документированная информация, представленная в электронной форме, т.е. в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах». Электронный документ и компьютерная информация тесно связаны между собой. Они логически соотносятся в тех случаях, когда предметом посягательства является конкретные документированные сведения в электронной форме (например, данные на кредитной пластиковой карте).

Как видим, приведенные в определении признаки документа одного и того же рода, как «электронная форма информации» в «виде, пригодном для восприятия человеком с использованием ЭВМ», в определении понятия компьютерной информации в УК РФ отсутствуют.

Напротив, в нем дан новый признак компьютерной информации – ее представление в «форме электрических сигналов». Но это не одно и то же, поскольку электрический

сигнал – это сигнал в электрической цепи, а электронная форма информации (не сигнала) – электронно-цифровой код, т.е. символ, в который преобразовывается содержание информации.

Вызывает споры и юридическая конструкция диспозиции ст. 272 УК РФ, которая имеет значение для других составов гл. 28 Кодекса: «Неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации...». Приведенная формулировка явно неудачна, поскольку в информационной среде злоумышленник нередко нарушает лишь правила доступа к информации, т.е. он только знакомится с ее содержанием (например, с персональными данными, банковской информацией), что не вызывает материальных последствий для целостности информации. Вместе с тем, конструкция состава преступления имеет так называемую «материальную форму», т.е. преступлением будет считаться только такое действие, которое должно привести к материальным последствиям в виде уничтожения, блокирования, модификации либо копирования компьютерной информации. Поэтому на практике зафиксированные активные действия злоумышленников, связанные с проникновением к компьютерной информации, чаще всего не признаются преступлением за отсутствием в их действиях его состава.

Очевидно, что эти и другие противоречия и несовершенство текстов законов не способствуют успеху в борьбе с информационными преступлениями, поскольку создают препятствия в понимании употребляемых определений терминов и понятий в ходе расследования уголовных дел, особенно при формулировании обвинения.

Сложность расследования киберпреступлений

Это проявляется, прежде всего, в том, что в законе не закреплены электронные формы доказательств. В частности, в ст. 84 УПК РФ говорится, что «документы могут содержать сведения, зафиксированные как в письменном, так и в ином виде. К ним могут относиться материалы фото- и киносъемки, аудио- и видеозаписи и иные носители информации».

Таким образом, электронные формы доказательств отнесены к иным документам и иным носителям информации – это все, что могут использовать органы расследования в борьбе с преступлениями в сфере информационных технологий.

Инертность законодателя в части восполнения названного пробела трудно объяснить, особенно если сравнить уголовно-процессуальный закон и другие процессуальные законы. Так, ст. 71 ГПК РФ к письменным доказательствам относит содержащие сведения об обстоятельствах, имеющих значение для рассмотрения и разрешения дела, акты, договоры, справки, деловую корреспонденцию, иные документы и материалы, выполненные в форме цифровой, графической записи, в том числе полученные посредством факсимильной, электронной или другой связи. В статье 75 АПК РФ к письменным доказательствам причислены иные документы, выполненные в форме цифровой записи или иным способом, позволяющим установить достоверность документа. При этом п. 3 статьи устанавливает, что документы, полученные посредством факсимильной, электронной или иной связи, в том числе с использованием сети «Интернет», а также документы, подписанные электронной подписью или иным аналогом собственноручной подписи, допускаются в качестве письменных доказательств.

Недостаточная строгость уголовного закона в отношении большинства составов преступления

Это явное несоответствие между распространенностью этого явления и строгостьюнаказания. В других странах (Китае, США и др.) за совершение компьютерных преступлений предусмотрена более суровая ответственность.

Проблемы определения юрисдикции, т.е. неопределенность в применении правовых мер ответственности за совершение информационных преступлений в ситуациях трансграничности информационного пространства, когда невозможно точно определить место совершения деяний.

Во-первых, в условиях использования сети «Интернет», которая, как известно, не знает территориальных границ, трудно своевремен-

но определить, где начало и окончание совершаемых преступлений, кто их совершает и в какое время, откуда поступают электронные сообщения и кто их отправляет. В них могут быть задействованы одновременно десятки юридических лиц, десятки или даже сотни (тысячи) граждан и организаций, которым причиняется вред, – все они могут находиться не только в разных территориальных пространствах, но и на территориях разных стран.

Во-вторых, практически невозможно определить закон, да и конкретную национальную правовую систему в тех случаях, когда действия совершаются с использованием сети «Интернет» и при этом используются десятки (сотни, тысячи) электронных адресов, расположенных в разных странах.

В-третьих, в разных странах действуют разные технические и технологические условия использования информационных систем, разные стандарты безопасности информации и информационной инфраструктуры. Поэтому при организации расследования сетевых информационных преступлений возникает проблема совместимости национальных стандартов безопасности информационных систем и информационной инфраструктуры, в том числе при фиксации следов преступления, их документировании и сборе доказательственной базы.

Международные проблемы борьбы с киберпреступлениями

Информационные преступления, особенно совершаемые с использованием сети «Интернет», носят глобальный характер. Для согласования и координации действий по борьбе с ними заключаются международные договоры и соглашения.

В частности, в Конвенции о киберпреступности Совета Европы от 23 ноября 2001 г. (далее – Конвенция) приводятся универсальные термины и определения в области борьбы с уголовными преступлениями. Россия, как известно, не присоединилась к Конвенции из-за отсутствия в ее тексте гарантий обеспечения баланса интересов в области национальной безопасности государств-участников, прав и законных интересов их граждан и юридических лиц.

Вместе с тем Конвенция предусмотрела меры, которые надлежало бы принять на национальном уровне, в том числе уголовно-правового (модельные нормы, позволяющие единообразно понимать компьютерную терминологию на законодательном уровне) и уголовно-процессуального характера (универсальные нормы, устанавливающие полномочия и процедуры при расследовании преступлений).

Конвенция предусмотрела также общие принципы международного сотрудничества по уголовным делам в отношении преступлений, связанных с компьютерными системами и компьютерными данными, правила взаимной правовой помощи при расследовании и на стадии судебного разбирательства, в том числе правила выдачи преступников, и др. Думается, что при желании, можно было решать вопрос об имплементации отдельных положений Конвенции в российское законодательство. Это сократило бы часть проблем в борьбе с киберпреступностью.

Страны-члены Шанхайской организации сотрудничества (ШОС) заключили межправительственное Соглашение о сотрудничествев области обеспечения международной информационной безопасности (далее –Соглашение), которое было подписано 16 июня 2009 г. и вступило в силу 2 июня 2011 г. Соглашение отвечает принципам и задачам деятельности ШОС, предусматривающим координацию действий, оказание взаимной поддержки и сотрудничества по важнейшим международным и региональным вопросам, к которым, в частности, относится и проблематика обеспечения международной информационной безопасности.

Уникальность документа заключается в том, что он впервые на уровне международного документа определяет наличие конкретных угроз в области международной информационной безопасности, а также основные направления, принципы, формы и механизмы сотрудничества в этой сфере. Соглашение открыто для присоединения других государств, что также отвечает идее и целям создания всеобъемлющей системы обеспечения международной информационной безопасности, в том числе противодействия кибертерроризму и информационной преступности, содействия обеспечению безопасного, стабильного функционирования сети «Интернет».

Важным является и то, что Соглашение определяет основные угрозы международной информационной безопасности, в частности такие, как информационная преступность, источником которой являются «лица или организации, осуществляющие неправомерное использование информационных ресурсов или несанкционированное вмешательство в такие ресурсы в преступных целях».

Признаками «информационной преступности» как угрозы Соглашение называет: проникновение в информационные системы для нарушения целостности доступности и конфиденциальности информации; умышленное изготовление и распространение компьютерных вирусов и других вредоносных программ; осуществление DOS-атак (отказ в обслуживании) и иных негативных воздействий; причинение ущерба информационным ресурсам; использование информационных ресурсов и методов для совершения таких преступлений, как мошенничества, хищение, вымогательство, контрабанда, незаконная торговля наркотиков, распространение детской порнографии и др.

К сожалению, не все эти признаки нашли отражение в тексте УКРФ, хотя Россия подписала Соглашение и, казалось бы, внесение соответствующих изменений и дополнений в российское законодательство должно было последовать незамедлительно.

КРУГЛЫЙ СТОЛ № 4
СОТРУДНИЧЕСТВО В ОБЛАСТИ ПРЕДОТВРАЩЕНИЯ ВОЕННЫХ КОНФЛИКТОВ И МИРНОГО РАЗРЕШЕНИЯ СПОРНЫХ СИТУАЦИЙ В ИКТ-СРЕДЕ

Модератор:
Эльяс В.П., Минобороны России

С.А. Комов
Эксперт Министерства обороны Российской Федерации

О НЕОБХОДИМОСТИ ФОРМИРОВАНИЯ МЕХАНИЗМА МИРНОГО РАЗРЕШЕНИЯ МЕЖДУНАРОДНЫХ СПОРОВ, ВОЗНИКАЮЩИХ В СВЯЗИ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ[1]

Уважаемые коллеги!

Последние двадцать лет США активно формируют всеобъемлющий международно-правовой режим, которым они намерены заменить созданную по инициативе СССР систему юридически обязывающих разоруженческих договоров.

В основу такого режима положена выработка т.н. «правил поведения государств» в соответствующей сфере международных отношений и мер реагирования на их нарушение. Элементы такого режима создаются в сферах контроля над использованием космического пространства; распространением биологического оружия и технологий, связанными с химическим и биологическим оружием; распространением ракетных технологий и баллистических ракет; распространением ядерного оборудования и обеспечением ядерной безопасности; распространением обычных вооружений.

В настоящее время Вашингтон начал применять аналогичные подходы в сфере использования ударных беспилотных летательных аппаратов (БЛА). Он возглавляет разработку принципов ОЭСР по «ответственному управлению надежным искусственным интеллектом» и формирует режим деятельности государств в информационном пространстве на основе признания применимости существующего международного права, выработки норм ответственного поведения и мер укрепления доверия в форматах ООН, ОБСЕ, ОЭСР и АРФ.

Особенностью создаваемого США режима является привлечение крупного западного бизнеса, экспертного, инженерного и академического сообщества, что выводит сферу его охвата далеко за рамки регулирования и оценки поведения только государств и аффилированных с ними структур. Другой его особенностью стала опора на силу как главное средство разрешений спорных ситуаций в информационном пространстве.

Существующие элементы всеобъемлющего международно-правового режима уже позволяют Вашингтону жестко направлять внешнюю и внутреннюю политику «государств-единомышленников», которые обязались его соблюдать, и оказывать многостороннее давление на тех, кто еще не присоединился к нему.

Ввиду того, что формируемый механизм во всех названных сферах лишен стройной централизованной системы сбора объективных доказательств виновности в нарушении правил ответственного поведения и каких-либо контрольных механизмов верификации соблюдения государствами этих правил, обвинения, раздающиеся из Вашингтона, как правило, имеют сугубо политизированный и необъективный характер.

Применяемые в ответ на якобы выявленные нарушения «правил поведения» односторонние рестрикции грубо нарушают международное право.

Во-первых, предъявление обвинений суверенным державам и наложение на них каких-либо наказаний является нарушением исключительных прерогатив Совета Безопасно-

1 Выступление подготовлено коллективом экспертов Минобороны России в области международной информационной безопасности в составе: Дылевский И.Н., Базылев С.И., Запивахин В.О., Комов С.А., Юниченко С.П., Шевченко А.Л., Завьялов Е.К., Каргин М.Н.

сти ООН. Такая практика ведет к разрушению существующей системы международного права, утрате авторитета Совета Безопасности ООН и к его подмене «атрибутивным механизмом», функционирующим под управление группы западных стран во главе с США.

Во-вторых, обвинения и наказания, налагаемые каким-либо государством или группой государств на физических или юридических лиц других государств, является прямым вмешательством в их внутренние дела.

В связи с этим необходимо активизировать работу по продвижению российского подхода к установлению внеблокового универсального режима международной информационной безопасности, основанного на принципе равной безопасности сторон и сосредоточении совместных усилий мирового сообщества на предотвращении межгосударственных споров и конфликтов.

Считаем, что в ходе работы на данном направлении основные усилия необходимо сосредоточить на создании альтернативного международного механизма разрешения инцидентов и конфликтов в информационной сфере, опираясь на полномочия Совета Безопасности ООН и положения Устава ООН о мирном разрешении международных споров.

Принципы построения такого механизма необходимо разрабатывать, опираясь на объективную оценку внешнеполитической обстановки в данной сфере.

В первую очередь, необходимо понять причины возникновения противоречий между американской и российской позициями в отношении принципов построения такого механизма. Без их уяснения сформировать выигрышную переговорную позицию и в последующем реализовывать ее на практике будет затруднительно.

По нашему мнению, развитию сотрудничества с Россией на этом направлении мешает отсутствие доверия со стороны американской администрации. Поэтому все попытки наладить такое взаимодействие наталкиваются в худшем случае на противодействие, а в лучшем – на отсутствие какой-либо ответной реакции. Причина недоверия Вашингтона к дипломатическим шагам российской стороны связана с убежденностью администрации Д. Байдена в том, что США находятся в состоянии «информационной войны» с Россией, в ходе которой провести грань между криминальными и агрессивными действиями в информационной сфере практически невозможно. Американские эксперты полагают, что использование ИКТ якобы в криминальных целях может служить хорошим прикрытием для решения военно-политических или иных внешнеполитических задач. Поэтому в Белом доме не верят в искренность мирных инициатив российской стороны в сфере международной информационной безопасности (МИБ). Там подозревают, что они играют роль дипломатического прикрытия «агрессивных планов Кремля», направленных на оказание деструктивного влияния на внутриполитические процессы в США и массированный вывод из строя американской критической информационной инфраструктуры. Отсюда многократные бездоказательные публичные обвинения и уголовные преследования должностных лиц ГРУ и ФСБ, а также «аффилированных с ними российских неправительственных структур» в попытках совершения или в совершении таких деяний.

Во-вторых, важно понимать насколько широко Вашингтону удалось распространить атмосферу недоверия к российским инициативам в сфере МИБ. По нашей оценке, большинство развивающихся стран на практике не ощущают в них того «деструктивного потенциала», о котором настойчиво твердит Вашингтон. Они так же не считают себя объектами российской «информационной войны». Именно это обстоятельство позволяет российской стороне добиваться дипломатических успехов в международных форматах, где решения принимаются большинством голосов стран «третьего мира». Яркий пример – успешное формирование по инициативе России специального комитета ООН для выработки всеобъемлющей конвенции о противодействии информационной преступности. Представляется, что этот позитивный опыт целесообразно использовать при продвижении инициативы разработки под эгидой ООН универсального механизма мирного разрешения споров, связанных с использованием ИКТ, отказавшись от попыток решить эту проблему в форматах, где США обладают перевесом сил.

И, наконец, необходимо преодолеть бытующее заблуждение, что чисто техническими методами можно решить проблему обеспечения МИБ. Несомненно, технический прогресс будет способствовать повышению защищенности информационной инфраструктуры будущего. Однако, пока наблюдаемая нами эволюция современных ИКТ только обогащает

спектр вызовов и угроз в информационной сфере. Поэтому без применения международно-правовых средств регулирования отношений государств в информационной сфере, в том числе при возникновении споров, связанных с использованием ИКТ, обойтись невозможно.

Ключевым вопросом в ходе формирования механизма мирного разрешения споров является определение принципов его построения. Общепризнанными принципами являются воздержание от использования силы или угрозы силой для навязывания другой стороне своего способа разрешения конфликта, урегулирование споров такими средствами, которые не будут способствовать эскалации конфликта и нести в себе угрозы миру и безопасности. Переговорная практика, связанная с разрешением международных споров свидетельствует о том, что еще одним базовым принципом является нацеленность сторон на совместное разрешение возникшей спорной ситуации, а не на максимизацию своего выигрыша в результате разрешения спора.

Взгляните с этих позиций на выработанный Вашингтоном «атрибутивный механизм», и вы увидите, что ни один из этих принципов в нем не применяется

Общий алгоритм разрешения спора, опирающийся на существующее международное право, хорошо известен. Пострадавшее государство, в качестве первого шага к мирному урегулированию и недопущении эскалации конфликта, должно уведомить другую сторону о своих озабоченностях и предложить ей обменяться информацией по данному вопросу. Затем стороны переходят к прямым переговорам по дипломатическим или иным имеющимся каналам. Если ситуация может представлять угрозу для международного мира и безопасности, стороны должны передать его на рассмотрение Совета Безопасности ООН, который уполномочен давать им рекомендации относительно процедуры, методов, средств и условий мирного урегулирования спора. Последние достаточно детально проработаны в существующих международно-правовых актах.

В заключение следует отметить, что ввиду актуальности рассматриваемой проблемы, пути использования имеющегося международно-правового инструментария для мирного разрешения споров, возникающих в связи с использованием ИКТ, целесообразно рассматривать как в многосторонних форматах, так и на двустороннем уровне, включая данный вопрос в повестку дня всех международных встреч по тематике МИБ.

Благодарю за внимание!

А.А. Стрельцов
Д.т.н., д.ю.н., профессор, член-корреспондент Академии криптографии, вице-президент НАМИБ

ВОПРОСЫ ПРИМЕНЕНИЯ МЕЖДУНАРОДНОГО ПРАВА В ИКТ-СРЕДЕ

Формирование системы международной информационной безопасности длительное время находится в центре внимания международного сообщества. Доклад Группы правительственных экспертов (ГПЭ ООН) по достижениям в области информатизации и коммуникаций в контексте международной безопасности (2015 г.)[1] был принят консенсусом и поддержан 70-ой сессией Генеральной Ассамблеи ООН[2].

В Докладе отмечено, что «соблюдение государствами международного права, в частности их обязанностей по Уставу, является существенно важной основой, определяющей их действия в сфере использования ИКТ и создания открытой, безопасной, стабильной, доступной и мирной ИКТ-среды. Эти обязанности имеют важнейшее значение для рассмотрения вопроса о применимости норм международного права к использованию ИКТ государствами».

Особенно актуальным представляется решение проблем применения международного права к вопросам сотрудничества в области противодействия:

- нарушению безопасности объектов национальной критической информационной инфраструктуры;
- вмешательству во внутренние дела суверенных государств посредством злоупотребления свободой массовой информации.

О необходимости решения этих вопросов отметил Президента Российской Федерации Владимира Владимировича Путина в заявлении о комплексной программе по восстановлению российско-американского сотрудничества в области международной информационной безопасности[3].

Президентом Российской Федерации предложены конкретные меры по их решению применительно к двусторонним отношениям Российской Федерации и США. В частности, предлагается:

- совместная разработка и заключение двустороннего межправительственного соглашения о предотвращении инцидентов в информационном пространстве по аналогии с действующим советско-американским Соглашением о предотвращении инцидентов в открытом море и воздушном пространстве над ним от 25 мая 1972 г.
- обмен гарантиями невмешательства во внутренние дела друг друга, включая избирательные процессы, в том числе с использованием ИКТ и высокотехнологичных методов.

Такой же подход к решению этих проблем может быть применен и на уровне международных организаций, в частности, ООН.

Для решения этих задач необходимо, как предложил Президент Российской Федерации, «дать ход профессиональному экспертному диалогу по вопросам международной информационной безопасности, не делая его заложником политических разногласий».

Нормативную основу сотрудничества экспертов в области международной информационной безопасности ИКТ-среды могут составить:

- добровольные и необязательные нормы ответственного поведения государств в глобальной ИКТ-среде;

1 A/70/174

2 A/RES/70/237

3 20 сентября 2020 г. http://www.kremlin.ru/events/president/news/64086

- политические нормы (нормы «мягкого» права), регулирующие реализацию мер укрепления доверия в ИКТ-среде и поддержания стратегической стабильности, создания глобальной культуры кибербезопасности и оценки национальных усилий по защите объектов критической информационной инфраструктуры;
- принципы международного права, касающиеся дружественных отношений и сотрудничества между государствами в соответствии с Уставом Организации Объединенных Наций, и прежде всего: суверенное равенство; разрешение международных споров мирными средствами таким образом, чтобы не подвергать угрозе международный мир и безопасность и справедливость; отказ 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 Организации Объединенных Наций; уважение прав человека и основных свобод; невмешательство во внутренние дела других государств.

Основным принципом сотрудничества должно быть уважение суверенитета государств и международных норм и принципов, проистекающих из суверенитета, которые применяются к осуществлению государствами деятельности, связанной с ИКТ, и к их юрисдикции над ИКТ-инфраструктурой, расположенной на их территориях.

В то же время, как отмечалось на XIV Международном форуме «Партнерство государств, бизнеса и гражданского общества при обеспечении международной информационной безопасности», «международное право пока не стало инструментом, способным на основе международного сотрудничества предотвращать использование ИКТ для нарушения открытости, стабильности, доступности и мерности ИКТ-среды[4]».

Определенная работа по созданию условий для экспертного обсуждения проблем формирования системы международной информационной безопасности в этом направлении международным сообществом уже проведена.

Во-первых, удалось продлить до 2025 года деятельность Рабочей группы открытого состава ООН как площадки для равноправного институционального диалога экспертов заинтересованных государств.

Во-вторых, достигнут консенсус экспертов по поводу акцентирования внимания экспертов на изучении проблем практического применения правил ответственного поведения на основе норм, правил и принципов ответственного поведения государств в ИКТ-среде. В наиболее общем виде эти правила изложены в итоговом докладе ГПЭ ООН (2015 г.) и в Резолюции Генеральной Ассамблеи ООН (2018 г.)[5].

К числу возможных направлений совместных исследований в области противодействия угрозам безопасности объектов критической информационной инфраструктуры можно отнести следующие:

- политические, правовые и технические аспекты атрибуции (обследование) инцидентов для целей применения мирных средств разрешения спорных ситуаций;
- закрепление границ зон ответственности государств в ИКТ-среде;
- определение содержания международного правового режима зоны ответственности государств;
- определение в ИКТ-среде признаков объектов КИИ, находящихся под защитой международного гуманитарного права, и содержания международного правового режима безопасности этих объектов.

Важным представляется также начать обсуждение проблем сотрудничества в области предотвращения вмешательства во внутренние дела суверенных государств посредством злоупотребления свободой массовой информации.

Как представляется, решение проблем противодействия угрозам нарушения международной информационной безопасности

4 Шерстюк В.П., Стрельцов А.А. Ключевые проблемы правового обеспечения международной информационной безопасности. Сборник докладов. 7-9 декабря 2020 г. Москва, Россия, стр. 48-52

5

должно осуществляться с целью создания открытой, безопасной, стабильной, доступной и мирной ИКТ-среды, укрепления международного мира и безопасности.

Для организации экспертного изучения проблем практического применения международным сообществом правил ответственного поведения государств в ИКТ-среде можно было бы использовать площадку Рабочей группы открытого состава ООН. При этом предварительную проработку предложений для обсуждения можно было бы осуществить на площадке Международного исследовательского консорциума информационной безопасности, созданного в 2010 г. в г. Гармиш-Партенкирхен (ФРГ).

Определенных опыт проведения таких исследований у Консорциума имеется. Так, в 2020 году был завершен совместный проект по исследованию проблем применения рада правил ответственного поведения государств в ИКТ-среде на основе международного права. В работе приняли участие эксперты Российской Федерации, США, Эстонии, Швейцарии. Отчет о работе размещен на сайте Национальной ассоциации международной информационной безопасности.

Ханнес Эберт
Центр Гуманитарного диалога (Швейцария)

МЕРЫ УКРЕПЛЕНИЯ ДОВЕРИЯ И МИРНОЕ УРЕГУЛИРОВАНИЕ СПОРОВ: ПЕРСПЕКТИВЫ И ОПАСНОСТИ С ТОЧКИ ЗРЕНИЯ ПОСРЕДНИЧЕСТВА

1. Введение:

- Моя работа будет посвящена перспективам внедрения эффективных мер укрепления доверия в ИКТ среде. Я расскажу о своем опыте работы в Центре гуманитарного диалога, также известном как HD. Центр гуманитарного диалога – это базирующаяся в Женеве организация частной дипломатии, специализирующаяся на посреднических процессах, способствующих мирному регулированию и разрешению конфликтов в строго независимой и нейтральной манере.
- Три года назад HD создал новый орган – Директорат по цифровым конфликтам, который стремится адаптировать свой 20-летний опыт посредничества, знания и сети к отличительным особенностям конфликтов в ИКТ среде. Тема этого круглого стола «Сотрудничество в области предотвращения военных конфликтов и мирного разрешения спорных ситуаций в ИКТ-среде» лежит в основе работы HD, и я благодарен, что могу поделиться некоторым опытом нашего зарождающегося диалога в этой области.
- Я хотел бы начать с одного общего наблюдения по всем направлениям нашего диалога: государства различаются и, вероятно, будут продолжать различаться в своих концепциях международной информационной безопасности. Это расхождение делает необходимым откровенный диалог о наличии общих интересов. Этот диалог может быть сосредоточен на различных механизмах мирного разрешения разногласий. Далее я, во-первых, объясню, почему мы решили сосредоточиться на конкретных видах мер укрепления доверия, и, во-вторых, рассмотрю, какие условия могут определять их эффективность.

2. Меры укрепления доверия: Эффективность и среда с низким уровнем доверия

- Почему мы решили сосредоточиться на мерах укрепления доверия? Это не очевидное решение. Откровенный диалог должен признать, что меры укрепления доверия в этой области были разработаны на разных уровнях, но также должен открыто оценить их эффективность. Нам необходимо общее понимание того, что сработало и не сработало из предыдущих соглашений и механизмов их реализации, включая двусторонние соглашения.
- Один из ключевых выводов из моей работы в HD заключается в том, что эффективность мер укрепления доверия, в частности, в отношениях между великими державами, которые определяют международную стабильность в более широком смысле, до сих пор была ограниченной. Вот почему нам необходим диалог, подобный этому круглому столу, и обсуждение того, как улучшить многочисленные системы мер укрепления доверия.
- Для начала нам необходимо тщательно проанализировать сильные и слабые стороны мер укрепления доверия на разных уровнях. Несколько госу-

дарств и институтов приложили большие усилия в этой области, особенно на региональном и многостороннем уровнях. Эти меры укрепления доверия обычно разрабатываются для повышения прозрачности, сотрудничества и стабильности. Тем не менее, эти меры нацелены на глобальную или региональную аудиторию и, как правило, не конкретизируют вопрос о том, между кем меры стремятся укрепить доверие.

- Региональные усилия были особенно эффективны в предоставлении целевой поддержки, отвечая на потребности конкретного региона, опираясь на уже существующие рамки сотрудничества. Их успехи были основаны на наличии технических и политических контактных пунктов и активных каналов связи, которые являются ключевыми отправными точками для укрепления доверия. Многосторонние процессы повысили глобальную осведомленность и признание. Однако они вряд ли станут платформами для разрешения разногласий между великими державами, чьи возможности, а также политика и институты намного более развиты, и чьи отношения в этом контексте неизбежно носят геополитический характер. Однако, как отмечали предыдущие ораторы, в этих отношениях в настоящее время отсутствует необходимое доверие. Меры укрепления доверия должны приспособиться к этой реальности. В заключение я предлагаю четыре условия, при которых эта адаптация может быть успешной.

3. Условия для повышения эффективности

a. **Управление ожиданиями.** Разработка мер укрепления доверия между великими державами должна основываться на реальных предположениях о том, что возможно, а что нет. Хотя меры укрепления доверия не предотвратят намеренную эскалацию конфликта, они могут помочь управлять риском непреднамеренной эскалации, вызванной, например, неправильной атрибуцией инцидентов или неправильным восприятием. Они не заменяют политическую волю к мирному урегулированию разногласий. Поэтому диалог должен признавать интересы государств и способствовать обмену мнениями об их различном восприятии угроз. Такое совместное понимание является предпосылкой для диалога, который может учитывать основные интересы каждой стороны. При соблюдении этого условия, как показал прошлый опыт, можно найти точки соприкосновения через геополитические разрывы даже при наличии фундаментальных различий во мнениях.

b. **Совместный анализ прошлых соглашений.** Это общее понимание ограничений мер укрепления доверия должно быть основано, в большей части, на **общем понимании прошлых соглашений,** некоторые из которых были упомянуты предыдущими ораторами. Это включает признание того, что перенос традиционной практики контроля над вооружениями в сферу информационной безопасности был очень трудным, и поэтому существует большая потребность в скорректированных или новых концепциях. Одним из важнейших аспектов в этом контексте являются механизмы проверки. Прошлые соглашения пострадали из-за различных представлений о соблюдении этих соглашений. Необходимы протоколы и стандарты представления доказательств, которые могут повысить прозрачность.

c. **Последовательность и многоуровневое сотрудничество.** Стоит еще раз подчеркнуть, что реализация мер укрепления доверия может происходить одновременно с нормативными дискуссиями по таким вопросам, как применение международного права и важность суверенитета. Оба эти аспекта взаимосвязаны, поскольку нормативные дискуссии влияют на то, как меры воспринимаются и реализуются на практике. Однако долгосрочные нормативные дискуссии не должны ограничивать прогресс в других областях. В то же время существующие факты

свидетельствуют о том, что внедрение мер укрепления доверия должно быть постепенным и основываться на поэтапном подходе. Создание обширного списка мер укрепления доверия сразу не даст результатов. Наличие функционирующей системы координационных центров как основы для многих других мер является ключевым фактором. Кроме того, наличие политических и технических координаторов может обеспечить многоуровневое сотрудничество. Даже когда политические дискуссии заходят в тупик, технические консультации, например, между национальными Компьютерными группами реагирования на чрезвычайные ситуации, могут продолжаться.

d. **Меры укрепления доверия по конкретным вопросам.** В условиях низкого доверия государства могут начать с определения конкретных областей, защита которых отвечает интересам каждой стороны. Сюда могут входить инфраструктуры, общие для всей международной системы, например, защита медицинских учреждений, исследований и распространения вакцин в контексте пандемии COVID-19 и другие.

Эти четыре принципа могут помочь отделить идеологическое от практического и способствовать диалогу в тех областях, где можно найти точки соприкосновения.

В.Н. Иванов
К.и.н., ведущий научный сотрудник, Центр Стимсона (США).

О ПРОГРАММЕ КИБЕРСОТРУДНИЧЕСТВА ЦЕНТРА СТИМСОНА

Доброе утро, уважаемые коллеги!

В минувшем декабре я выступал на 14-м ежегодном Форуме НАМИБ в качестве представителя Института «Восток-Запад» в России. Как тогда и ожидалось, эта американская экспертная организация самораспустилась в результате обострения ряда системных проблем деятельности международных НКО в условиях короновирусной пандемии. Теперь, оставаясь в Москве, я сотрудничаю с другим неправительственным научным центром США, – базирующимся в Вашингтоне Центром Стимсона.

Центр был основан под занавес холодной войны, в 1989 году, и назван именем выдающегося американского дипломата первой половины 20го века Генри Льюиса Стимсона. По духу и формам работы Центр имеет сильное сходство с Институтом «Восток-Запад». Основные направления работы касаются таких областей, как предотвращение и разрешение международных конфликтов, глобальные проблемы военной, экономической и ресурсной безопасности, нераспространение ОМУ, влияние технического прогресса на стратегическую стабильность, международная торговая и технологическая политика, эффективность международных организаций. У Центра неплохие связи в дипломатических и военных кругах в Вашингтоне; анализ и разработка идей для внешней политики США – один из главных приоритетов. При этом Центр стремится к непредвзятому, взвешенному, разностороннему и основанному на строгом научном подходе анализу международных процессов.

Российское направление, как и кибербезопасность, до сих пор не выделялись в качестве отдельных программ, что открывает возможности для построения конструктивной и не отягощенной негативным опытом совместной повестки дня с российскими партнерами. Именно в этом я вижу свою среднесрочную задачу – передать и развить, на базе Стимсона, тот плодотворный опыт работы с Россией, который был наработан Институтом «Восток-Запад» за его сорокалетнюю историю.

Что касается вопросов международной киберполитики, то в контексте повестки настоящего Форума два программных направления, разрабатываемых с Стимсоне, представляются наиболее интересными.

Во-первых, это оценка и снижение рисков эскалации стратегического военного конфликта между Россией и США, связанных с милитаризацией ИКТ среды. Этой темой мы, в частности, занимаемся в рамках неправительственного Диалога между американскими и российскими военными. Диалог был инициирован еще Институтом «Восток-Запад» в начале 2020 года – в виде серии регулярных встреч отставных офицеров высокого ранга. В какой-то степени инициатива является ответом на дефицит системного военного сотрудничества между двумя ведущими ядерными державами, возникший после введения соответствующего запрета американскими законодателями в 2016 году. Это сюжет, на котором на днях сделал акцент председатель Комитета начальников штабов ВС США Марк Милли после встречи с начальником Генштаба ВС России Валерием Герасимовым. Позвольте процитировать Милли: «Нам необходимо внедрить политику и процедуры, чтобы снизить неопределенность, уменьшить недоверие, увеличить уровень стабильности, чтобы избежать просче-

тов и уменьшить вероятность войны великих держав... Это фундаментальная вещь, которую мы должны попытаться сделать, и я постараюсь это сделать», – сказал Милли. При кажущейся очевидности, эти высказывания вызвали громкую полемику на Капитолийском холме, как и прямые звонки Милли его китайскому коллеге, еще при Трампе, продиктованные тем же стремлением, – избежать недопонимания и эскалации рискованных военных приготовлений.

Так вот влияние гонки кибервооружений на стратегическую стабильность для военного диалога имеет первостепенное значение. Тут на конференции я слышал призывы к тому, чтобы в первую очередь противостоять самой милитаризации ИКТ среды, а не фокусироваться на регулировании военного киберконфликта. Я исходил бы из того, что милитаризация киберпространства – это факт, с которым в краткосрочной перспективе ничего не поделаешь. Необходимо думать над мерами взаимного контроля и снижения рисков непреднамеренного столкновения, способного нанести ущерб критической, в том числе ракетно-ядерной инфраструктуре, структурам командования и управления, системам раннего предупреждения и т.п. Так же, как наши страны договариваются в других сферах контроля вооружений – но с поправками на особенности ИКТ-среды, учитывая легкость распространения кибероружия среди негосударственных игроков.

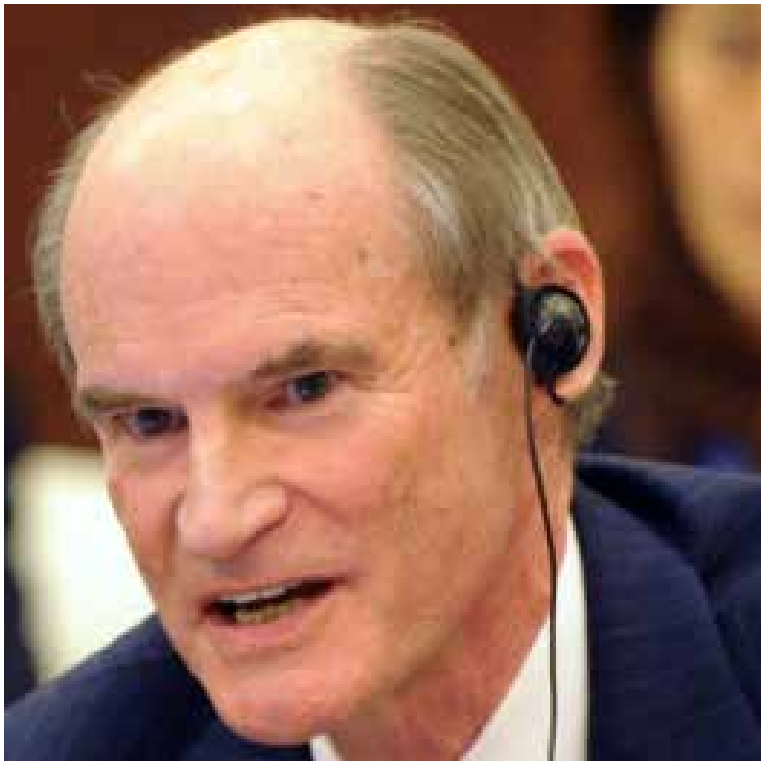
Второе, и связанное с первым, приоритетное направление в Центре Стимсона – проект по формированию и продвижению механизмов возложения ответственности и правоприменения за киберпреступления и акты киберагрессии. Речь идет о масштабном исследовании (а затем общественном обсуждении его результатов) соответствующих практик в традиционных сферах, где имеет место международное сотрудничество по снижению рисков вооруженного столкновения, – на суше, на море и в воздухе, и возможностях применения этого опыта к ИКТ-пространству. Тут открывается широкое поле для сотрудничества между частным сектором и экспертами госструктур, в частности по вопросам международной атрибуции киберинцидентов, обмена данными, определении составов преступлений и мерам наказания.

Надеюсь, что мои комментарии позволят лучше понять программный контекст следующего выступления, которое мы увидим в записи. Мой коллега Брюс МакКоннелл хорошо известен многим участникам Форума. Он несколько лет руководил программой кибер-сотрудничества в Институте «Восток-Запад» и ныне – один из ведущих экспертов по этому направлению в Стимсоне.

В заключение хочу выразить признательность организаторам Форума за развитие столь динамичной площадки для профессиональной международной дискуссии. Готов продолжить рабочие контакты со всеми участниками, заинтересованными в сотрудничестве.

Благодарю за внимание!

Брюс В. МакКоннелл
Заслуженный научный сотрудник Центра Стимсона и Американского филиала Исследовательского фонда "Observer" (ORF America)



НОВЫЕ ВЫЗОВЫ ДЛЯ НАЦИОНАЛЬНОЙ СТРАТЕГИИ КИБЕРОБОРОНЫ

Приветствую всех. Рад видеть многих своих друзей на этой встрече форума «Гармиш-в-Москве». Жаль, что я не могу быть с вами лично.

Меня зовут Брюс МакКоннелл. Я бывший президент Института «Восток-Запад» (EWI), который, к сожалению, закрылся после 40 лет работы. Сейчас я являюсь заслуженным научным сотрудником Центра Стимсона и американского филиала международного исследовательского фонда «Observer» (Observer Research Foundation – ORF America). Эти две базирующиеся в США неправительственные организации подхватывают и развивают работу, которую Институт «Восток-Запад» вел на протяжении многих лет. Вместе со мной на этой встрече присутствуют д-р Владимир Иванов из Центра Стимсона и д-р Андреас Кюн из ORF America. Моя тема сегодня – «Новые вызовы для национальной стратегии кибероборны».

Сегодня я не буду тратить время на обсуждение уровня атак в киберпространстве, скажу лишь, что они продолжают расти и становятся все более опасными. Ставки растут, а действия правительств все менее сдержанны, чем когда-либо. Это не война, но определенно не похоже и на мир.

Как мы пришли к такой ситуации? Традиционные подходы к обороне оказались неэффективными в киберпространстве. Страны поняли, что «атаки побеждают», и, соответственно, отказались от традиционных теорий сдерживания, разработанных и отточенных во время холодной войны, в пользу новых стратегий ведения конфликта и управления конфликтами. Таким образом, мы являемся свидетелями новой эры политических вооружений – термина, первоначально определенного в 1948 году американским дипломатом и бывшим послом США в Москве Джорджем Кеннаном как «использование всех средств, находящихся в распоряжении государства, за исключением войны, для достижения своих национальных целей».

Сети, связывающие людей по всему миру и обеспечивающие современную экономику, представляют собой идеальное поле для подрыва могущественных государств и ограбления предприятий и частных лиц в совершенно новых масштабах. В то же время военные силы, действующие во взаимосвязанном глобальном пространстве киберпространства, находятся в постоянном контакте с источниками силы своих конкурентов. Государственных границ больше не существует, сети крупных государств имеют опорные узлы практически везде и переплетаются с сетями конкурентов. Сегментация сетей больше невозможна. Цифровой код сам по себе становится территорией. Таким образом, мы совместно работаем и живем отныне в среде с неотъемлемой системной уязвимостью.

Сегодня все крупные державы проводят непрерывные кибер-операции в сетях своих конкурентов, не достигая порога вооруженного конфликта. Действуя в рамках присущих США демократических институтов и процедур выработки политки, правительство США предоставляло много публичной информации об этой оперативной практике, называемой «постоянным взаимодействием». Но не стоит полагать, что эта практкика уникальна. Подход США весьма схож с подходом их основных конкурентов, включая Россию и Китай,

и, в действительности, был частично разработан в ответ на аналогичную тактику, уже используемую этими и другими державами.

В 2018 году США заявили, что прежняя доктрина сдержанности и сдерживания в киберпространстве как стратегия оказалась неэффективной. Чрезвычайно способные конкуренты преднамеренно действовали против интересов США ниже порога вооруженного конфликта. США утверждали, что их сдержанность поощряет подобную «низкопороговую» деятельность. Для преодоления порога недостаточно одного инцидента или нападения, однако кумулятивные последствия атак (например, кража интеллектуальной собственности) были настолько значительными, что требуют нового подхода.

В связи с этим Америка пересмотрела предыдущие политические решения, которые ограничивали военные кибер-операции военными сетями, за исключением тех случаев, когда они проводились в зонах объявленных военных действий. Вместо этого киберстратегия 2018 года ориентирует кибервойска США на «прогрессивную защиту» – для пресечения или прекращения злонамеренной киберактивности в ее источнике, а также для постоянного оспаривания подобной активности в повседневной конкуренции. Основной целью данной тактики является снижение эффекта от вредоносных киберкампаний – снизить их значительность с течением времени.

Таким образом, киберстратегия США перешла от сдерживания к попыткам лишить конкурентов возможности добиться успеха. Ключевым элементом настойчивого взаимодействия является концепция «инициативы». С оперативной точки зрения, захват и поддержание инициативы означает создание и изменение условий безопасности, чтобы поставить конкурента в невыгодное положение или заставить его перестроиться. Эта доктрина была опробована на выборах в США в 2020 году. В этот период американские военные предупредили иностранных партнеров, которые неосознанно являлись организаторами вредоносной деятельности, помогли им защитить свои сети и уведомили индустрию, чтобы помочь устранить пробелы.

На уровне теории стратегии это новый мир – отчасти. Появился новый понятийный аппарат, в котором речь идет о проведении кампаний, а не об инцидентах, о взаимодействии, а не об эскалации. Активность непрерывна, а не эпизодична. Она накапливается, использует уязвимости. В дополнение к постоянному взаимодействию у нас есть «передовая оборона», «передовые операции по поиску», наступательные операции и информационные операции.

Происходит фундаментальный сдвиг в наших представлениях о нападении и обороне, а также о войне как таковой. В отличие от обычной войны, где победа достигается на поле боя, и в отличие от ядерной войны, где победа определяется отсутствием войны, новая теория кибервойны – это непрерывная деятельность на уровне ниже порога вооруженного конфликта; сохранение инициативы, как альтернатива войне. Цель – предвидение, защита на опережение во времени и сокращение возможностей, доступных конкуренту.

Повторюсь, сегодня все крупные кибердержавы действуют более или менее схожим образом. Эти страны утверждают (или утверждали бы, если бы признали это), что их деятельность разрешена международным правом. Так ли это, и вписываются ли они в рамки и укладываются ли они в формирующиеся нормы Организации Объединенных Наций, до конца не проанализировано.

К сожалению, с этим подходом связано много проблем. Во всем мире, в небольших странах и особенно в неприсоединившихся государствах, выражается сильная озабоченность по поводу растущей секьюритизации киберпространства и потенциала для дальнейшей эскалации гонки кибервооружений.

Эта тактика проводится всеми конкурентами безоговорочно в защиту своих собственных национальных интересов, при том, что интересы союзников и партнеров могут не полностью совпадать с интересами крупной державы. Таким образом, нынешний подход вызывает обеспокоенности у стран по поводу того, что они могут оказаться в центре соперничества крупных кибердержав и будут вынуждены выбирать сторону.

США не остаются в стороне от этой критики, но, по крайней мере, они ведут себя прозрачно, что само по себе является стабилизирующим фактором, повышающим предсказуемость. Отсутствие прозрачности в отношении характера и масштабов постоянного

участия различных субъектов создает нестабильность в киберпространстве и увеличивает вероятность просчетов. Вы находите в своей сети код конкурента и не знаете, с какой целью он там находится. Это дестабилизирующий и опасный фактор.

Какова альтернатива? Некоторые считают, что альтернативой является многоуровневое киберсдерживание – стратегия, которая сочетает в себе множество инструментов власти и сосредоточена в меньшей степени на нападении и в большей степени на обороне, основанной на позитивных целях, связанных с долгосрочной национальной стратегией. Степень изменения структуры международной системы менее значительна, чем степень роста связей между государствами и обществом. В мире по-прежнему существуют великие державы, международные институты и глобализированная экономическая деятельность. Задача состоит в том, чтобы защитить эти связи, а не использовать их для проведения однократных атак в киберпространстве или даже кампаний.

Аргумент здравый, но предлагаемая стратегия, в той мере, в какой она еще не утвердилась в национальной практике, избегает признания новой реальности. Действительно, кибер-операции нельзя рассматривать изолированно. Государства уже реагируют на кибератаки, используя угрозы применения военной силы, судебные обвинения, санкции и множество других инструментов. Более того, тот факт, что большая часть критически важной инфраструктуры находится в частных руках, меняет отношение государств к конкуренции в киберпространстве. Государство не должно переходить в наступление, если его собственные частные сети не являются достаточно защищенными и устойчивыми, и государство не может обеспечить непрерывность экономических процессов и другие меры, необходимые для возвращения сетей в рабочее состояние после крупного киберинцидента. Но они наступают, и их сети, равно как и их экономика находятся под угрозой.

Сегодня, вместо того чтобы работать над тем, чтобы сделать Интернет более безопасным и надежным, государства используют публичное пространство Интернета как зону конфликта без правил. Это подобно тому, как, если бы соперничающие кланы сражались на агоре, открытой рыночной площади, или на школьных дворах. Правительства должны сдерживать подобное поведение. Они должны работать над достижением официальных соглашений, основанных на договоренностях, уже достигнутых в Организации Объединенных Наций, о цивилизованных правилах ведения конфликта в киберпространстве. Они должны внедрять, соблюдать и обеспечивать соблюдение этих правил.

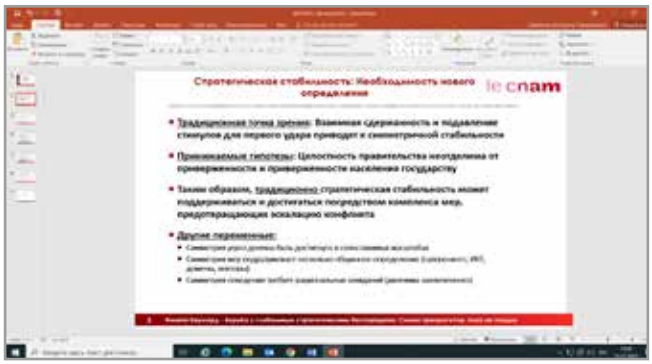
Такие правила должны быть расширены и включать положения об уведомлении третьих стран перед проведением операций в их сетях или через них. Кроме того, государства должны сотрудничать в деятельности по отслеживанию и наказанию киберпреступников, действующих внутри своих стран. Они должны требовать от компаний выпускать более безопасную продукцию. И они должны просвещать своих граждан по вопросам кибербезопасности. Только в случае принятия этих мер киберпространство сможет реализовать свой истинный потенциал как полезная технология для всех человеческих начинаний.

Спасибо за внимание.

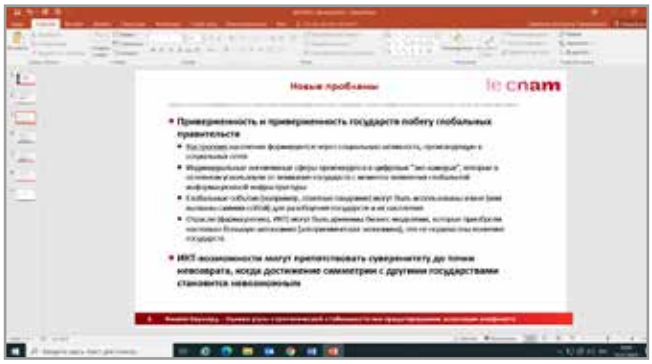
Филипп Бомард
Политехническая школа Парижа (Франция)
Директор исследовательской группы по вопросам безопасности и обороны (ESDR3C) - Cnam

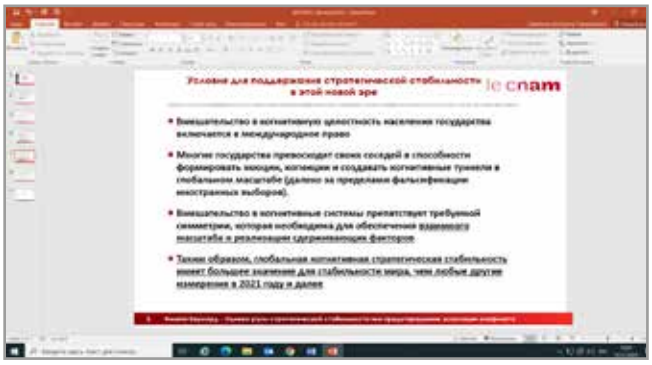
ОЦЕНКА УГРОЗ СТРАТЕГИЧЕСКОЙ СТАБИЛЬНОСТИ ИЛИ ПРЕДОТВРАЩЕНИЕ ЭСКАЛАЦИИ КОНФЛИКТА

СТРАТЕГИЧЕСКАЯ СТАБИЛЬНОСТЬ. НЕОБХОДИМОСТЬ НОВОГО ОПРЕДЕЛЕНИЯ:

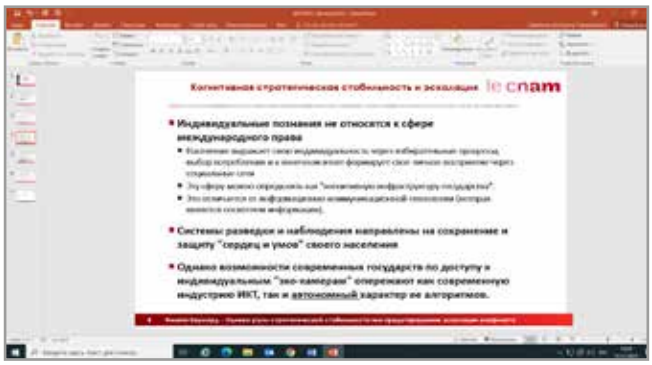


УСЛОВИЯ ДЛЯ ПОДДЕРЖАНИЯ СТРАТЕГИЧЕСКОЙ СТАБИЛЬНОСТИ В ЭТОЙ НОВОЙ ЭРЕ:

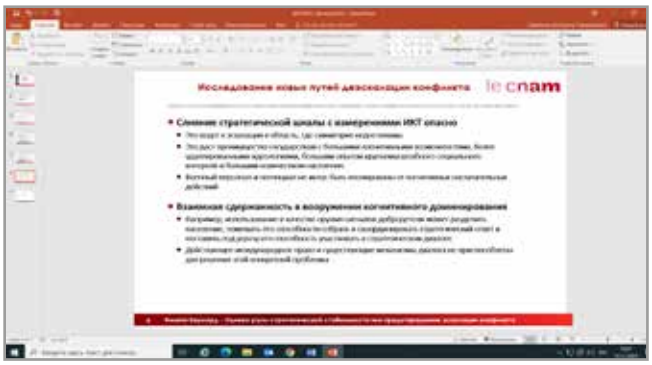




КОГНИТИВНАЯ СТРАТЕГИЧЕСКАЯ СТАБИЛЬНОСТЬ И ЭСКАЛАЦИЯ:



ИССЛЕДОВАНИЕ НОВЫХ ПУТЕЙ ДЕЭСКАЛАЦИИ КОНФЛИКТА:



Н.П. Ромашкина[1]
К.полит.н., профессор, центр международной безопасности Института мировой экономики и международных отношений имени Е. М. Примакова (ИМЭМО) РАН

ВЛИЯНИЕ ИКТ НА УРОВЕНЬ СТРАТЕГИЧЕСКОЙ СТАБИЛЬНОСТИ: НОВЫЙ ФОРМАТ

Уважаемые коллеги!

Мне приятно, что сегодня можно констатировать выход на новый формат проблемы обеспечения стратегической стабильности и влияния на ее уровень со стороны информационно-коммуникационных технологий (ИКТ). Речь идет не только о признании наличия этой проблемы, но и о возобновлении межгосударственных переговоров на высоком уровне по этой проблематике.

Ведь еще совсем недавно на самых различных площадках звучали мнения о том, что обсуждать даже на экспертном уровне вопросы увязки ядерных и кибер проблем в военной области нецелесообразно, что никакие договоренности в этой области невозможны и так далее.

Однако естественный процесс развития научно-технического прогресса, в том числе, в военной области и, в том числе, в сфере ИКТ, приводит к созданию новых возможностей как наступательных, так и оборонительных вооружений. В то же время естественное осознание уязвимости от ускоренного роста вероятности применения вредоносного ИКТ в военной сфере привели к тому, что эта тема обрела новый формат.

После заявлений Президента России В.В. Путина в 2020–2021 годах о необходимости подписания как двусторонних между РФ-США документов, в частности, Двустороннего межправительственного соглашения о предотвращении инцидентов в информационном пространстве, а также универсальных международно-правовых договорённостей, направленных на предупреждение конфликтов и выстраивание взаимовыгодного партнёрства в мировом информационном пространстве, эта проблема обрела реальное воплощение.

Так, на брифинге для иностранных военных атташе 24 декабря 2020 года Начальник Генерального штаба ВС РФ генерал армии В.В. Герасимов отметил: «Военное противоборство распространяется на киберпространство и космос, в результате повышаются риски возникновения инцидентов из-за вмешательства в функционирование систем управления и обеспечения применения ядерного оружия… В этих условиях ключевым элементом обеспечения военной безопасности Российской Федерации остается ядерное сдерживание»[2].

Проблема влияния ИКТ на уровень международной безопасности и стратегической стабильности также звучала во многих выступлениях и на ежегодной Московской конференции по международной безопасности Министерства Обороны России в июне 2021 года.

В своем докладе на открытии Конференции Министр обороны Российской Федерации С.К. Шойгу, говоря об актуальных проблемах международной безопасности, сообщил, что «Гиперзвук, цифровизация и роботизация выходят на первый план при разработке новых

1 Ромашкина Наталия Петровна, Руководитель подразделения проблем информационной безопасности ЦМБ ИМЭМО РАН, профессор, член-корреспондент АВН РФ, кандидат политических наук, Romachkinan@yandex.ru.

2 Начальник Генерального штаба ВС РФ генерал армии Валерий Герасимов провел брифинг для иностранных военных атташе. Официальный сайт Министерства обороны Российской Федерации. https://function.mil.ru/news_page/country/more.htm?id=12331668@egNews.

вооружений. Космос и киберпространство всё активнее вовлекаются в военное противоборство. В составе вооружённых сил ряда стран создаются космические и киберкомандования, главной задачей которых является не оборона, а планирование и проведение наступательных операций в соответствующих сферах. Бережное отношение к международным обязательствам подменяется односторонними санкциями и внедрением некоего порядка, основанного на неизвестно кем придуманных правилах. Мир стремительно погружается в новое противостояние, гораздо более опасное, чем во времена холодной войны»[3].

Логично, что во время военных учений передовых в военном отношении государств, указанная проблема уже учитывается. В России, по данным Министерства обороны, подобные задачи решались в ходе учения в Кемеровской области в сентябре 2021 года: связисты общевойскового объединения Центрального военного округа отразили кибератаку условного противника на засекреченные каналы связи и обеспечили скрытое управление войсками. По замыслу учения отрабатывался один из актуальных в настоящее время сценариев вредоносного использования ИКТ: условный противник предпринял попытку сетевой атаки на засекреченные каналы связи по управлению войсками с целью искажения и подмены передаваемой информации. В ответ на эти действия был организован непрерывный мониторинг работоспособности техники и создан специальный технологический барьер, препятствующий сетевой атаке. Получая информацию об очередной попытке кибератаки операторы в ручном режиме производили блокировку атакованного канала связи и переходили на резервные проводные и спутниковые каналы связи[4].

Важнейшим фактором, определяющим выход указанной проблемы на новый формат, стало объявление о запуске российско-американского диалога по стратегической стабильности по итогам встречи президентов России и США В.В. Путина и Дж. Байдена в Женеве 16 июня 2021. В Совместном заявлении Президентов России и США по стратегической стабильности указано, что Россия и Соединенные Штаты будут участвовать в «интегрированном двустороннем диалоге о стратегической стабильности», цель которого «заложить основу для будущего контроля над вооружениями и мерам по снижению риска»[5]. После завершения саммита В.В. Путин назвал решение начать двусторонние консультации в сфере кибербезопасности «чрезвычайно важным» – как для Москвы и Вашингтона, так и для всего мира.

По заявлениям зам. Министра иностранных дел С.А. Рябкова, в основе будущих договоренностей по стратегической стабильности должно лежать новое «уравнение безопасности», в котором учитывались бы все факторы, влияющие на эту сферу, в том числе стратегические оборонительные и наступательные вооружения в их взаимосвязи, а также стратегические наступательные вооружения в неядерном оснащении, то есть системы, позволяющие без применения ядерных боезарядов решать задачи стратегического характера в плане поражения целей на территории другой стороны. Архиважны заявления России о том, что в этом новом «уравнении безопасности» нужно учесть ситуацию в космосе, где нарастает опасность гонки вооружений, а также проблемы кибербезопасности[6].

Первый раунд переговоров РФ-США по стратегической стабильности прошел в Женеве 28 июля, второй – 30 сентября 2021 года. Российскую межведомственную делегацию возглавляет заместитель Министра иностранных дел РФ С.А. Рябков, американскую – первый заместитель государственного секретаря У. Шерман. На втором заседании было принято решение о формировании двух рабочих групп: Рабочую группу по принципам и задачам будущего контроля над вооружениями и Рабочую группу по потенциалам и действиям, способным иметь стратегический эффект.

3 Министр обороны Российской Федерации открыл IX Московскую конференцию по международной безопасности. Официальный сайт Министерства обороны Российской Федерации. https://mil.ru/mcis/news/more.htm?id=12368274@egNews.

4 Связисты ЦВО отразили кибератаку условного противника на засекреченные каналы связи. Официальный сайт Министерства обороны Российской Федерации. https://function.mil.ru/news_page/country/more.htm?id=12384785@egNews.

5 Совместное заявление Президентов России и США по стратегической стабильности. Президент России. http://www.kremlin.ru/supplement/5658.

6 Рябков: новое «уравнение безопасности» с США должно учитывать тематику кибербезопасности. ТАСС. https://tass.ru/politika/11535921.

После встреч в рамках рабочих групп запланировано третье пленарное заседание[7].

Таким образом, переговоры по стратегической стабильности нацелены не только на достижение нового договора по ограничению стратегических ядерных вооружений в перспективе. Обсуждению подлежат меры прозрачности и снижения рисков непреднамеренной или преднамеренной эскалации с использованием ядерного оружия во время кризиса или конфликта. Кроме того, планируется работа по анализу выдвигаемых доктрин, которые могут усугубить напряженность или усложнить управление возникающими кризисами.

Однако, существует огромное количество проблем, затрудняющих диалог. Речь идет об отсутствии общего понимания даже самого термина «стратегическая стабильность», что можно было предвидеть после длительного вакуума – по сути более 20 лет – конструктивного диалога между РФ и США по этой проблематике. Логично, что в таких условиях Россия и США предлагают разные концепции, и, следовательно, имеют разные приоритеты в отношении вновь зарождающегося диалога. Спорными и сложными для достижения компромисса ожидаемо являются вопросы противоракетной обороны США и их союзников; включение в диалог всех типов систем вооружений с возможным стратегическим эффектом, как ядерных, так и неядерных; стратегические системы доставки ядерных вооружений средней и межконтинентальной дальностей; тактическое ядерное оружие; деструктивное влияние ИКТ на военно-политические процессы и т.д., и т.д.

Поэтому обсуждение вопросов кибербезопасности в рамках этого комплексного диалога в Женеве максимально важно. Речь идёт об очень широком спектре вопросов, которые появились за долгий период отсутствия диалога. В частности, это озабоченности России в отношении планов США по противоракетной обороне, усиливающие угрозы от вредоносных ИКТ; рост рисков милитаризации космоса и интереса к новым типам противоспутникового оружия; вмешательство в выборы и др.

На данный момент прошло уже пять основных и промежуточных консультаций между РФ и США по вопросам кибербезопасности. Кроме того, за истекший период продолжались контакты в формате видеоконференцсвязи на уровне экспертов, обмен посланиями и сигналами на уровне посольств.

Важнейшим результатом этой работы можно считать уже само начало российско-американского диалога по этим максимально актуальным и жизненно важным вопросам. Кроме того, по заявлениям сторон, уже отработан формат участников и практика обмена мнениями помимо проведения онлайн-встреч по закрытому каналу. Запланированы новые контакты в предстоящий период.

Однако, американская сторона, пытаясь добиться односторонних преимуществ, на переговорах по кибербезопасности стремится всю работу сфокусировать исключительно на интересах США, игнорируя озабоченности России в этой сфере. Россия готова обсуждать с американцами то, что их интересует (сейчас это, прежде всего, пресечение деятельности хакерских группировок, атакующих объекты в США при помощи вирусов-вымогателей), но считает, что разговор по этой теме должен включать не только обсуждение нападения каких-то группировок на мясокомбинат с целью получения выкупа, но и многие другие аспекты: «При всем значении, которое американская сторона придает тому, что она считает хакерскими атаками кибермошенников, мы должны посмотреть на кибербезопасность и с точки зрения более прямой связки с задачей укрепления стратегической стабильности в целом»[8]. Россия, в частности, считает важным обсудить риски кибератак на элементы системы управления вооруженными силами.

Расширение тематики и повестки дня с учетом интересов России, по-прежнему, является важнейшей задачей профессионалов из различных областей, но на данном этапе, уже в первую очередь, российской дипломатии. Поэтому тема влияния ИКТ на стратегическую стабильность сегодня максимально важна в стенах Дипломатической Академии.

7 Совместное заявление по итогам встречи в рамках российско-американского диалога по стратегической стабильности в Женеве, 30 сентября 2021 г. 1950-30-09-2021. https://www.mid.ru/diverse/-/asset_publisher/zwl2FuDbhJx9/content/sovmestnoe-zaavlenie-po-itogam-vstreci-v-ramkah-rossijsko-amerikanskogo-dialoga-po-strategiceskoj-stabil-nosti-v-zeneve-30-sentabra-2021-g-.

8 Рябков: Россия и США провели уже четыре раунда консультаций по кибербезопасности. Коммерсантъ. https://www.kommersant.ru/doc/4910861?utm_source=yxnews&utm_medium=desktop.

Сдвиги в этом направлении есть, но они недостаточны. По мнению МИД России, говорить о каких-либо договоренностях обязывающего характера в этой сфере пока преждевременно, так как пока нет опыта в разработке договоренностей обязывающего характера в этой сфере в связи с задачей укрепления стратегической стабильности[9].

Действительно, проблемы согласования и верификации запретов или ограничений систем кибервойны сейчас могут казаться неразрешимыми, но уже сегодня можно надеяться и нужно работать, как минимум, на целенаправленный диалог России и США для заключения взаимного политически обязывающего отказа от кибератак на стратегические управляющие системы друг друга для предотвращения непреднамеренного обмена ядерными ударами. При этом целесообразно использовать опыт обязательств великих держав о ненацеливании ядерных ракет друг на друга, что нельзя проверить, но осуществляется на практике и имеет стабилизирующий политический эффект.

Россия рассчитывает, что диалог с США по кибербезопасности станет регулярным, если будет обсуждаться широкая повестка дня.

Напомню о главных факторах влияния ИКТ на уровень стратегической стабильности, а также о самых опасных ИКТ-уязвимостях в стратегических ядерных силах. Они представлены на слайдах.

В контексте нового формата проблемы влияния ИКТ на уровень стратегической стабильности в настоящее время достаточно остро встает вопрос о перспективах подписания юридически обязывающих документов. Это связано со следующей проблемой. С одной стороны, в настоящее время новейшие системы оружия и военные технологии, в том числе, ИКТ создают трудности для развития контрольно-ограничительных режимов в отношении стратегической стабильности. С другой стороны, новые ИКТ-возможности объективно добавляют неопределенности, а, следовательно, повышают риски начала ядерной войны. А значит, и в дальнейшем способствуют осознанию этой угрозы, осознанию равной для всех субъектов стратегической стабильности уязвимости. А это в результате приводит к достижению компромисса.

Эта проблема по многом стала одной из причин возникновения теории о том, что перемены миропорядка и революционные военные технологии требуют упразднения переговоров и договоров по ограничению вооружений, в том числе, кибернетических, заменяя их многосторонними форумами государств и экспертов широкого профиля – в целях согласования некоей общей философии стабильности. Кроме того, звучат доводы за полный отказ от контрольно-ограничительных договоров в пользу военного соперничества без правил – для достижения стратегического превосходства. А это прямой путь к катастрофе.

В настоящее время осознание значения контроля над вооружениями, желание и умение последовательно добиваться соглашений в этой области, опираясь на полувековой опыт своих предшественников, играет глобальную роль. В результате мир сможет избежать новых циклов гонки вооружений, дальнейшего распространения ядерного оружия, роста количества конфликтов с высокой вероятностью эскалации к широкомасштабной ядерной войне.

При наличии политической воли сторон, система ограничения и нераспространения вооружений может быть сохранена и адаптирована для охвата многих новейших дестабилизирующих вооружений. Как бывало и в прошлом, не все инновационные технологии можно уже сейчас или завтра взять под контроль. Однако, продолжение продуктивного переговорного процесса – при ведущей роли России и США – является непременным условием последующего включения новейших вооружений и технологий в договорно-правовые режимы. Это необходимо и для будущей перестройки системы контроля над вооружениями с двухстороннего на многосторонние форматы, и для создания базы по обеспечению необходимого и достаточного уровня стратегической стабильности.

В недавнем интервью, говоря о проблеме кибербезопасности, Директор Службы внешней разведки России С.Е. Нарышкин отметил: «Конечно, мы следим за развитием в этой

9 Ждем «предметной реакции». Рябков дал оценку переговорам с США в Женеве. 28.07.2021. РИА-Новости. https://radiosputnik.ria.ru/20210728/ryabkov-1743345002.html?chat_room_id=1743345002.

сфере, потому что мы не должны отстать, и мы должны обеспечить национальную безопасность, включая кибербезопасность... Мы видим, как наши партнеры наращивают свой наступательный киберпотенциал как в Соединенных Штатах, так и странах-членах НАТО, но я могу заверить, что Россия способна обеспечить и обеспечит информационную безопасность. Россия вносит свой вклад в создание системы глобальной безопасности в киберсфере»[10].

Логично предполагать, что одной из важнейших задач при этом является международно-правовое обеспечение стратегической стабильности с учетом ИКТ-угроз.

Более подробно о проблеме влияния ИКТ на уровень стратегической стабильности вы можете прочитать в монографиях нашего подразделения Проблем информационной безопасности ЦМБ ИМЭМО РАН им. Е.М. Примакова и, в частности, в монографии «Международная безопасность, стратегическая стабильность и информационные технологии» (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/files/File/ru/publ/2020/2020-017.pdf).

Спасибо за внимание!

10 Dumb intelligence? Sergey Naryshkin, director of the Russian Foreign Intelligence Service 26 Sep, 2021. https://www.rt.com/shows/worlds-apart-oksana-boyko/535830-intelligence-information-dumb-naryshkin/.

Сильвия Тот
Сотрудник по вопросам кибербезопасности, Организация по безопасности и сотрудничеству в Европе

УСИЛИЯ ОБСЕ ПО РАЗРАБОТКЕ И ВНЕДРЕНИЮ МЕР УКРЕПЛЕНИЯ ДОВЕРИЯ В ОБЛАСТИ ИКТ И КИБЕРБЕЗОПАСНОСТИ

Организация по безопасности и сотрудничеству в Европе 10 March 2016 Постоянный совет

1092-е пленарное заседание
PC Journal No. 1092, пункт 1 повестки дня

Решение № 1202
Меры укрепления доверия в рамках обсе с целью сокращения рисков возникновения конфликтов в результате использования информационных и коммуникационных технологий

В Решении № 1039 Постоянного совета (26 апреля 2012 года) государства-участники ОБСЕ постановили активизировать самостоятельные и коллективные усилия по обеспечению безопасности при всеобъемлющем и межизмеренческом использовании информационных и коммуникационных технологий (ИКТ) в соответствии с обязательствами в рамках ОБСЕ и во взаимодействии с соответствующими международными организациями, о чем далее будет говориться как о «безопасности при использовании ИКТ и самих ИКТ». Они далее постановили разработать проект комплекса мер укрепления доверия (МД) с целью повышения межгосударственного сотрудничества, транспарентности, предсказуемости и стабильности и уменьшения рисков ошибочного восприятия, эскалации и конфликтов, которые могут возникнуть в результате использования ИКТ.

Государства – участники ОБСЕ, напоминая о роли ОБСЕ в качестве регионального соглашения по смыслу главы VIII Устава ООН, подтверждают, что разрабатываемые в ОБСЕ МД дополняют усилия ООН по содействию принятию МД в сфере безопасности при использовании ИКТ и самих ИКТ. При осуществлении согласованных в рамках ОБСЕ мер укрепления доверия в сфере безопасности при использовании ИКТ и самих ИКТ государства – участники ОБСЕ будут руководствоваться: международным правом, включая, среди прочего, Устав ООН и Международный пакт о гражданских и политических правах; хельсинкским Заключительным актом; а также взятыми ими на себя обязательствами по уважению прав человека и основных свобод.

Следующие МД были первоначально приняты Решением № 1106 Постоянного совета от 3 декабря 2013 года:

1. Государства-участники будут на добровольной основе представлять свои соображения по различным аспектам национальных и транснациональных угроз в сфере безопасности при использовании ИКТ и самих ИКТ. Объем такой информации будет определяться представляющими ее сторонами.
2. Государства-участники будут на добровольной основе облегчать сотрудничество между национальными компетентными органами и обмениваться информацией по вопросам безопасности при использовании ИКТ и самих ИКТ.
3. Государства-участники будут на добровольной основе проводить консультации на надлежащем уровне с целью снизить вероятность ошибочного восприятия и возможного возникновения политической или военной напряженности либо конфликта, которые могут

возникнуть в результате использования ИКТ и обеспечить защиту критически важной национальной и международной ИКТ-инфраструктуры, включая обеспечение ее целостности.

4. Государства-участники будут на добровольной основе делиться информацией о принятых ими мерах по обеспечению открытости, функциональной совместимости, безопасности и надежности Интернета.
5. Государства-участники будут использовать ОБСЕ в качестве платформы для диалога, обмена передовым опытом, повышения осведомленности и информирования о наращивании потенциала в отношении безопасности при использовании ИКТ и самих ИКТ, в том числе об эффективном реагировании на угрозы в этой сфере. Государства- участники будут изучать вопрос о дальнейшем повышении роли ОБСЕ в этом отношении.
6. Государствам-участникам желательно ввести современные эффективные национальные законодательные нормы, позволяющие облегчить на добровольной основе двустороннее сотрудничество и эффективный своевременный обмен информацией между компетентными ведомствами, включая правоохранительные органы, государств-участников с целью противодействия использованию ИКТ в террористических или преступных целях. Государства – участники ОБСЕ соглашаются в том, что ОБСЕ не будет дублировать усилия, прилагаемые по существующим правоохранительным каналам.
7. Государства-участники будут на добровольной основе обмениваться информацией о своей организационной структуре, стратегиях, политике и программах, в том числе о сотрудничестве между государственным и частным секторами, в сфере безопасности при использовании ИКТ и самих ИКТ, причем ее объем будет определяться представляющими ее сторонами.
8. Государства-участники определят контактный пункт, предназначенный для упрощения связи и ведения диалога по вопросам безопасности при использовании ИКТ и самих ИКТ. Государства-участники будут на добровольной основе представлять контактные данные о существующих официальных национальных структурах, которые занимаются инцидентами, связанными с ИКТ, и координируют принятие мер реагирования, с целью создать условия для прямого диалога и облегчения взаимодействия между уполномоченными национальными ведомствами и экспертами. Государства-участники будут ежегодно обновлять контактную информацию и уведомлять о происшедших в ней изменениях не позднее чем через 30 дней после того, как они произошли. Государства-участники будут на добровольной основе принимать меры, призванные обеспечить оперативную связь на уровне директивных органов, с тем чтобы обеспечить возможность постановки вызывающих озабоченность вопросов уровня национальной безопасности.
9. С тем чтобы снизить вероятность возникновения недопонимания в отсутствие согласованной терминологии и содействовать продолжению диалога, государства- участники в качестве первого шага представят на добровольной основе перечень используемых ими терминов, касающихся безопасности при использовании ИКТ и самих ИКТ, сопровождаемый пояснением или определением по каждому термину. Каждое государство-участник на добровольной основе отберет те термины, которые ему представляются наиболее уместными для обмена. В более долгосрочной перспективе государства-участники попытаются составить согласованный консенсусом глоссарий.
10. Государства-участники будут на добровольной основе обмениваться мнениями, используя, с соблюдением соответствующего решения ОБСЕ, платформы и механизмы ОБСЕ, среди прочего, Сеть связи ОБСЕ, эксплуатируемую Центром по предотвращению конфликтов Секретариата ОБСЕ, с целью облегчить связь по вопросам МД.
11. Государства-участники будут, по меньшей мере, трижды в год проводить

в рамках Комитета по безопасности и его неофициальной рабочей группы (НРГ), учрежденной Решением № 1039 Постоянного совета, совещания на уровне назначенных национальных экспертов с целью обсуждения представленной в ходе обменов информации и рассмотрения вопроса о дальнейшем надлежащем развитии МД. НРГ могла бы в будущем рассмотреть, в частности, предложения, фигурирующие в сводном перечне, распространенном председательством НРГ в виде документа PC.DEL/682/12 от 9 июля 2012 года, на том условии, что до его утверждения будут проведены дискуссии и достигнут консенсус.

Следующие МД были первоначально приняты Решением № 1202 Постоянного совета от 10 марта 2016 года:

12. Государства-участники будут на добровольной основе делиться информацией и облегчать межгосударственные обмены в различных форматах, включая рабочие совещания, семинары и круглые столы, в том числе на региональном и/или субрегиональном уровне; цель этого – изучение целого спектра основанных на сотрудничестве мер, а также других процессов и механизмов, которые могли бы позволить государствам-участникам сокращать риски возникновения конфликтов в результате использования ИКТ. Такая деятельность должна быть направлена на предотвращение конфликтов в результате использования ИКТ и на обеспечение использования ИКТ в мирных целях.

В отношении такой деятельности желательно, чтобы государства-участники среди прочего:

- осуществляли ее в духе упрочения межгосударственного сотрудничества, повышения траспарентности, предсказуемости и стабильности;
- дополняли подобного рода деятельностью усилия ООН и избегали дублирования работы, проводимой на других форумах; и
- учитывали потребности и требования государств-участников, принимающих участие в такой деятельности.

Желательно, чтобы государства-участники приглашали к участию и задействовали в такой деятельности представителей частного сектора, научных кругов, центров передового опыта и гражданского общества.

13. Государства-участники будут на добровольной основе проводить мероприятия для должностных лиц и экспертов с целью оказать поддержку в упрощении использования одобренных властями и защищенных каналов связи для предотвращения и снижения рисков ошибочного восприятия, эскалации напряженности и конфликта, а также с целью уточнения технических, правовых и дипломатических механизмов рассмотрения запросов, касающихся ИКТ. Это не исключает использования каналов связи, упомянутых в Решении № 1106 Постоянного совета.
14. Государства-участники будут на добровольной основе и в соответствии с национальным законодательством способствовать государственно-частному партнерству и развивать механизмы обмена передовым опытом реагирования на общие вызовы безопасности, связанные с использованием ИКТ.
15. Государства-участники будут на добровольной основе поощрять и облегчать региональное и субрегиональное взаимодействие между законно уполномоченными органами власти, отвечающими за безопасность критически важной инфраструктуры, и/или участвовать в этом взаимодействии с целью обсуждения существующих возможностей и решения проблем, стоящих перед национальными и трансграничными ИКТ-сетями, от которых зависит вышеупомянутая критически важная инфраструктура.

Взаимодействие может, в частности, включать в себя:

- обмен информацией об угрозах, связанных с ИКТ;
- обмен передовым опытом;
- разработку, сообразно обстоятельствам, совместных мер реагирования на общие вызовы, включая процеду-

ры регулирования кризиса в случае широкомасштабного или транснационального сбоя в функционировании критически важной инфраструктуры, зависящей от ИКТ;

– принятие на добровольной основе национальных систем классификации инцидентов в сфере ИКТ в зависимости от их масштабов и серьезности;
– обмен мнениями между государствами насчет категоризации той зависящей от ИКТ инфраструктуры, которую они считают критически важной;
– повышение безопасности критически важной национальной и транснациональной инфраструктуры, зависящей от ИКТ, включая обеспечение ее целостности на региональном и субрегиональном уровнях; и
– повышение осведомленности о важности защиты систем управления производственными процессами и о проблемах, касающихся их безопасности, связанной с ИКТ, а также о необходимости разработки процессов и механизмов реагирования на эти проблемы.

16. Государства-участники будут на добровольной основе поощрять ответственное информирование о факторах уязвимости, затрагивающих безопасность при использовании ИКТ и самих ИКТ, и делиться связанной с этим информацией об имеющихся способах устранения таких факторов уязвимости, в том числе с соответствующими секторами ИКТ-индустрии и бизнеса, в целях наращивания сотрудничества и повышения транспарентности в регионе ОБСЕ. Государства – участники ОБСЕ согласны в том, что при осуществлении такого обмена информацией между государствами следует во избежание дублирования усилий использовать одобренные властями и защищенные каналы связи, включая контактные пункты, назначенные в соответствии с МД № 8, изложенной в Решении № 1106 Постоянного совета.

Практические соображения[1]

Положения данного раздела "Практические соображения" не затрагивают принципа добровольности при осуществлении мероприятий, касающихся упомянутых выше МД.

Государства-участники намерены провести первый обмен информацией к

31 октября 2014 года, после чего обмен информацией, предусмотренный в упомянутых выше МД, будет проводиться ежегодно. С целью получения синергетического эффекта государства-участники могут устанавливать сроки проведения ежегодного обмена в синхронизации с другими инициативами в этой области, которые осуществляются ими в рамках ООН и других форумов.

Каждое государство-участник, которое представляет информацию в порядке обмена, обязано прежде свести ее в единый документ. Материалы должны составляться таким образом, чтобы обеспечить их максимальную транспарентность и практическую полезность.

Информация может представляться государствами-участниками на любом из официальных языков ОБСЕ с приложением перевода на английский язык либо только на английском языке.

Информация будет распространяться среди государств-участников с использованием механизма распространения документов ОБСЕ.

Государству-участнику, желающему получить разъяснения по поводу того или иного индивидуального сообщения, предлагается делать это на заседаниях Комитета по безопасности и его неофициальной рабочей группы, учрежденной

Решением № 1039 Постоянного совета, либо посредством прямого диалога с представившим его государством с использованием имеющихся механизмов для контактов, включая список адресов электронной почты и дискуссионный форум POLIS.

Государства-участники будут осуществлять деятельность по изложенным выше пунктам 9 и 10 по линии существующих органов и механизмов ОБСЕ.

Департамент по противодействию транснациональным угрозам будет оказывать госу-

1 Первоначально приняты в качестве составной части Решения № 1106 Постоянного совета от 3 декабря 2013 года.

дарствам-участникам по их просьбе и в пределах имеющихся ресурсов содействие в осуществлении вышеуказанных МД.

При осуществлении МД государства-участники, возможно, пожелают воспользоваться итогами дискуссий и опытом, накопленным в других соответствующих международных организациях, занимающихся проблемами, связанными с ИКТ.

Соображения[2]

Государства-участники будут, по меньшей мере, трижды в год проводить в рамках Комитета по безопасности и его неофициальной рабочей группы, учрежденной Решением № 1039 Постоянного совета, совещания на уровне назначенных национальных экспертов с целью обсуждения представленной в ходе обменов информации и рассмотрения вопроса о дальнейшем надлежащем развитии МД. НРГ могла бы в будущем рассмотреть, в частности, предложения о МД, направленные на укрепление сотрудничества и повышение транспарентности и стабильности в отношениях между государствами при использовании ИКТ. В рамках этих усилий, в той мере, в которой они относятся к мандату НРГ, следует принимать во внимание и стараться дополнять подготовленные на основе консенсуса на уровне экспертов в 2013 и 2015 годах доклады Группы правительственных экспертов ООН по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности, включая их рекомендации о добровольных МД, и работу этой группы по поддержке добровольных, не имеющих обязательной силы норм, правил и принципов ответственного поведения государств при использовании ИКТ.

Департамент Секретариата ОБСЕ по противодействию транснациональным угрозам в лице своего сотрудника по вопросам кибербезопасности будет, по просьбе государств-участников и в пределах имеющихся ресурсов, оказывать им содействие в осуществлении вышеизложенных МД и в разработке возможных будущих МД.

КУРС ЭЛЕКТРОННОГО ОБУЧЕНИЯ ПО МЕРАМ УКРЕПЛЕНИЯ ДОВЕРИЯ В ОБЛАСТИ КИБЕР/ИКТ БЕЗОПАСНОСТИ ОБСЕ

Цели электронного учебного курса:

- Понять более широкий контекст международной кибер/ИКТ безопасности, в частности, основные процессы ООН;
- Понять актуальность международных рамок киберстабильности и роль мер укрепления доверия в этих рамках;
- Понять контекст, в котором были приняты меры укрепления доверия ОБСЕ по кибер/ИКТ безопасности, включая вовлеченных участников и процессы;
- Понять общий характер кибер-мер укрепления доверия, их цель и механизмы действия;
- Вспомнить ключевую направленность каждой из 16 мер укрепления доверия в области кибербезопасности, приводя конкретные примеры их реализации на национальном уровне.
- реализации;
- Оценить кибер-меры укрепления доверия ОБСЕ в более широком региональном и международном контексте;
- Использовать меры укрепления доверия в интерактивном упражнении.

Курс доступен на английском языке: https://elearning.osce.org/courses/course-v1:OSCE+TNTD-%20CYBERCBM_v1+2020_11/about и на русском языке: https://elearning.osce.org/courses/course-v1:OSCE+TNTD-%20CYBERCBM_RU+2021_06/about

Прежде чем получить доступ к курсу, необходимо пройти короткую регистрацию. Прохождение курса занимает примерно 1,5 часа.

2 Первоначально приняты в качестве составной части Решения № 1202 Постоянного совета от 10 марта 2016 года.

И.В. Сурма
Заведующий кафедрой государственного управления во внешнеполитической деятельности Дипломатической академии МИД России, к.э.н., член-корреспондент РАЕН

НАТО-2030: НОВАЯ КИБЕРПОЛИТИКА СЕВЕРОАТЛАНТИЧЕСКОГО АЛЬЯНСА

Базовые стратегии и основы киберполитики Североатлантического альянса

За все время, начиная от создания, развития и нынешнего существования Организация Североатлантического Договора (НАТО) сменила семь стратегических концепций (1950 г., 1952 г., 1957 г., 1968 г., 1991 г., 1999 г., 2010 г.), последняя из которых была утверждена 19 ноября 2010 г. на Лиссабонском саммите НАТО. Первые две стратегические концепции (1950 и 1952 гг.) касались эволюции военно-организационной структуры НАТО, а начиная с 1957 г. Североатлантический альянс, используя элементы концептуального подхода президента Д. Эйзенхауера, утвердил доктрину «массированного ядерного удара». Экспертные доклады «Комитета трёх мудрецов» 1956 г. и доклад Армеля («Будущие задачи альянса») 1967 г. явились основой модернизации стратегии НАТО в соответствующий период своего развития.

Фактически после окончания периода «холодной войны» стратегии 1991 г., 1999 г. и 2010 г. характеризовались переходом к концепции кризисного урегулирования, продвижением демократии и стремлением к вовлечению и сотрудничеству с бывшими представителями советского блока. Концепция 2010 г., в целом, закрепляла роль альянса в качестве «глобального полицейского», но при этом не упоминала ни о растущем значении киберпространства, ни о региональных и глобальных амбициях Китая. В целом после 2010 года Североатлантический альянс стали называть герметичным гибридным альянсом. Но проблема совершенствования политического механизма и развития диалога между странами-союзниками по блоку осталась и до настоящего времени. Исторически НАТО активно стремился к расширению своей «зоны ответственности», принимая во внимание Суэцкий кризис и Венгерское восстание 1956 г. Но именно Суэцкий кризис впервые указал на важность политического диалога в рамках альянса для предупреждения возможных разногласий среди стран-союзников: вначале между Великобританией и Францией и США, позднее после Берлинского кризиса 1961 г., а также выхода Франции из НАТО в 1966 г. и с переходом к стратегии «гибкого реагирования» в целом между европейскими странами и США. Трансатлантический раскол в связи с интервенцией в Ирак в 2003 г. С одной стороны усилил поворот ЕС в сторону стратегической автономии, а с другой посеял сомнения в американской среде о надёжности и полезности союзников по НАТО и в необходимости согласовывать или обсуждать с ними действия на международной арене. В последние годы Североатлантический альянс также сталкивается с накопившимися внутренними проблемами. Так, президент Франции прямо говорил о «смерти мозга НАТО», а европейские страны прорабатывают возможность создания собственного военного блока. США и Турция, имеющие особую роль в организации, рассорились из-за поставок российской военной техники и, кроме того, возможно возникновение новых противоречий, которые, в конечном итоге, ухудшат общую ситуацию в НАТО. Косвенно об этом свидетельствует и учреждение НАТО альтернативных платформ для проведения международных операций – Европейской инициативы реагирования (EI2) в июне 2018 г.

и Совместного экспедиционного корпуса под командованием Великобритании (JEF), который также официально начал полноценную работу в июне 2018 г. Эти инициативы возникли во многом в связи с недостатком оперативности в деятельности НАТО при решении таких вопросов безопасности как несостоявшиеся государства, терроризм и незаконная миграция, по которым весьма трудно достичь единогласия среди участников.

Кроме того, эксперты по итогам президентства Д. Трампа стали говорить о необратимой потере доверия между союзниками, поэтому в процессе последнего саммита в Брюсселе была осуществлена попытка эту ситуацию смягчить. Тем не менее, общий список угроз пока недостаточно структурирован, а финансовые обязательства четко не прописаны, что отражает несовпадение интересов в области безопасности и разную степень оценки угроз, как и разный уровень интересов и возможностей по финансированию общего бюджета альянса. Поэтому в начале 2022 г. Европейский Союз собирается принять «Стратегический Компас» как рамочную стратегию для многих реализуемых ЕС инициатив в области обороны и безопасности, которая должна, в конечном счете, определить модель взаимоотношений ЕС-НАТО.

В целом, по итогам саммита Североатлантического альянса 14 июня 2021 г. утверждение новой стратегической концепции планируется на следующем саммите в Испании в 2022 г. Решение о разработке комплекса мер по совершенствованию структур и стратегий было принято еще в декабре 2019 г. на саммите НАТО в Лондоне. В соответствии с этим решением, планировалось собрать несколько групп специалистов, которым предстояло изучить текущую обстановку и определить наиболее вероятные сценарии ее развития. В апреле 2020 г. была сформирована «независимая группа» при генеральном секретаре организации, ответственная за выработку плана «НАТО-2030». В нее вошли десять опытных политиков из разных стран. В течение нескольких следующих месяцев этот совет провел десятки различных встреч и мероприятий с участием специалистов. В ноябре группа издала доклад «NATO 2030: United for a New Era».

Документ описывает текущие и ожидаемые вызовы и угрозы, сильные и слабые стороны НАТО, а также способы совершенствования имеющихся стратегий и структур. В общей сложности предлагается порядка 140 различных мер и решений.

Наряду с привлечением экспертов, впервые в истории НАТО к выработке новой стратегии было подключено и молодое поколение. В ноябре 2020 года была собрана «группа молодых лидеров» из 14 специалистов, которые 4 февраля 2021 г. представили доклад «NATO 2030: Embrace the Change, Guard the Values». Параллельно с этим проводились мероприятия при участии студентов ряда американских и европейских вузов, которые в будущем могут стать новыми руководителями НАТО.

В конечном итоге, доклад совета при генсеке предлагает несколько основных мер, которые, должны позволить адаптировать НАТО к новым вызовам. Так, общие цели и задачи Альянса должны оставаться прежними – коллективная безопасность, совместное выполнение различных мероприятий, сотрудничество с нейтральными странами и т.д. При этом в руководящие документы предлагается официально внести новую цель в виде противодействия КНР и России, а также иные актуальные угрозы.

В составе организации должен появиться новый военно-аналитический орган с участием разных стран. Его задачей станет постоянный анализ обстановки и возникающих ситуаций с целью своевременного выявления новых угроз. Также предлагается сформировать специализированный орган, который будет следить за действиями России и Китая.

В составе НАТО должно появиться собственное агентство перспективных разработок по типу американского DARPA, которое обеспечит более эффективный обмен современными разработками и технологиями между странами организации. Одновременно, для сокращения известных рисков, требуется сократить или исключить доступ Китая к перспективным европейским разработкам. Союзники договорились ускорить инновации в области гражданской и военной обороны для Северной Атлантики (DIANA – Defence Innovation Accelerator for the North Atlantic). Этот «ускоритель» будет стимулировать трансатлантическое сотрудничество в области критически важных технологий, способствовать интероперабельности (функциональной

совместимости) и применять гражданские инновации путем взаимодействия с научными кругами и частным сектором, включая стартапы. DIANA будет иметь представительства и испытательные центры по всему Альянсу, а также будет управлять базой данных о надежных источниках инвестиций. Союзники также договорились о создании многонационального инновационного фонда НАТО, в который страны-члены могут вносить взносы на добровольной основе, для инвестирования в стартапы, работающие над технологиями двойного назначения и новыми подрывными технологиями и инновациями в областях, имеющих решающее значение для безопасности стран-союзников по Альянсу.

Комплексная политика кибероборонны и действующие программы НАТО в сфере IT, связи и киберпространстве

Основные итоги саммита НАТО в Брюсселе (14 июня 2021) в области кибербезопасности показали, что НАТО стремится к укреплению институциональных позиций в области развития инновационных технологий и обеспечения кибербезопасности. С этой целью Альянс ведет разработки в области развития сетей 5G, военных и передовых технологий связи, стратегических коммуникаций и искусственного интеллекта.

Планируется принять ряд следующих мер:

- по повышению защищенности объектов критически важной инфраструктуры, каналов поставок стратегических ресурсов и информационно-коммуникационных сетей (в первую очередь стандарта 5G);
- предполагается расширять информационный обмен в рамках альянса о вредоносной активности в компьютерном пространстве;
- отдельное внимание в ближайшей перспективе намечено уделить выработке единых стандартов обеспечения устойчивости стран блока к гибридным угрозам.

Кроме того, предусматривается создание специализированного комитета НАТО для контроля над выполнением данных задач.

Участники саммита утвердили всеобъемлющую политику альянса в области кибероборонны для реагирования на систематичные хакерские атаки и прочие киберпреступления. Констатируется, что НАТО «будет продвигать свободное, открытое, мирное и безопасное киберпространство», а также продолжит прилагать усилия «по повышению стабильности и снижению риска конфликтов, поддерживая международное право и добровольные нормы ответственного поведения государства в киберпространстве». Кроме того, в последние годы Североатлантический Альянс активизировал свою работу по новым технологиям, в том числе путем принятия стратегии внедрения, направленной на обеспечение превосходства НАТО в семи ключевых технологиях (искусственный интеллект, данные и вычисления, автономность, квантовые технологии, биотехнологии, гиперзвуковые технологии и космос).

Среди основных программ НАТО по развитию информационной безопасности, связи и искусственного интеллекта можно выделить следующие:

1. Технологии 5G
2. Спутниковые коммуникации SATCOM (Satellite Communication)
3. Стратегические коммуникации STRATCOM (Strategic Communication)
4. Разработка автономных интеллектуальных агентов киберзащиты AICA (Autonomous Intellectual Cybersecurity Agent)

В рамках программ НАТО одним из приоритетных направлений является обеспечение безопасности при внедрении сетей поколения 5G. Концепция безопасности 5G включает гибкость реагирования на новые угрозы и автоматизированные системы, использующие искусственный интеллект, но безопасность в системах 5G связана с рядом проблем:

- виртуализация сетевых функций и ресурсов;
- уязвимость элементов 5G;
- цепочки поставок оборудования 5G.

Проблема виртуализации сетевых функций и ресурсов связана с переносом функциональных возможностей, которые предоставляются аппаратными средствами в область программного обеспечения. Это связано с появлением программно-определяемых сетей (Software Defined Network, SDN) и программно-определяемой радиосистемы (Software Defined Radio, SDR). Происходит разделение

платформы сетевого устройства на независимые унифицированные компоненты аппаратное «железо», операционную систему и приложения. Сетевая виртуализация и методы разделения (концепция Network Slicing) позволяют запускать несколько логических сетей как независимые операции в общей физической инфраструктуре.

Каждый сетевой сегмент представляет собой независимую виртуализированную сквозную сеть и позволяет операторам параллельно развертывать несколько служб с разными архитектурами в одной и той же физической сети. Общие физические платформы в инфраструктуре 5G могут использоваться для создания скрытых каналов.

Проблема, связанная с тремя основными элементами 5G: улучшенная мобильная широкополосная связь; связь на основе массивных машин (Massive machine type communications, mMTC); и сверхнадежная связь с малой задержкой (Ultra-Reliable Low-Latency Communication, URLLC). Элементы mMTC и URLLC обеспечивают массовое масштабирование и строгие требования к надежности, но также расширяют возможности для кибератак для новых типов устройств, например, датчиков и киберфизических систем, автономной транспортировки, дополненной и виртуальной реальности. Например, злоумышленники смогут взять под контроль любое автономное транспортное средство.

Проблема надежности поставок для сетей 5G заключается в возможности нарушений конфиденциальности и безопасности. Например, США оказывают давление на союзников по НАТО в отношении использования оборудования Huawei.

Huawei Technologies лидирует по количеству заявленных патентов 5G, Samsung и LG Electronics занимают, соответственно, второе и третье места в мире. Среди десяти ведущих компаний в этой категории только две находятся в Европе: Nokia и Ericsson, две в США: Qualcomm и Intel.

SATCOM (*Satellite Communications*) определяется НАТО как мгновенное глобальное соединение с коммуникационной инфраструктурой НАТО, передача критически важных разведданных, способность устанавливать жизнеспособные коммуникации в местах с ограниченной или отсутствующей инфраструктурой и т.д. (по данным NATOs Mission-Critical Space Capabilities under Threat: Cybersecurity Gaps in the Military Space Asset Supply Chain).

Эта программа обеспечивает прямой доступ к космическим активам и связанными с ними услугами. Космические активы представляют системы сбора разведывательных данных и связи о военных маневрах кораблей, самолетов, телекоммуникациях и финансах. Это позволяет обеспечить защиту национальной безопасности НАТО, а также структурировать внешнеполитический курс.

Системы спутниковой связи могут обеспечивать постоянное беспроводное покрытие, чтобы дополнять и расширять наземные сети связи. Они будут включены в беспроводные сети 5G и их последующие расширения.

Сегодня на системах LEO (Low Earth Orbit) запущено несколько проектов, например, OneWeb и SpaceX для обеспечения бесперебойной связи.

Стратегические коммуникации STRATCOM (*Strategic Communication*). Одним из главных подразделений НАТО, ведущих информационную работу в отношении России, является Центр передового опыта в области стратегических коммуникаций (StratCom), расположенный в Риге и соучредителями которого выступили Латвия, Литва, Эстония, Польша, Германия, Италия и Великобритания. В официальном пресс-коммюнике альянса говорится, что создание центра в 2014 году стало «ответом НАТО на активизацию России в информационном пространстве».

Идея стратегической коммуникации стала новой концепцией, включающей в себя целый спектр возможностей публичной дипломатии и общественных отношений, начиная от убеждений при помощи информационно-психологических операций и заканчивая непосредственно применением силы. Основными функциями центра в Риге являются работа со СМИ, информирование о деятельности НАТО с помощью инструментов публичной дипломатии, развитие гражданско-военных связей и проведение информационно-психологических операций. Рижский центр регулярно организует различные конференции, издает журналы и публикует доклады о результатах проведенных исследований. Сектор рассматриваемых проблем включает различные аспекты, такие как:

1. особенности тактики ведения информационной войны с применением «мемов»;
2. кибервойна;
3. основные нарративы экстремистских организаций;
4. безопасность в Европейском союзе;
5. биометрические технологии;
6. национализм и др.

В работе центра передового опыта в Риге России уделяется достаточно пристальное внимание. Изучаются особенности применения современных информационных технологий в российской армии. Кроме того, публикуются материалы о якобы «российском вмешательстве на Украине», а также обзоры санкций против России. Продвигая мысль об активном вмешательстве России и о ведение ею гибридной войны, Рижский центр стратегической коммуникации НАТО (STRATCOM) ранее опубликовал несколько аналитических исследований «Кремлевский Сборник Пьес. Понимание российского влияния в Центральной и Восточной Европе», «Когда гибридная война поддерживает идеологию: Россия сегодня» и «Кибервойна Путина: государственная политика России в пятой области» (2016), а также исследования о военных маневрах России (2020).

Любопытно, что в состав центра входят подразделения, название которых свидетельствует о характере деятельности, далекой от заявленной научно-методической – например, некий «отдел оперативной поддержки». Интересно также, что директор StratCom Янис Сартс в одном из интервью заявлял, что центр «не проводит психологических операций». Однако на его сайте можно найти определение «стратегических коммуникаций», одной из составляющих которых являются «информационные операции». В свою очередь, одной из целей таких «информационных операций» заявлена «деятельность по созданию желаемого воздействия на волю, понимание и возможности противников и других сторон». Ежегодно организация выпускает около десяти объемных материалов жесткой антироссийской направленности, а за все время существования центра было выпущено около 50 таких документов. Особое место среди них занимает материалы по истории России и стран постсоветского пространства. Центр также отрабатывает тематику «агрессивной политики России в Европе и в отношении стран СНГ», а также внутриполитические проблемы РФ.

Партнерами StratCom являются Королевский колледж Лондона и Стэнфордский университет (США). Материалы центра в переводе на русский язык публикуются на сайте телерадиокомпании «Радио Свобода» (организация включена Минюстом в список иноагентов).

Кроме этого, с 2015 года в рамках программ STRATCOM, GLOBSEC Policy Institute (GPI) отслеживает дезинформационную и пропагандистскую деятельность и публикует анализ дезинформационных действий в форме еженедельного журнала Information War Monitor для Словакии, Чехии и Венгрии; проводит регулярные исследования манипуляций в социальных сетях и пр.

Разработка автономных интеллектуальных агентов киберзащиты AICA (Autonomous Intellectual Cybersecurity Agent). Сложность инфраструктуры информационных технологий требует новых подходов к обеспечению кибербезопасности. Концепция разработок AICA заключается в формировании поля взаимодействия в области кибератак и киберзащиты между искусственными интеллектуальными объектами без участия человеческих ресурсов. AICA разрабатываются для оборонных информационных систем управления, но могут использоваться в любой другой области обеспечения информационной кибербезопасности. AICA имеет ряд функций для обеспечения своей работы: зондирование и идентификация состояния мира. Функция высокого уровня AICA позволяет агенту киберзащиты получать данные из среды, систем, в которых он работает и от самого себя (самообучение) для достижения понимания текущего состояния мира и обнаружения рисков. При зондировании используются два источника данных: внешние (связанные с системой и устройством) дескрипторы текущего состояния мира и внутренние (связанные с агентом) дескрипторы текущего состояния.

При идентификации состояния мира также используются два источника данных: обработанные дескрипторы текущего состояния и паттерны состояния изученного мира. Паттерны состояния изученного мира хра-

нятся в репозитории мировых знаний агента. Обработанные дескрипторы текущего состояния и паттерны состояния изученного мира сравниваются для выявления проблемных паттернов текущего состояния мира (то есть таких, которые представляют аномалию или риск). При выявлении проблемного паттерна текущего состояния мира функция определения состояния мира запускает следующую высокоуровневую функцию планирование и выбор действий. Это высокоуровневая функция AICA, которая позволяет агенту киберзащиты разработать от одного до нескольких предложений действий и предложить их функции выбора действий, которая определяет действие или набор действий для выполнения.

Вместо заключения

Результаты анализа свидетельствуют о дуальной природе НАТО в международных отношениях. На официальном уровне присутствует декларативное сотрудничество, и на неофициальном уровне сохранение антагонистической повестки.

Каждая программа НАТО направлена на сдерживание и/или предотвращения кибератак со стороны России, Китая и других потенциальных противников. С этой целью детально изучаются программы кибербезопасности в России, законодательство в этой области. Разрабатываются системы раннего обнаружения кибератак и дезинформационных атак.

В рамках проектов НАТО разрабатываются программы по стратегическим коммуникациям, внедрению специальных киберагентов для поиска вредоносного ПО, и обеспечению спутниковой связи.

Проекты характеризуются:

- высокой политизацией сферы наукоемких технологий;
- стремлением обеспечить лидерские позиции США в развитии стратегических приоритетных направлений;
- сдерживанием потенциальных противников;
- всесторонним анализом аналогичных проектов в странах не членах НАТО.

В заключение подчеркнем, что чрезвычайно важной линией киберполитики НАТО и коллективного Запада, вообще, является восприятие Российской Федерации как одного из главных агрессоров в киберпространстве. Более того, они имеют достаточно согласованную позицию и политику по вопросам кибербезопасности. Экспертные сообщества и политический истеблишмент стран Запада склонны обвинять Россию в организации массовых кибератак на их информационную инфраструктуру. Ранее заместитель помощника генпрокурора США Ричард Даунинг заявил, что Россия возглавляет список стран, с территорий которых осуществляются кибератаки против Соединённых Штатов. По его словам, при этом он «не стал бы утверждать, что правительство России стоит за этими атаками»[1].

Тем не менее, позиция Запада основывается на многочисленных и порой противоречащих друг другу идеях, включая различия в подходах к обеспечению кибербезопасности, особенно в вопросах активной киберзащиты и ответных мер. Каждая страна имеет достаточно четкую позицию по этим вопросам, определяемую, прежде всего, национальными интересами. Но так как Интернет не признает государственных границ, поэтому будущее как национальной, так и международной кибербезопасности будет зависеть от того, насколько государства будут готовы к конструктивному диалогу и сотрудничеству в решении актуальных проблем информационной безопасности. Для России имеет значение – понижение порога реакции на потенциальные угрозы кибербезопасности, главным виновником которых часто называют Москву. В этой сфере действительно необходимо продолжение серьезного диалога. Поддержание взаимодействия по тем вопросам, где это возможно – единственный способ если не улучшить отношения России и НАТО, то хотя бы не допустить их дальнейшей деградации.

Список литературы

1. Biscop S. EU and NATO Strategy: A Compass, a Concept, and a Concordat. – Security Policy Brief № 141, March 2021.

1 Россия, начиная с 2020 года ответила на 12 запросов правоохранительных органов США по кибератакам. Без реакции американской стороны остаются запросы российских компетентных органов относительно кибератак. В 2020 году таких было 45, а в первом полугодии 2021 года — 35.

2. Conley H. A. The Strategic Argument for a Political NATO – NDC Policy Brief № 5, March 2021.
3. Galic M. Navigating by Sun and Compass. – Policy Brief Three: The Future of Japan-NATO Relations, January 2021.
4. Olesen M. R. What to Do About China? Forging a Compromise between the US and Europe in NATO. – DIIS Policy Brief, January 2021. 5. Wivel A., Crandall M. Punching Above Their Weight, But Why? Explaining Denmark and Estonia in the Transatlantic Relationship // Journal of Transatlantic Studies, Vol.17, Issue 3, 2019, pp. 392-419.
5. Указ Президента России от 15 января 2013 г. № 31с. «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации»// Информационно-правовой портал «ГАРАНТ.РУ»: [сайт]. – URL: https://www.garant.ru/products/ipo/prime/doc/70199068/ (дата обращения: 29.07.2021). – Текст: электронный.
6. Концепция государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации: [Утверждена Президентом РФ 12.12.2014 № К 1274] // Справочно-правовая система «Консультант Плюс»: [сайт]. – URL: http://www.consultant.ru/document/cons_doc_LAW_181661/7327668c04c0470317b26d354e36cb828a4af319/ (дата обращения: 21.07.2021). – Текст: электронный.
7. Смирнов А.И. Новейшие киберстратегии США – преамбула войны?/ А.И.Смирнов // Международные процессы. - 2018. Том 16. Номер 4 (55). с. 181–192
8. Resolution adopted by the General Assembly on 5 December 2018. 73/27. Developments in the field of information and telecommunications in the context of international security: [сайт]. – URL: https://undocs.org/A/RES/73/27 (дата обращения: 21.07.2021). – Текст: электронный.
9. Резолюция Генеральной Ассамблеи ООН 73/266 от 22 декабря 2018 года. Поощрение ответственного поведения государств в киберпространстве в контексте международной безопасности: [сайт]. – URL: https://undocs.org/ru/A/RES/73/266 (дата обращения: 20.07.2021). – Текст: электронный.
10. Hybrid Threats Description 1500/CPPCAM/FCR/10-270038 AND 5000 FXX/0100/TT-0651/SER: NU0040 Dated 25 August 2010: BI-SC Input for a new Capstone Concept for The Military Contribution to Countering Hybrid Threats dated (para 7)) : [сайт]. – URL: https://www.act.nato.int/images/stories/events/2010/20100826_bi-sc_cht.pdf (дата обращения 30.07.2021). – Текст: электронный.
11. Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization: [сайт]. – URL: https://www.nato.int/cps/ru/natohq/topics_82705.htm (дата обращения 30.07.2021). – Текст: электронный.
12. Бартош А. Гибридные войны в стратегии США и НАТО./А.Бартош// : [сайт]. – URL: https://topwar.ru/60101-gibridnye-voyny-v-strategii-ssha-i-nato.html (дата обращения 01.08.2021). – Текст: электронный.
13. Смирнов А.И. Современные информационные технологии в международных отношениях: монография. / А.И. Смирнов. - Москва: МГИМО-Университет, 2017. С. 248.
14. Tallinn Manual on the International Law Applicable to Cyber Warfare / M.N. Schmitt. Cambridge University Press, 2013. 300 p.
15. Tallinn manual 2.0 on the international law applicable to cyber operations / ed. by M.N. Schmitt. Cambridge University Press, 2017. 638 p.
16. Москва знает о центрах антироссийской пропаганды в Прибалтике – мнение: [сайт]. – URL: https://regnum.ru/news/polit/3341326.html (дата обращения 15 августа 2021) . – Текст: электронный.
17. Конли, Дж. Мина, Р. Стефанов, М. Владимиров. – «Кремлевский Сбор-

ник Пьес. Понимание российского влияния в Центральной и Восточной Европе»: [сайт]. – URL: https://www.stratcomcoe.org/hconley-jminarstefanov-mvladimirov-kremlin-playbook-understanding-russian-influence-central-and (дата обращения 02.08.2021). – Текст: электронный.
18. Когда Гибридная Война Поддерживает Идеологию: Russia Today: [сайт]. – URL: https://www.stratcomcoe.org/when-hybrid-warfare-supports-ideology-russia-today (дата обращения 31.12.2019). – Текст: электронный.
19. Сурма И.В. Цифровая дипломатия в дискурсе глобальной политики./ И.В. Сурма// Вестник МГИМО Университета. – 2014. №6(39). – с.53-60
20. Фоксолл А. «Кибервойна Путина: государственная политика России в пятой области»: [сайт]. – URL: https://www.stratcomcoe.org/afoxall-putins-cyberwar-russias-statecraft-fifth-domain (дата обращения 01.08.2021). – Текст: электронный.
21. Сурма И.В. Международные исследовательские центры по проблемам войны, мира и безопасности. / И.В.Сурма// В сборнике: Государственное управление во внешнеполитической деятельности и международная безопасность. Сборник научно-практических материалов. Сер. «Государственная гражданская служба – дипломатическая служба и внешнеполитическая деятельность: основы государственного управления»: – Москва, 2013. – с. 260–261.
22. Аникин В.И., Абдеев Р.Ф., Сурма И.В. Философские аспекты информационной цивилизации и современные проблемы управления в ракурсе глобальной безопасности. // В.И.Аникин, Р.Ф.Абдеев, И.В.Сурма// Вопросы безопасности. – 2017. №2. – с.44–54.
23. Brussels Summit Declaration Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Brussels 11-12 July 2018: [сайт]. – URL: https://www.nato.int/cps/en/natohq/official_texts_156624.htm (дата обращения: 08.08.2021). – Текст: электронный.

Лю Чуанинь
Директор Исследовательского центра глобального киберпространства и управления (КНР)

СОЗДАНИЕ ПОРЯДКА И МЕХАНИЗМА УПРАВЛЕНИЯ В ЦИФРОВОМ ПРОСТРАНСТВЕ

Быстрый рост цифровых технологий и данных выявил острую необходимость наведения порядка в цифровом пространстве. Однако на самом деле, прежде чем навести порядок, необходимо решить множество проблем. С одной стороны, технологии и бизнес стремятся создать единое, стандартизированное и интегрированное цифровое пространство. С другой стороны, международная структура и дилеммы безопасности побуждают мощь политики и национальной безопасности участвовать в построении порядка в цифровом пространстве, которые демонстрируют философию управления, отличную от философии технологий и бизнеса. В этом докладе сначала уточняется определение понятия «цифровое пространство», затем определяются новые вызовы, стоящие перед наведением порядка в цифровом пространстве, и предлагается, чтобы все страны укрепляли сотрудничество и совместно строили сообщество общего будущего в цифровом пространстве.

I. Понимание «цифрового пространства»

Вообще говоря, «пространство» – это восприятие и объективное описание объективной среды, в которой живут люди. Социологическое значение «пространства» в большей степени связано с развитием социальной деятельности человека и продолжением социальных отношений. Эдвард В. Соджа, ведущий мировой теоретик пространства, считал, что первое пространство – это физическая среда, которую можно нанести на карту, количественно измерить и «увидеть» в реальном мире. Второе пространство – это концептуальное пространство, которое создается в умах людей, его населяющих. Третье пространство – это «реальное и воображаемое» пространство, пространство жизни, то, в котором люди действительно живут и которое они ощущают. По его мнению, третье пространство – это жизнь, которую мы проживаем как индивиды, то есть опыт, который мы получили от общества, и наш индивидуально воображаемый опыт с социальным пространством в целом[1]. С развитием технологий социологи после Соджи стали более остро осознавать влияние современных технологий на восприятие и формирование пространства. Дэвид Харви считал, что традиционное пространство – это объективное и независимое существование, которое «натурализовано»[2]. Однако с развитием технологий и коммуникаций восприятие людьми времени и пространства полностью изменилось. Время объединяет различные пространства, образуя новое пространство.

Следует отметить, что пространство в социологическом смысле не только рассматривает особенности пространств, такие как отличительные качества земли, воздуха, моря, космоса и киберпространства, но и подчеркивает общность пространств, то есть пространство – это место, где человечество получает ресурсы, расширяет сферу деятельности и формирует социальные отношения с помощью науки и техники. Например, освоение

1 Соджа, Эдвард В. и Вера Чуинард. "Третье пространство: путешествия в Лос-Анджелес и другие реальные и воображаемые места". Canadian Geographer 43.2 (1999): 209.

2 Харви, Дэвид. Пространство как ключевое слово. na, 2006.

морского пространства неотделимо от навигационных технологий; освоение космического пространства неотделимо от космических аппаратов; а освоение киберпространства неотделимо от интернет-технологий. Поэтому очень важно понимать следующие два момента, касающиеся «пространства»: Во-первых, пространство может существовать физически или виртуально, или даже в духовном мире людей; во-вторых, ценность пространства заключается в том, позволяет ли оно человечеству получать доступ к ресурсам и осуществлять деятельность в нем. Эти два положения закладывают основу для обсуждения «нового пространства», порожденного развивающимися наукой и технологиями, включая «киберпространство» и «цифровое пространство».

Поэтому данный отчет также подходит к понятию «цифровое пространство» с социологической точки зрения. В нем обсуждается революционное воздействие технологических инноваций на традиционное пространство. В частности, он фокусируется на том, как создается новое пространство и формирует социальную производственную деятельность человека и его социальное взаимодействие. В данном отчете предлагается понять «цифровое пространство» со следующих точек зрения.

Во-первых, с точки зрения преобразующего воздействия технологий и их применения на пространство, цифровое пространство – это «оцифровка» всех пространств. В настоящее время в международных научных и политических кругах нет четкого определения понятия «пространство». Китайские ученые довольно рано выдвинули концепцию «цифрового пространства». Вэй Фэнгси, академик Китайской академии наук, считал, что в буквальном смысле «цифровое пространство» означает пространство, созданное путем оцифровки восприятия и применения пространства на Земле[3]. Как он сказал в своей речи: «Почти десять лет я думал о том, как интегрировать знания и применение космоса с развитием информационных технологий, чтобы осуществить интеграцию технологий и экономики и лучше содействовать развитию человеческого общества. Цифровой космос», как важная развивающаяся стратегическая область, несомненно, является хорошей отправной точкой. Прогресс космических технологий, расширение соответствующих знаний, повышение потенциала использования, расширение применения технологий и быстрое развитие информационных технологий – все это говорит о том, что наступает эра «цифрового космоса»[4]. Его точка зрения подтверждается тем, что проект «Стратегические исследования цифрового пространства» был одобрен на второй сессии шестого консультативного комитета Академии наук Китая.

Профессор Вэй подчеркнул, что «цифровой космос» – это новый рубеж, объединяющий космическую науку, технику, применение и обслуживание с развитием современных информационных технологий. Таким образом, ученые рассматривают «цифровое пространство» как традиционное понятие пространства, включающее землю, воздух, море и космическое пространство, а также киберпространство, оцифрованное с помощью новых информационных технологий, таких как большие данные и искусственный интеллект, основанных на космических коммуникационных сетях, включающих спутники и навигационные системы. Чжоу Хунжэнь, исполнительный заместитель председателя Консультативного комитета по государственной информатизации Китая, который является пионером в деле информатизации Китая, считает, что киберпространство и физическое пространство тесно переплетены и обмениваются информацией посредством непрерывного гомоморфного отображения и обратной связи[5].

Поэтому «цифровое пространство» – это не столько новое пространство, сколько «модернизация» всех пространств. По этой причине ученые рассматривают развитие «цифрового пространства» как важный стратегический шаг, призванный сломать нынешнюю пространственную модель мира.

Во-вторых, с точки зрения влияния на социальную деятельность человека, цифровое пространство – это новая область интеллектуальной трансформации об-

3 魏奉思：《数字空间 "是空间科技战略新高地》，中国科学院官网，2016年9月6日：http://www.cas.cn/zjs/201609/t20160906_4573875.shtml

4 Там же

5 周宏仁：《网络空间的崛起与战略稳定》，《国际展望》2019年第3期，第21-34页。

щества. Ян Цзе, председатель China Mobile, выступил с программной речью на MWC21 28 июня 2021 года. Он сказал: «По мере того как информационные технологии следующего поколения, представленные 5G, все быстрее интегрируются в экономику, общество и жизнедеятельность людей, формируется цифровое пространство, которое отображает реальный мир и сосуществует с ним. В будущем, с ускорением миграции повседневной жизни людей и производственной деятельности, такой как развлечения, общение и транзакции, в цифровое пространство, ИТ и данные будут усиливать, контролировать и умножать ценность традиционных факторов, включая труд и капитал, более значительными способами. А они, в свою очередь, подталкивают человечество к преодолению препятствий в развитии и достижении скачкообразного роста производительности. Расширение цифрового пространства, по сути, является прогрессом цифро-интеллектуальной трансформации экономики и общества, а именно процессом преобразования реального мира с помощью ИТ и данных.»[6] Цифровое пространство – это не просто отображение реального общества, а скорее симбиоз, где все аспекты социальной жизни находятся в процессе цифро-интеллектуальной трансформации, формируя тем самым новую социальную форму.

В-третьих, с точки зрения эффективного управления, цифровое пространство в будущем станет серьезным вызовом для международного управления. Цифровое пространство – это новый рубеж, который несет в себе бесконечный потенциал развития для человеческого общества и представляет собой направление дальнейшей эволюции информационного общества в будущем. Поэтому стратегическая важность разумного и упорядоченного развития цифрового пространства очевидна. Международному сообществу необходимо направлять развитие цифрового пространства в сторону рационального развития и эффективного управления на благо человечества. Однако история доказала, что развитие нового несет в себе как возможности, так и вызовы. Цифровое пространство, или цифровая трансформация всех пространств, представляет собой беспрецедентные вызовы[7]. Существующие модели и механизмы управления должны быть адаптированы к потребностям новой цифровой эры, что требует не только фундаментального изменения концепции, но и серьезных инноваций в управлении[8]. Поэтому международное управление цифровым пространством требует совместных усилий всех сторон международного сообщества. Они должны сосредоточиться на технологических и социальных последствиях, вызванных цифровой трансформацией, укрепить международное сотрудничество и координацию, а также изучить новую структуру управления.

II. Проблемы установления порядка в цифровом пространстве

Дилемма безопасности для цифровых технологий

С быстрым развитием цифровых технологий вопросы безопасности стали новым фактором, влияющим на принятие решений. Развитие цифрового пространства прошло через множество этапов, но никогда не обходилось без проблем безопасности. По мере усложнения и широкого применения цифровых технологий стратегическая ценность цифрового пространства становится все более значимой, а важность безопасности поднимается на беспрецедентную высоту. Стоит обратить внимание на следующие проблемы безопасности в цифровом пространстве.

Во-первых, уязвимости в системе безопасности – обычное явление. Цифровые технологии построены на кодах, которые имеют непреодолимые недостатки. Чем сложнее программа, тем больше кодов используется, следовательно, больше потенциальных недостатков. Особенно когда различные цифровые технологии применяются вместе, будет больше несовместимостей между кодами разных продуктов[9]. Это и есть уязвимость цифровых

6 杨杰：《加速数智化转型　共创数字空间新世界》，新华网，2021年6月28日：http://www.xinhuanet.com/info/2021-06/28/c_1310032314.htm

7 Абернати, Уильям Дж. и Ким Б. Кларк. "Инновации: Картирование ветров созидательного разрушения". Исследовательская политика 14.1 (1985): 3-22.

Кастельс, Мануэль. Возникновение сетевого общества. Том 12. John wiley & sons, 2011.

9 Хансен, Лене и Хелен Ниссенбаум. "Цифровая катастрофа, кибербезопасность и Копенгагенская школа". International studies quarterly 53.4 (2009): 1155-1175.

продуктов, и хакеры могут использовать эту уязвимость для получения разрешений, чтобы проникнуть в систему и нарушить целостность компьютеров. В результате уязвимости безопасности, вызванные недостатками в кодах, являются обычным явлением в цифровых технологиях и могут быть устранены только с помощью постоянных исправлений, некоторые из которых требуют длительного времени для устранения.

Во-вторых, стоимость поддержания безопасности чрезвычайно высока. В связи с широким применением цифровых технологий в информационном обществе цифровое и традиционное пространство теснее переплетаются. В результате для поддержания цифровой безопасности требуется больше инвестиций, причем не только со стороны государства, но и со стороны предприятий и частных лиц. Это повлечет за собой огромные расходы, и вопрос о том, как покрыть эти расходы, является актуальным. Пока проблема не будет решена, нам придется смириться с тем, что цифровое пространство небезопасно.

В-третьих, ситуация с безопасностью становится все более сложной. По мере ускорения развития цифровых технологий, новые технологии, такие как искусственный интеллект, квантовая информация, облачные вычисления и блокчейн, продолжают прогрессировать, создавая более сложные проблемы безопасности. Традиционные категории сетевой безопасности и информационной безопасности уже не отвечают новым технологиям, поэтому в соответствии с новой ситуацией необходимо создать более сложную когнитивную структуру цифровой безопасности. Таким образом, проблемы безопасности в цифровом пространстве чрезвычайно сложны и находятся за пределами возможностей подавляющего большинства субъектов.

В-четвертых, существует множество ограничений для глобального сотрудничества в области цифровой безопасности. Цифровое пространство является крайне состязательным с точки зрения безопасности, и субъекты надеются получить конкурентные преимущества за счет приобретения технологий безопасности. В то же время, с точки зрения построения порядка, обеспечение безопасности цифрового пространства неотделимо от сотрудничества между крупными державами, а недоверие препятствует такому сотрудничеству. Построить взаимное доверие в цифровом пространстве непросто, поскольку цифровые технологии имеют стратегическую ценность, а обеспечить обнаруживаемость, проверяемость и необратимость в нематериальном цифровом пространстве сложнее, чем в традиционном сотрудничестве в области контроля над вооружениями.

Реинвентаризация суверенитета в цифровом пространстве

В развитии цифрового пространства действуют многочисленные силы. В то время как силы технологий и бизнеса ведут цифровое пространство к унификации, силы политики и национальной безопасности пытаются определить границы цифрового пространства, фрагментируя рынки и даже цепочки поставок и технологические стандарты[10]. Другими словами, игра между странами в цифровом геопространстве угрожает целостности цифрового пространства. Государственные субъекты оказывают влияние, провозглашая суверенитет в цифровом пространстве. По сравнению с физическим пространством, цифровое пространство является виртуальным и не имеет границ, что сильно отличается от физического мира, где формируется и развивается понятие суверенитета. Государственные субъекты укрепляют понимание и регулирование цифровых технологий, а также адаптируют институты к развитию цифровых технологий, чтобы восстановить суверенитет в цифровом пространстве. Однако это противоречит логике развития технологий и бизнеса в цифровом пространстве.

Во-первых, государства усилили регулирование цифровых предприятий, ограничив их бесконтрольное расширение с помощью антимонопольных мер. Китай, США и ЕС активизировали антимонопольные расследования и наложили штрафы за нарушение закона, чтобы снизить недобросовестную конкуренцию, вызванную использованием технологическими компаниями своего доминирующего положения в области масштабов, данных и технологий. Это ограничит экспан-

10 杨剑：《当全球数字生态遭遇霸权政治:5G市场谈判中的 "华为冲突"》，《太平洋学报》2021年第1期：第21-34页。

сию цифровых компаний в будущем. После быстрого роста технологические компании расширяются в традиционные области, что вызывает обеспокоенность правительства по поводу монополий и недобросовестной конкуренции.

Во-вторых, государства создали новые модели управления, в которых технологические предприятия должны взять на себя больше обязанностей по управлению, чтобы реализовать управление цифровыми технологиями. Развитие цифровых технологий обострило проблемы государственного управления. С одной стороны, правительствам трудно адаптироваться к быстрому развитию и широкому применению цифровых технологий, и им приходится наращивать потенциал регулирования. С другой стороны, государства ужесточили надзор за ведущими технологическими предприятиями, требуя от них большей ответственности за управление цифровыми технологиями[11]. Государства переложили затраты на регулирование на технологические компании, требуя от них усиления самоограничения и саморегулирования, что, по сути, является переосмыслением государственной власти в цифровом пространстве.

В-третьих, государства увеличили вклад в цифровые технологии и способствовали лучшему использованию цифровых технологий для удовлетворения национальных стратегических потребностей. Хотя государственные структуры считаются поздними в цифровом пространстве, по мере того, как государство продолжает вкладывать инвестиции в цифровые технологии и цифровые таланты, цифровые технологии все больше внедряются в национальную стратегию. Крупнейшие страны усилили поддержку цифровых технологий для стимулирования промышленного развития. В то же время правительства приспосабливаются к развитию цифровых технологий, создавая новые департаменты. Более того, внедряя инновационный механизм сотрудничества между государственным и частным секторами, государства могут укрепить национальную мощь в области цифровых технологий с помощью предприятий.

Тревоги по поводу национальной безопасности, усиленные цифровым пространством.

Влияние цифровых технологий на национальную безопасность во многом определило поведение государств в цифровом пространстве, вызывая все большее беспокойство по поводу национальной безопасности. Все страны придают большое значение безопасности в цифровом пространстве, но схема взаимодействия между акторами в цифровом пространстве еще не установлена, что оставляет возможности для более легкой эскалации конфликтов, увеличения различий в политике и усиления геополитической игры. В основе такой нестабильности лежит беспокойство государственных субъектов по поводу национальной безопасности.

Во-первых, национальная безопасность в цифровом пространстве – это в значительной степени, если не полностью, новая концепция, которая перевернула традиционное понимание национальной безопасности. В контексте национальной безопасности в цифровом пространстве развитие цифровых технологий носит подрывной характер, а легитимность суверенитета, основанного на территориальном принципе, сталкивается в цифровом пространстве со многими техническими проблемами. Например, Интернет все больше становится «главным полем боя» для иностранных враждебных сил для сбора информации и манипулирования общественным мнением. С точки зрения поддержания национальной безопасности, на техническом уровне невозможно помешать другим странам собирать разведданные в Интернете.

Во-вторых, риски и угрозы в цифровом пространстве растут, а неопределенность появляется. Страны уже имеют уязвимые места с точки зрения национальной безопасности в цифровом пространстве, а растущая неопределенность еще больше усиливает их беспокойство за собственную безопасность. Действия государства в цифровом пространстве в основном считаются «серой зоной». Еще предстоит ответить на многие вопросы, включая то, как повысить уровень осведомленности о национальной безопасности в цифровом пространстве, с какими формами угроз следует бороться и какие последствия при-

11 Фливербом, Миккель, Рональд Дейберт и Дирк Маттен. "Управление цифровыми технологиями, большими данными и интернетом: Новые роли и обязанности для бизнеса". Business & Society 58.1 (2019): 3-19.

дется пережить странам и обществам. Пока эти вопросы не решены, для национальной безопасности в цифровом пространстве все еще существует большая неопределенность.

В-третьих, недостаточный потенциал национальной безопасности, широкое применение цифровых технологий и размытость цифровых границ делают поддержание национальной безопасности сложной задачей. На сегодняшний день трудно обнаружить угрозы в цифровом пространстве, следовательно, трудно предотвратить инциденты, угрожающие национальной безопасности. Многие крупные инциденты безопасности не сразу обнаруживаются государственными органами, ответственными за национальную и кибербезопасность[12]. Взлом SolarWinds, например, поставил в немилость американские агентства по национальной и кибербезопасности, поскольку система обнаружения вторжений Einstein, которая стоила миллиарды долларов, оказалась совершенно бесполезной перед лицом сложной кибератаки.

III. Содействие созданию сообщества с общим будущим в цифровом пространстве

Для решения глобальных проблем в цифровом пространстве странам необходимо идти по пути беспроигрышного сотрудничества и взаимного доверия для общего управления. Укрепление сотрудничества и установление порядка в цифровом пространстве будет способствовать развитию цифровых технологий и решению вопросов безопасности цифровых технологий. Мы призываем международное сообщество укреплять сотрудничество в следующих областях.

Избегайте идеологической конкуренции в цифровых технологиях

Во-первых, цифровые технологии ведут развитие производительности в новом направлении. В цифровую эпоху одним из главных приоритетов страны является полное использование движущей и ведущей роли информационных технологий, активное развитие цифровой экономики и придание нового импульса экономическому развитию[13]. С точки зрения бизнеса, преобразование всех секторов и рынков посредством цифровизации может способствовать производству более качественных товаров и услуг при более низких затратах. В то же время цифровые технологии играют ключевую роль в геополитике. Поэтому, чтобы создать мирную и стабильную среду для развития глобальной цифровой экономики и справиться со сложными и диверсифицированными вызовами цифрового пространства, необходимо избегать идеологической конкуренции в сфере науки и технологий. В условиях конкуренции в цифровом пространстве все стороны должны предотвращать геополитическое мышление в области технологий, избегать увязывания идеологических разногласий с хакерскими атаками в киберпространстве, безопасностью данных и развитием новых достижений науки и техники. Также крайне важно избегать узкого мышления, такого как игра с нулевой суммой, политизация технологических вопросов и технологический национализм.

Во-вторых, странам необходимо совместно создать механизм посредничества в конфликтах, правила обеспечения безопасности данных и систему обеспечения стабильности цепочки поставок посредством откровенного общения. Под эгидой ООН страны должны совместно сформулировать нормы национального поведения в киберпространстве, основанные на принципе равенства. Страны должны участвовать и поддерживать формулирование международных правил в киберпространстве в рамках ООН, использовать существующие механизмы ООН, чтобы облегчить и избежать прямой конфронтации между крупными державами в киберпространстве, а также создать условия для координации между крупными державами. С одной стороны, крупные страны должны управлять своими разногласиями, укреплять сотрудничество и диалог по кибербезопасности, обеспечивать безопасность путем взаимной стратегической сдержанности и расширять общие интересы путем сотрудничества. С другой стороны, крупные страны должны предоставлять общественные

12 Крэмптон, Джереми В. "Собрать все: Национальная безопасность, большие данные и управление". GeoJournal 80.4 (2015): 519-531.

13 习近平：《习近平关于网络强国论述摘编》，求是网，2021年02月03日：http://www.qstheory.cn/laigao/ycjx/2021-02/03/c_1127060232.htm

блага в киберпространстве, осуществлять международное сотрудничество с более активной и открытой позицией и в полной мере учитывать роль правительств, международных организаций, интернет-компаний, технологических сообществ, неправительственных организаций и отдельных граждан.

Облегчение трансграничного потока данных.

По мере цифровизации мировой экономики возникает всеобщая потребность в обеспечении безопасного и свободного потока данных. Безопасность данных имеет огромное значение, особенно в случае трансграничного потока данных, который касается не только личной конфиденциальности, но и промышленных и национальных интересов. Страны осознали стратегическую ценность данных и поэтому ввели политическое вмешательство в трансграничные потоки данных на основании защиты национальной безопасности и интересов. Таким образом, в эпоху цифровой экономики суверенитет данных стал основным проявлением национального суверенитета в цифровом пространстве. В последние годы не прекращаются споры о формулировании и применении правил регулирования трансграничных данных. Политика каждой страны в отношении трансграничных потоков данных неизбежно служит ее собственным политическим и экономическим интересам[14]. Однако «длиннорукая юрисдикция» над данными в глобальном масштабе вызвала широкое сопротивление даже законам, блокирующим потоки данных, в довольно многих традиционных союзниках США и большинстве развивающихся стран, а также обострила конфронтацию и нестабильность в киберпространстве. Чтобы создать равные условия для удовлетворения потребностей развития глобальной цифровой экономики, международное сообщество должно совместно работать над созданием согласованной на международном уровне и единой структуры для координации суверенитета данных и потока данных, чтобы данные могли свободно распространяться и служить благосостоянию человечества.

Прежде всего, странам следует разрешить вводить политику в области данных с определенной степенью гибкости регулирования в соответствии с их различными этапами развития, и избегать необоснованного расширения юрисдикции в области данных с целью ущемления суверенитета данных других стран. Далее, в рамках переговоров по цифровой торговле страны должны разработать международную структуру для трансграничных потоков данных с участием крупнейших стран и регионов, таких как Китай, США и ЕС, которая должна не только обеспечить четкие руководящие принципы соблюдения требований для развития глобального бизнеса, но и отражать инклюзивность и взаимное доверие в глобальном управлении данными и развитии цифровой экономики, а также способствовать равенству и взаимной выгоде в эпоху цифровой экономики.

Содействие многообразию в цепочке поставок ИКТ.

В настоящее время эффективная работа современного общества, будь то государственные функции или система универсального обслуживания, как никогда зависит от цифрового пространства, где безопасность цепочки поставок ИКТ является главной заботой всех сторон. В то же время цепочка поставок ИКТ-индустрии отличается тем, что ее продукты и услуги разрабатываются, интегрируются и поставляются через высоко децентрализованную глобальную цепочку поставок[15]. Однако пересечение технологических недостатков, рыночных монополий и геополитики привело к ухудшению глобального ландшафта цифровой безопасности[16]. Для достижения устойчивого развития глобальной цифровой экономики необходимо построить фундамент доверия между промышленностью и странами.

Во-первых, правительство должно поощрять компании предоставлять больше продуктов, разрушать монополию на глобальном рынке цифровых продуктов и способствовать разнообразию продуктов через промышлен-

14 Вулимири, Ашиш и др. "Wanalytics: Гео-распределенная аналитика для мира с интенсивным использованием данных". Труды международной конференции по управлению данными ACM SIGMOD 2015. 2015.

15 陈晓桦：《ICT供应链安全，我国该如何管理？》，2019年6月28日：http://www.djbh.net/webdev/web/AcademicianColumnAction.do?p=getYszl&id=8a8182566b88e153016b9c3d7998000d

16 Мейнард, Эндрю Д. "Навигация по четвертой промышленной революции". Nature nanotechnology 10.12 (2015): 1005-1006.

ную кооперацию, тем самым повышая безопасность цепочки поставок.

Во-вторых, поставщики цифровых продуктов должны уважать права и интересы пользователей, воздерживаться от злоупотребления властью, предоставляемой технологиями и рынком, и брать на себя ответственность и обязательства по обеспечению безопасности данных, защите частной жизни и безопасности сети.

В-третьих, страны должны создать механизмы укрепления доверия для сдерживания безответственного поведения, такого как установка бэкдора и использование уязвимостей в продуктах ИКТ. Страны должны совместно разработать объективные, справедливые и прозрачные международные стандарты безопасности и меры сертификации для продуктов ИКТ, чтобы предприятия могли направить свою энергию на повышение безопасности цифровых технологий и укрепление общественного доверия в цифровом пространстве.

Укрепление глобального сотрудничества по защите критической информационной инфраструктуры.

Национальная критическая информационная инфраструктура принимает на себя все больше социальных функций. Ее повреждение, хотя и не приведет к прямым жертвам, вызовет социальную панику, если ее нельзя будет мгновенно восстановить. Масштабы ущерба от кибератак, которые продолжают осуществляться по всему миру, свидетельствуют о том, что кибератаки, направленные на критическую инфраструктуру, эволюционируют. С одной стороны, вымогательское ПО и его разновидности стали основным оружием кибердиверсий, серьезно повлияв на ключевые отрасли и сектора, такие как энергетика, финансы, здравоохранение и образование[17]. Более того, лазейки, вредоносные коды и методы сетевых атак на промышленные системы управления были освоены некоторыми странами и хакерскими организациями. С другой стороны, эффект «палки о двух концах» новых технологий продолжает провоцировать появление новых методов и средств сетевых атак. Новые технологии, такие как Интернет вещей, искусственный интеллект, облачные вычисления и блокчейн, порождают новые проблемы. Заражение цепочки поставок, мошенничество с криптовалютой и майнинг предоставляют новые методы для хакеров, спонсируемых государством, и риски безопасности критической инфраструктуры страны растут.

Управление безопасностью в цифровом пространстве должно идти в ногу с меняющейся средой. Выявление уязвимостей и отслеживание атак - это не только сложные проблемы в управлении киберпространством, но и фундаментальные вопросы, влияющие на стабильность киберпространства. Международное сообщество должно начать с этих двух пунктов и в дальнейшем наращивать потенциал для обеспечения безопасности киберпространства.

Во-первых, международное сообщество должно создать взаимовыгодный и стабильно работающий международный механизм управления уязвимостями, который также может стать прорывом для внедрения норм ответственного поведения в киберпространстве. Используя этот механизм в качестве краеугольного камня, страны должны стремиться к укреплению доверия в киберпространстве и устранению потенциальных угроз для цифровых технологий и инфраструктуры, зависящей от цифровых технологий.

Во-вторых, международное сообщество должно создать международный механизм отслеживания атак в киберпространстве. В многосторонних рамках Организации Объединенных Наций следует создать международно признанное, беспристрастное и прозрачное агентство третьей стороны для отслеживания кибератак и способствовать внедрению международного правила, учитывающего эффективность электронного обнаружения, судебный суверенитет и безопасность данных соответствующих стран.

В-третьих, международное сообщество должно обмениваться стандартами и программами по защите международной и внутренней критической информационной инфраструктуры, включая системную безопасность ядерных объектов. Защита критической инфраструктуры является заметной и актуальной проблемой в киберпространстве. Обнаружение и вторжение в информационные системы

17 卿斯汉：《关键基础设施安全防护》，《信息网络安全》2015年第2期：第1-6页。

критической инфраструктуры может повлиять на стабильность киберпространства[18]. Развитые страны в сфере ИТ должны оказывать поддержку в области возможностей обнаружения, отслеживания и обмена информацией об уязвимостях, уделяя особое внимание помощи развивающимся странам в создании потенциала киберзащиты.

В-четвертых, международное сообщество должно найти способы совместного противодействия угрозам кибербезопасности со стороны негосударственных субъектов. В киберпространстве негосударственные субъекты все чаще обладают разрушительными возможностями для подрыва национальной безопасности. Страны должны достичь консенсуса по предотвращению распространения кибероружия и злонамеренного использования кибердеятельности, а также совместно бороться с киберпреступлениями путем сотрудничества.

Библиография

1. 蔡翠红.国际关系中的网络政治及其治理困境[J].世界经济与政治,2011(05):94-111+158-159.
2. 蔡翠红.网络空间的中美关系:竞争、冲突与合作[J].美国研究,2012,26(03):107-121+5.
3. 黄建伟,陈玲玲.国内数字治理研究进展与未来展望[J].理论与改革,2019(01):86-95.
4. 刘杨钺,杨一心.网络空间 "再主权化 "与国际网络治理的未来[J].国际论坛,2013,15(06):1-7+77.
5. 鲁传颖.网络空间安全困境及治理机制构建[J].现代国际关系,2018(11):49-55+66+68.
6. 吕晓莉.全球治理:模式比较与现实选择[J].现代国际关系,2005(03):8-13.
7. 米加宁,章昌平,李大宇,徐磊. "数字空间 "政府及其研究纲领--第四次工业革命引致的政府形态变革[J].公共管理学报,2020,17(01):1-17+168.
8. 沈逸.后斯诺登时代的全球网络空间治理[J].世界经济与政治,2014(05):144-155+160.
9. 沈逸.数字空间的认知、竞争与合作--中美战略关系框架下的网络安全关系[J].外交评论(外交学院学报),2010,27(02):38-47.
10. 徐汉明,张新平.网络社会治理的法治模式[J].中国社会科学,2018(02):48-71+205.
11. 徐顽强.社会治理共同体的系统审视与构建路径[J].求索,2020(01):161-170.

1. Чен, Ю-Че, Фади Салем и Аннеке Зуидервейк. "Управление в эпоху искусственного интеллекта, материалы 20-й Международной конференции по исследованию цифрового управления (DGO2019)". Материалы 20-й Международной конференции по исследованию цифрового управления (DGO2019) (18 июня 2019 года), Dubai. 2019.
2. Дуке, Густаво Гуарин и Хулиан Давид Зулуага Торрес. "Усиление электронной коммерции с помощью блокчейна (DLT): Нормативный парадокс для цифрового управления". Global Jurist 20.2 (2020).
3. Гарриссон Смит, Тревор. "Политизация цифрового пространства: Теория, Интернет и обновление демократии". (2017): 154.
4. Горва, Роберт. "Что такое управление платформами?". Information, Communication & Society 22.6 (2019): 854-871.
5. Линьков, Игорь, и др. "Стратегии управления для устойчивого цифрового мира". Sustainability 10.2 (2018): 440.
6. О'хара, Кирон и Венди Холл. "Четыре интернета: геополитика цифрового управления". (2018).
7. Ван Дийк, Жозе. "Управление цифровыми обществами: Частные платформы, общественные ценности". Computer Law & Security Review 36 (2020): 105377.
8. Витали-Розати, Марчелло. "О редактуре: Структурирование пространства и авторитета в цифровую эпоху". (2018).

18 Колеснюк, Дэн. "Киберпространство и критические информационные инфраструктуры". Informatica Economica 17.4 (2013).

В.И. Булва
Центр международной информационной безопасности и научно-технологической политики МГИМО МИД России, эксперт, помощник директора

ВЫЗОВЫ И УГРОЗЫ СТРАТЕГИЧЕСКОЙ СТАБИЛЬНОСТИ В ИКТ-ПРОСТРАНСТВЕ

Информационно-коммуникационные технологии способствуют не только внутреннему экономическому развитию государства, но и его позиционированию на международной арене. Стремление отдельных государств и их объединений играть доминирующую роль как в сфере технологического развития, так и в области международной информационной безопасности приводит к появлению вызовов и угроз стабильности в ИКТ-пространстве, основные среди которых, по мнению автора, следующее:

1. рост киберугроз;
2. милитаризация киберпространства (силовой компонент американской кибер-политики);
3. сдерживание противника в ИКТ-среде;
4. агрессивная деятельность НАТО;
5. политика киберсакнций, проводимая коллективным Западом.

Развитие ИКТ привело к *экспоненциальному росту угроз в цифровом пространстве.* По данным Совета безопасности Российской Федерации, который ссылается на сведения российских правоохранительных органов, за январь-ноябрь 2020 г. было зафиксировано в 3 раза больше киберпреступлений по сравнению с 2018 г., а за 2020 г. количество преступлений с использованием информационно-коммуникационных технологий увеличилось на 94,6%. При этом, доля киберпреступлений от общего числа правонарушений по статистике МВД за 2020 г. составила 23%[1].

По данным Cision Company, к маю 2020 г., когда не прошло и полгода спустя вспышки пандемии, 46% интернациональных компаний подверглись кибератакам по крайней мере один раз[2]. Что касается банковского сектора, по состоянию на 14 мая 2020 г. количество взломов банковских сетей выросло на 238% с начала года[3].

Возрастает и финансовый ущерб от кибератак. По разным оценка, он может достичь от 6[4] до 8[5] трлн долл. к 2021 г. и превысить 10 трлн долл. к 2025 г[6]. Подобная тенденция негативно может сказаться не только на компаниях-объектах кибератак, но и на государствах, в которых они функционируют, ведь банкротство фирмы означает утрату рабочего места налогоплательщиками (проблема безработицы) и, как следствие, сокращение поступлений в национальный бюджет.

Что касается *милитаризации киберпространства и сдерживания противника в ИКТ-среде,* то эти две тенденции тесно вза-

1 Совбез сообщил о стремительном нарастании киберугроз в 2020 году // Moscow Daily News, 13.01.2021. – URL: https://www.mn.ru/articles/sovbez-soobshhil-o-stremitelnom-narastanii-kiberugroz-v-2020-godu (дата обращения: 07.09.2021).

2 Top Cyber Security Experts Report: 4,000 Cyber Attacks a Day Since COVID-19 Pandemic // Cision – URL: https://www.prnewswire.com/news-releases/top-cyber-security-experts-report-4-000-cyber-attacks-a-day-since-covid-19-pandemic-301110157.html (дата обращения: 07.09.2021).

3 Там же.

4 Cybercrime To Cost The World $10.5 Trillion Annually By 2025 // Steve Morgan, Editor-in-Chief – URL: CyberSecurity Ventures (дата обращения: 07.09.2021).

5 The Global Risks Report 2021 // World Economic Forum, 19.01.2021. – URL: https://www.weforum.org/reports/the-global-risks-report-2021(дата обращения: 07.09.2021).

6 2021 Must-Know Cyber Attack Statistics and Trends // Embroker – URL: https://www.embroker.com/blog/cyber-attack-statistics/ (дата обращения: 07.09.2021).

имосвязаны. Так, в США, которые являются автором и основным проводником стратегии сдерживания и проактивной обороны, в фокусе внимания находится реагирование на киберугрозами всеми возможными средствами, включая военные. Причем объектом реагирования являются «враги американского государства», которые, согласно официальным документам Вашингтона, представляют собой политически неугодные страны (Россия, Китай, Северная Корея).

Важно отметить, что в основе подобного кибersдерживания лежит не принцип паритетности мер реагирования, а идея глобального доминирования Соединённых Штатов в цифровом пространстве. Для достижения этой цели в качестве приоритетной задачи американская администрация определяет развитие механизма сдерживания потенциального противника с опорой на силовой фактор. В частности, речь идет о проведении превентивных кибероперациий, которые наносили бы неприемлемый ущерб оппоненту, с участием партнеров по блоку НАТО. Помимо этого, США сохраняют за собой право применять военную силу в ответ «на любую значительную кибератаку, направленную против американской экономики, правительства или военных»[7] (в декабре 2011 Конгресс США санкционировал возможность осуществления наступательных киберопреаций)[8].

Сегодня Соединённые Штаты реализуют стратегию сдерживания в новых реалиях – в условиях глобальной стратегической конкуренции. Особенность заключается в отсутствие прямых военных киберконфликтов, которые подпадали бы под понятие «акт агрессии»[9]. В связи с этим, оказывается недостаточно ни традиционного метода наказания (введение ответных мер, в том числе непропорциональных по масштабу), ни ранее популярного метода воспрещения (повышение уровня оборонного потенциала собственного государства для того, чтобы убедить потенциального противника в бесполезности кибератаки). Поэтому в дополнение к ним, Министерство обороны США опирается на нанесение упреждающих ударов в рамках кибероперациий, которые не переходят на стадию военного конфликта, укрепляя тем самым не только собственные позиции в ИКТ-среде, но и подрывая превосходство потенциальных противников[10].

На практике, реализацию подобного подхода можно проследить *в деятельности военно-политического блока НАТО*. Страны Альянса регулярно проводят киберучения в непосредственной близости от российских границ. Например, с 2010 г. проходят учения Locked Shields, задача которых «стимулировать рост сотрудничеств» в ИКТ-пространстве между членами Передового центра кибернетической обороны (расположен в Таллине, Эстония), государствами НАТО и партнерами Альянса[11]. Крупнейшими являются учения Cyber Coalition, ориентированные на повышение оборонного потенциала блока.

Кроме того, Североатлантический Альянс способствовал созданию Центра кибербезопасности для ВС Монголии[12] и Центр реагирования на киберинциденты для ВС Молдовы[13], государств-соседей РФ. Этим странам была оказана техническая помощь, содействие в подготовки специалистов, а также осуществлены поставки необходимого оборудования в рамках программы «Наука ради мира и безопасности».

НАТО продолжает курс на укрепление внутреннего киберпотенциала государств-членов, конечная цель которого – сокращение

7 A Report to Congress Pursuant to the National Defense Authorization // Department of Defense: Policy Report, November 2011. – URL: https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-059.pdf (дата обращения: 07.09.2021).

8 Congress Authorizes Offensive Military Action in Cyberspace / Steven Aftergood // December 14, 2011. – URL: https://fas.org/blogs/secrecy/2011/12/offensive_cyber/ (дата обращения: 07.09.2021).

9 Fischerkeller M. P., Harknett R. J. What Is Agreed...; Fischerkeller M. P., Harknett R.J. Persistent Engagement and Cost Imposition: Distinguishing Between Cause and Effect/ Lawfare. Washington, DC, 2020. – URL: https://www.lawfareblog.com/persistent-engagement-and-cost-imposition-distinguishingbetween-cause-and-effect (дата обращения: 29.07.2021).

10 The Department Of Defense Cyber Strategy 2018: Summary / U.S. Department of De-fense. Washington, DC, 2018. P. 1, 2. – URL: https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/%20CYBER_STRATEGY_SUMMARY_FINAL.PDF (дата обращения: 29.07.2021).

11 The NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). About us // URL: https://ccdcoe.org/about-us/ (дата обращения: 05.05.2020)

12 НАТО способствует укреплению потенциала киберзащиты Монголии // Официальный сайт НАТО – URL: https://www.nato.int/cps/ru/natohq/news_180697.htm?selectedLocale=ru (дата обращения: 09.03.2021)

13 В Республике Молдова при поддержке НАТО создан потенциал реагирования на киберинциденты – URL: https://www.nato.int/cps/ru/natohq/news_180758.htm?selectedLocale=ru (дата обращения: 09.03.2021)

цифрового разрыва между странами Альянса. Так, в рамках программ блока внедряются современные системы связи (Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance), проводятся реформы структур управления ВС, осуществляется переподготовка кадров и вноситься необходимые корректировки в нормативно-правовые национальные документы.

Особую настороженность в России вызывает политика НАТО по борьбе с дезинформацией на различных уровнях (дипломатическом, экономическом, военном и информационном) в рамках «противодействия гибридным угрозам»[14]. Для этих целей были сформированы центры антироссийской пропаганды в Варшаве, Риге и Таллине[15]. На базе данных подразделений готовятся кадры и создается «информационное оружие» для его последующего распространения на территории РФ.

Наконец, озабоченность российского руководства вызывает *политика санкционного давления,* проводимая коллективным Западом. Осенью 2020 г. США ввели санкции в отношении 7 российских граждан, нескольких компаний, функционирующих на территории РФ[16] и правительственного исследовательского института[17] за нанесение экономического ущерба Соединённым Штатам в ходе кибератак. Европейский Союз впервые задействовал механизм киберсанкций против России, КНР и КНДР летом 2020 г[18]. Новая киберстратегия ЕС упрощает процедуру введения санкций – принятие санкций путем голосования квалифицированным большинством[19].

Таким образом, на современном этапе существует ряд вызовов и угроз стратегической стабильности в ИКТ-пространстве. Для их устранения или, по крайней мере, снижения последствий необходимо возобновить неполитизированные консультации между западными государствами и Россией на регулярной основе, причем опыт подобного взаимодействия (специальные каналы связи Россия-США по линии Центров по уменьшению ядерной опасности), а также готовность российского руководства (заявление В.В. Путина от 25 сентября 2020 г.[20]) уже есть. Важно рассматривать все аспекты МИБ комплексно, без дробления повестки на отдельные пункты, что позволяло бы акцентировать внимание на одних проблемах и игнорировать наличие других. Наконец, ввиду огромной вовлеченности бизнеса в проблематику МИБ, следовало бы выстраивать международное сотрудничество на данном направлении с опорой на государственно-частное партнерство.

14 НАТО-2030: трансатлантическая повестка дня на будущее» // НАТО: официальный сайт, 04.07.2021 - URL: https://www.nato.int/cps/ru/natohq/opinions_184636.htm (дата обращения 19.05.2021).

15 Шойгу рассказал о центрах антироссийской пропаганды в Европе // РИА-Новости, 06.08.2021. – URL: https://ria.ru/20210806/propaganda-1744625304.html (дата обращения: 07.09.2021).

16 Michael R. Pompeo. The United States Sanctions Russian Nationals for Phishing Campaign // Press Statement: State Department, 16.09.2020 – URL: https://2017-2021.state.gov/the-united-states-sanctions-russian-nationals-for-phishing-campaign/index.html (дата обращения: 05.04.2021).

17 Treasury Sanctions Russian Government Research Institution Connected to the Triton Malware // Press Releases: US Department of the Treasury, 23.10.2020 – URL: https://home.treasury.gov/news/press-releases/sm1162 (дата обращения: 05.04.2021).

18 Council implementing regulation (EU) 2020/1125 of 30 July 2020 implementing Regulation (EU) 2019/796 concerning restrictive measures against cyber-attacks threatening the Union or its Member States – URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2020.246.01.0004.01.ENG&toc=OJ:L:2020:246:TOC (дата обращения: 03.02.2021).

19 The EU's Cybersecurity Strategy for the Digital Decade // Council conclusions on the EU's Cybersecurity Strategy for the Digital Decade – URL: https://data.consilium.europa.eu/doc/document/ST-6722-2021-INIT/en/pdf (дата обращения: 25.03.2021) - p. 16-17.

20 Заявление Владимира Путина о комплексной программе мер по восстановлению российско-американского сотрудничества в области международной информационной безопасности // Официальный сайт Президент России, 25.09.2021. – URL: http://kremlin.ru/events/president/news/64086 (дата обращения: 07.09.2021).

М.В. Конохов
Научный сотрудник сектора информационного права и международной информационной безопасности Института государства и права Российской академии наук, кандидат юридических наук

А.К. Дубень
Младший научный сотрудник научно-организационного отдела Института государства и права Российской академии наук

МЕЖДУНАРОДНО-ПРАВОВОЕ РЕГУЛИРОВАНИЕ ПОВЕДЕНИЯ ГОСУДАРСТВ В ИНФОРМАЦИОННОМ ПРОСТРАНСТВЕ В ПЕРИОД ВООРУЖЕННОГО КОНФЛИКТА

Не вызывает сомнений, что одной ключевых составляющих национальной безопасности на современном этапе развития цифровых технологий является информационная безопасность[1]. По оценкам Минобороны России, угроза милитаризации киберпространства ставит ее на одно из первых мест в ряду существующих вызовов международному миру и стратегической стабильности[2]. А.В. Крутских отмечает, что в отличие от ядерного оружия кибероружие уже применяется во вредоносных целях[3]. В свою очередь кибероружие по сопоставимости ущерба в современных условиях глобализации информационного пространства приравнивается к оружию массового поражения[4]. Как справедливо отмечает ЕС. Зиновьева, на международном уровне наметилась гонка информационных и кибервооружений[5].

1 Полякова Т.А., Шмаков М.А. Развитие конституционных основ обеспечения информационной безопасности: векторы научных исследований в области информационного права. // Военное право и современные информационные технологии в сфере национальной безопасности и военно-технического сотрудничества : Сборник докладов международной научно-практической конференции (Москва, 24-25 августа 2020 г. М., 2021. С. 59; Костенко Н.И. // Теоретические проблемы формирования права МИБ. М., 2019. С. 203.; Новиков В.К. информационное оружие-оружие современных и будущих войн – 3-е изд., испр. и доп. – М., 2020. С. 13.

2 Запивахин В.О. Милитаризация киберпространства – главная угроза международной информационной безопасности / Сборник докладов участников четырнадцатого международного форума «Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности» (7-9 декабря 2020 г.). С. 37.

3 Крутских А.В. Современные вызовы МИБ : Международная информационная безопасность: Новая геополитическая реальность / под ред. Е.С. Зиновьевой, М.Б. Алборовой. М., 2021. С. 10.

4 Шойгу сравнил угрозу кибербезопасности с оружием массового поражения URL: https://ria.ru/20131019/971215505.html (дата обращения: 28.08.2021 г.).

5 Зиновьева Е.С. Международное сотрудничество по обеспечению информационной безопасности: субъекты и тенденции эволюции. Дис. … д-ра полит. наук. М., 2019. С.5.

Учитывая изложенное, в Основах государственной политики Российской Федерации в области международной информационной безопасности (далее – Основы), принятых 12 апреля 2021 г., актуализированы вопросы учета национальных интересов Российской Федерации при реализации в рамках государственной политики совокупности скоординированных мер, направленных на формирование системы обеспечения международной информационной безопасности (далее-МИБ)[6].

В связи с этим следует отметить, что национальные интересы государства в сфере информационной безопасности отражены в Стратегии национальной безопасности Российской Федерации (далее-Стратегия), п. 17 которой определяет информационное пространство как новую сферу ведения военных действий[7].

Подтверждением этому является тот факт, что за последние три года на информационную инфраструктуру Вооружённых Сил было совершено более 25 тысяч высокотехнологичных компьютерных атак из-за рубежа. При этом ежегодно их количество увеличивается в среднем на 12%»[8]. Не вызывает сомнений утверждение о том, что в условиях вооруженного конфликта с участием Российской Федерации их количество будет только увеличиваться.

В п. 11 Военной доктрины Российской Федерации (далее-Военная доктрина) отмечено, что наметилась тенденция смещения военных опасностей и военных угроз в информационное пространство. П. 15 Военной доктрины в качестве одной из характерных особенностей современных вооруженных конфликтов определяет комплексное применение военной силы, в том числе и в глобальном информационном пространстве[9].

В связи с этим, в контексте формирования специальных механизмов международно-правового регулирования поведения государств в информационном пространстве в условиях вооруженного конфликта п. 11 Основ в качестве одного из основных направлений реализации государственной политики в области международной информационной безопасности (далее – МИБ) определяет создание условий для принятия государствами – членами Организации Объединенных Наций (ООН) Конвенции об обеспечении МИБ[10] (далее – Конвенция).

В предложенном на обсуждение мировому сообществу проекте Конвенции Российской Федерацией представлен довольно широкий спектр предложений по регулированию поведения государств в международном пространстве в период вооруженного конфликта, в частности: государства-участники признают, что агрессивная «информационная война» составляет преступление против международного мира и безопасности; каждое государство-участник имеет неотъемлемое право на самооборону перед лицом агрессивных действий в информационном пространстве в отношении него при условии достоверного установления источника агрессии и адекватности ответных мер; каждое государство-участник будет определять свой военный потенциал в информационном пространстве на основе национальных процедур с учетом законных интересов безопасности других государств, а также необходимости содействовать укреплению международного мира и безопасности, а также ряд других правил поведения в информационном пространстве, адаптированных к нормам международного гуманитарного права[11].

Не вызывает сомнений вывод о том, что принятие проекта Конвенции, содержащего приведенные нормы, регулирующего правила поведения государств в информационном пространстве в период вооруженного

6 Указ Президента РФ от 12 апреля 2021 г. № 213 «Об утверждении Основ государственной политики Российской Федерации в области МИБ». UR

7 Указ Президента Российской Федерации от 02.07.2021 г. № 400 О Стратегии национальной безопасности Российской Федерации URL: http://www.kremlin.ru/acts/bank/47046/page/5 (дата обращения: 28.08.2021 г.).

8 Шойгу рассказал о кибератаках на объекты Минобороны из-за рубежа URL: https://ria.ru/20200325/1569116726.html (дата обращения: 28.08.2021 г.).

9 Военная доктрина Российской Федерации (утв. Президентом РФ 25 декабря 2014 г. № Пр-2976) // URL: https://base.garant.ru/70830556/ (дата обращения: 28.08.2021 г.).

10 Конвенция об обеспечении МИБ // URL: https://www.mid.ru/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/191666 (дата обращения: 26.08.2021 г.).

11 Костенко Н.И. Указ. соч. С. 313-316.

конфликта, несомненно, способствовало бы укреплению мер доверия между государствами-членами мирового сообщества, а также существенному повышению уровня МИБ как в мирное время, так и в условиях вооруженных конфликтов.

В то же время подавляющее большинство концепций государств, входящих в блок НАТО, по обеспечению информационной безопасности в военной области предполагают применение специальных военных операций, как в глобальном, так и в национальных информационных пространствах, в том числе упреждающего характера, на основании одновременного комплексного использования, как различных систем вооружения, так и политических, экономических и иных мер невоенного характера[12]. И, как представляется, указанное обстоятельство, является основной причиной препятствования ведущими западными государствами принятию упомянутого проекта Конвенции, содержащей запреты на проведение многих из перечисленных операций.

На официального сайта Международного Комитета Красного Креста (далее – МККК) опубликован весьма содержательный доклад по вопросам применимости международного гуманитарного права (далее, соответственно, Доклад и МГП) к кибероперациям.

В Докладе акцент делается на следующие вопросы: потенциальные гуманитарные последствия киберопераций; применение МГП к кибероперациям во время вооруженных конфликтов; защита, предоставляемая существующими нормами МГП; необходимость обсудить, как применяется МГП; присвоение поведения в киберпространстве в целях установления ответственности государств[13]. В докладе особо подчеркнуто, что МГП не легитимизирует кибервойну, как и любой другой вид войны. Международные споры должны разрешаться мирными средствами во всех областях, в том числе в киберпространстве[14].

А.Л. Козик на основе анализа Доклада приводит примеры применения МГП в киберпространстве. Так, МГП налагает абсолютный запрет на нападения против гражданских объектов. Критическая гражданская инфраструктура – такая, например, как электрические сети, питающие жилые зоны, в терминах МГП являются гражданскими объектами. По мнению МККК запрет на нападения на гражданские объекты распространяются и на кибероперации, спроектированные таким образом, чтобы вывести их из строя без физического уничтожения.

МГП предоставляет особую защиту медицинским учреждениям и медицинскому персоналу. В соответствии с МГП стороны в вооруженном конфликте обязаны в любое время уважать и защищать медицинские учреждения. Это означает, что в дополнение к требованию воздержаться от создания препятствий к их функционированию, государства должны предпринимать все возможные меры для организации их работы и предотвращать ущерб в отношении их, включая причиненный путем кибероперацией.

Некоторые типы критической инфраструктуры, квалифицируемые как необходимые для выживания гражданского населения, такие, например, как установки, обеспечивающие питьевую воду, в соответствии с МГП также подлежат особой защите. Они защищены против любых кибероперацией, включая те, которые приостанавливают их функционирование[15].

В Докладе отмечается, что в современных вооруженных конфликтах кибероперации стали реальностью. МККК обеспокоен потенциальными гуманитарными последствиями растущего использования кибероперацией во время вооруженных конфликтов. Толкование государствами существующих норм МГП определит, в какой степени МГП защищает от последствий кибероперацией.

В частности, государства должны занять четкую позицию относительно своей готовно-

12 Бутрим И.И. Правовые аспекты информационной безопасности в военной области (сравнительно-правовой анализ) // Цифровая трансформация: вызовы праву и векторы научных исследований : коллективная монография, под общ. ред. А.Н. Савенкова; отв. ред. Т.А. Полякова, А.В. Минбалеев. Москва, Институт государства и права РАН, 2021. С. 187.

13 Международное гуманитарное право и кибероперации во время вооруженных конфликтов: изложение позиции МКК // URL: https://www.icrc.org/ru/document/mezhdunarodnoe-gumanitarnoe-pravo-i-kiberoperacii-vo-vremya-vooruzhennyh-konfliktov (дата обращения: 27.09.2021 г.).

14 Там же (дата обращения: 27.09.2021 г.).

15 Козик А.Л. Защита гражданской инфраструктуры и международное гуманитарное право / Сборник докладов участников четырнадцатого международного форума «Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности» (7-9 декабря 2020 г.). С. 84.

сти толковать МГП так, чтобы уберечь объекты гражданской инфраструктуры от серьезных повреждений и защитить данные гражданского назначения. Наличие такой позиции также повлияет на оценку того, достаточно ли существующих норм или же требуются новые. Если государства сочтут необходимым разработать новые нормы, они должны взять за основу и укрепить существующую правовую базу, включая МГП.

В то же время МККК полагает, что необходимо дальнейшее обсуждение – особенно среди государств – того, как следует толковать и применять МГП в киберпространстве. Существует настоятельная потребность в таком обсуждении. Если разрабатывать новые нормы для защиты гражданских лиц от последствий кибероперации или с другими целями, необходимо взять за основу и укрепить существующую правовую базу, включая МГП[16].

Российская Федерация поддерживает выраженную в докладе официальную позицию МККК по вопросам применимости МГП к вооруженным конфликтам в киберпространстве, что следует, в том числе и из анализа приведенного выше проекта Конвенции.

Продвижение на международной арене российских инициатив, в том числе и по урегулированию поведения государств в информационном пространстве в период вооруженного конфликта приносит свои результаты. В 2015 г. по инициативе Российской Федерации на рассмотрение Генеральной ассамблеи ООН был предоставлен документ «Правила поведения в области международной информационной безопасности». В 2018 г. свод правил поведения в области информационной безопасности был поддержан в качестве резолюции Генеральной Ассамблеи ООН[17].

В контексте обозначенных подходов МККК к применению норм международного гуманитарного права к ведению войны в информационном пространстве, а также содержащихся в проекте Конвенции, будет уместен следующий пример использования ответных мер применения военной силы в ответ на действия противника в информационном пространстве. В ответ на кибератаку палестинской группировки «Хамас» 5 мая 2019 г. Армия обороны Израиля (АОИ) нанесла ракетный удар по зданию в секторе Газа, где, по ее данным, находился штаб хакеров. Причем данный удар носил упреждающий характер, то есть имел место еще до начала предполагаемой кибератаки[18]. Доклад, определяющий подходы к применению МГП к конфликтам в киберпространстве, не охватывают подобных ситуаций, связанных с применением военной силы в ответ на предполагаемую кибератаку противника. Из этого следует необходимость дальнейшего совершенствования международно-правового регулирования военных действий в информационном пространстве.

Представляется, что в данном случае военные действия должны основываться на принципах соразмерности в случае применения силы, угроза кибератаки должна носить реальный, а не предполагаемый характер, также представляется необходимым определить предполагаемый размер ущерба военной инфраструктуре. В проекте Конвенции в общем плане данный вопрос урегулирован в части учета принципа соразмерности в ответ на применение противником информационного оружия, поэтому в случае реализации российской инициативы по принятию проекта Конвенции, адаптированной к нормам международного гуманитарного права, она была бы в рассматриваемой ситуации востребована в практическом плане.

Формирование системы МИБ с учетом национальных интересов Российской Федерации, предотвращение (урегулирование) межгосударственных конфликтов в глобальном информационном пространстве возможны только на основе соответствующего международно-правового режима, содействие установлению которого определено главной целью государственной политики в области международной информационной безопасности[19]. Неотъемлемой частью этого режима должны стать правила поведения государства

16 Указанный электронный ресурс (дата обращения: 27.09.2021 г.).

17 Резолюция ГА ООН A/C.1/73/L.27IRev.1 «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» от 29.10.2018 г. // URL: https://undocs.org/pdf?symbol=ru/A/RES/73/27 (дата обращения 23.08.2021 г.).

18 Кукова А., Чернухина К. «Это условие выживания». Эксперты сочли силовую атаку Израиля на палестинских хакеров соразмерной. URL: https://360tv.ru/news/proisshestviya/chempion-po-grebnomu-slalomu-pogib-na-altae/ (дата обращения 23.08.2021 г.).

19 Бойко С.М Новые стратегические ориентиры России в области международной информационной безопасности // Международная жизнь. 2021. № 6. С. 53.

в информационном пространстве в условиях вооруженного конфликта.

Как показал опыт атак вируса Stuxnet на ядерные объекты Ирана, важнейшей угрозой в рамках информационной войны является воздействие на критические инфраструктуры государства посредством нарушения нормального функционирования информационных сетей и систем, обеспечивающих их работу[20]. Крайне важным в этом случае представляется защита гражданским объектам, предоставляемая таким объектом нормами МГП. Это обстоятельство является достаточно весомым аргументом в пользу урегулирования правил поведения в информационном пространстве в период вооруженного конфликта.

Развитие информационных и телекоммуникационных технологий привело к появлению в международном праве достаточно новых терминов «информационное оружие» и «информационная война», которые требуют научного осмысления с позиций международного гуманитарного права. Как отмечает С.Е. Зиновьева, информационные формы оружия привнесли много нового в формы и методы ведения войны. Указанный автор, опираясь на определения информационного оружия и критических инфраструктур, выделяет четыре принципиально различных направления информационного противоборства: использование традиционных вооружений против традиционной критической инфраструктуры (ситуация, аналогичная войнам XX века, подпадает под действие международного гуманитарного права); использование традиционных вооружений против традиционной критической инфраструктуры – атака с использованием глобальной системы позиционирования (GPS, ГЛОНАС и др.) на транспортные и иные инфраструктурные сети, сетевые войска, атака с видео поддержкой, атака дистанционно управляемого воздушного аппарата на объекты критической инфраструктуры; использование информационных вооружений против сетевой критической инфраструктуры – собственно войны будущего; атака с помощью программного обеспечения на правительственные информационные системы, закладки и др[21]. Выводы названного автора свидетельствуют о многообразии форм и методов ведения информационной войны, необходимости формирования международно-правовых норм, регулирующих ее ведение.

Как отмечает А.В. Коротков, следует выделить несколько ключевых особенностей информационной сферы в целом и конфликтов в частности, оказывающих существенное влияние на применимость международно-правовых норм к данной области: защищенные и незащищенные и незащищенные объекты критической инфраструктуры в информационной пространстве тесно переплетены между собой; гуманитарные объекты критической инфраструктуры не обладают отличительными знаками, отмечающими их правовой статус; в информационной войне сложно провести разделение между гражданскими и военными целями; влияние негосударственных участников и неправительственных акторов в информационной войне сопоставимо с государственной мощью; информационное оружие обладает характеристиками, отличающими его от традиционных вооружений, вследствие чего его действие частично выпадает из сферы действия международного гуманитарного права; информационная война может вестись без предупреждения, сложно определить инициаторов информационной атаки, однозначно оценить масштаб ущерба, а также меру ответного удара; международной-правовое регулирование информационной войны необходимо для сохранения сложившейся системы международной безопасности»[22].

А.В. Крутских считает, что актуальной правовой проблемой также является реализация права государств на нейтралитет, в случае если их информационные системы используются третьими странами для осуществления информационных атак или иных противоправных действий[23].

Е.В. Зиновьева выделяет следующие проблемы адаптации международного гумани-

20 Зиновьева Е.С. Международная информационная безопасность : монография / Е.С. Зиновьева М., 2014. С. 72.

21 Международная информационная безопасность: Теория и практика: В трех томах. Том 1: Учебник для ВУЗов /под общ. Ред. А.В. Крутских. М., 2019. С. 229.

22 Цит. по Зиновьева Е.С. Международное сотрудничество по обеспечению информационной безопасности: субъекты и тенденции эволюции. Дис. … д-ра полит. наук. М., 2019. С. 141.

23 Цит. по Зиновьева Е.С. Указ. соч. С. 144.

тарного права к информационному пространству. К сфере гуманитарного права в связи с использованием в вооруженных конфликтах ИКТ относится целый ряд вопросов, а именно: встает вопрос о критериях отнесения информационных структур к гражданским/военным объектам, что осложняется тем фактом, что большинство критических информационных инфраструктур являются объектами двойного назначения, и могут быть использованы как в гражданских, так и в военных целях; согласно нормам международного гуманитарного права необходимо обеспечить соблюдение принципов пропорциональности и избирательности при проведении атак, однако в информационном пространстве применение данного принципа представляется затруднительным[24].

По ее мнению обозначенные проблемные вопросы осложняют применимость норм международного права к информационному пространству и обуславливают потребность в выработке новых правовых норм[25].

Указанный автор отмечает несколько ключевых особенностей информационной сферы, которые влияют на восприятие государствами угроз международной информационной безопасности: проблема однозначного определения источника атаки (проблема атрибуции) в информационном пространстве; трансграничный характер информационного пространства и взаимосвязь государств в данной сфере усиливают уязвимость государств и негосударственных акторов; «цифровая дилемма безопасности» в информационной сфере носит острый характер, что обусловлено асимметрией оборонительного и наступательного потенциала кибер- и информационного оружия; влияние негосударственных участников и неправительственных акторов в информационной сфере выше, чем в большинстве других областей мировой политики; защищенные и незащищенные объекты критической инфраструктуры в информационном пространстве тесно переплетены между собой, в информационной войне сложно провести разделение между гражданскими и военными целями, что осложняет регламентацию в данной области и ведет к тому, что информационные атаки могут осуществляться в мирное время, как часть межгосударственной конкуренции[26].

Следует согласиться с утверждением В.К. Новикова о том, что современный уровень человечества подошел к такой черте, когда использование огневых средств, оружия массового поражения для уничтожения живой силы и объектов становится неприемлемым по многим причина: нарушение экологии, массовая гибель гражданского населения, разрушение инфраструктуры и т.п. Поэтому возникшие глубокие противоречия между развитиями государствами и развивающимися за обладание сырьевыми, энергетическими, людскими ресурсами, запасами питьевой воды, продуктов питания можно разрешить, как считают руководители развитых стран, путем применения информационного оружия. Становится очевидным, что можно достичь победы над противником, не применяя живую силу[27].

В настоящее время создан достаточно многочисленный класс информационно-технического оружия и еще более многочислен и разнообразен класс информационно-психологического оружия, который постоянно совершенствуется с целью наращивания возможностей. Непрерывно также создаются новые его виды, способы и формы применения[28].

Как справедливо отмечает С.Н. Пыхтин, государства законодательно должны ставить заслоны атакам в кибернетическом пространстве, а также уменьшать их негативные последствия в случае их проявления. Опыт Великобритании, США, Германии, Южной Кореи и Японии говорит о том, что обеспечить безопасность исключительно своими силами и средствами одному государству не под силу. Противодействие кибератакам потребует организации коллективной защиты на международном уровне в рамках ОДКБ и ШОС

24 Зиновьева Е.С. указ. соч. С.5.

25 Там же. С. 5.

26 Зиновьева Е.С. Указ. соч. С.149.

27 Новиков В.К. Указ. соч. С. 11.; Пыхтин С.Н. Информационные войны как угроза национальной безопасности Российской Федерации Информационные войны. 2020, № 2 (54). С. 73 (71-74)

28 Там же. С. 280.

с привлечением частно-государственного партнерства[29].

Достижение цели реализации стратегических задач формирования системы МИБ невозможно без обязательного участия России в процессе решения задач во всех возможных форматах: двустороннем, многостороннем, региональном и глобальном[30]. Но, как представляется. несмотря на усилия мирового сообщества по недопущению конфликтных ситуаций в информационном пространстве, возможность возникновения информационных войн и применения информационного оружия на современном этапе развития информационных технологий представляется весьма вероятной.

Таким образом, следует прийти к выводу о необходимости продвижения российских инициатив в вопросах регулирования поведения государств в международном информационном пространстве, соответствующих официальным позициям МККК, на двустороннем, региональном и глобальном уровнях, посредством политики «мягкой силы».

В соответствии с п. 35 Военной доктрины основными задачами развития военной организации определяется развитие диалога с заинтересованными государствами о национальных подходах к противодействию военным опасностям и военным угрозам, возникающим в связи с масштабным использованием информационных и коммуникационных технологий в военно-политических целях. В свою очередь, в качестве основных внутренних военных опасностей для Российской Федерации определяется деятельность по информационному воздействию на население (п 13 Военной доктрины).

В связи с этим следует отметить, что в настоящее время в официальных документах и научной литературе все чаще фигурирует такое понятие, как когнитивное оружие, под которым понимается инструмент воздействия на сознание и разум с целью ослабления национального потенциала. Может использоваться для внедрения в интеллектуальную среду другого государства ложных научных теорий, концепций и стратегий[31]. Вопрос об ограничении применения когнитивного оружия в условиях вооруженного конфликта в современных условиях представляется весьма актуальным и требует отдельного обсуждения экспертным и научным сообществом как на международном, так и на внутригосударственном уровне.

Также следует отметить, что в приведенном докладе МККК государствам предложено определиться в вопросе о необходимости формирования международно-правовых норм, регламентирующих правила поведения государств в информационном пространстве в условиях вооруженного конфликта. В случае наличия такой необходимости за основу рекомендовано взять существующие нормы МГП.

Думается, что с учетом приведенных в статье мнений ученых, а также примера применения военной силы в ответ на кибератаку, этот вопрос является достаточно актуальным. Вопрос о необходимости формирования специальных международно-правовых норм, регулирующих правила поведения государств в информационном пространстве в условиях вооруженного конфликта, в настоящее время должен стать предметом обсуждения научного и экспертного сообщества.

С учетом той высокой роли и значения, уделяемой МККК, иными организациями и членами мирового сообщества, научным и экспертным сообществом, вопросам применения МГП в условиях вооруженного конфликта в информационном пространстве, представляется возможным рассмотрения вопроса о принятии в форме третьего протокола к Женевским Конвенциям такого документа как «Особенностей применения норм МГП в условиях вооруженного конфликта в информационном пространстве». Принятие такого документа, будет способствовать защите гражданского населения и гражданских объектов, объектов критической инфраструктуры при ведении военных действий в информационном пространстве.

29 Пыхтин С.Н. Указ. соч.С. 74.

30 Об этом подробней: Бойко С.М. Указ. соч. С. 56 Полякова Т.А. Теоретико-методологические проблемы цифровизации и трансформация информационного права // Третьи Бачиловские чтения. Цифровая трансформация: вызовы праву и векторы научных исследований : материалы Международной научно-практической конференции. М., 2020. С. 25.

31 Бирюков А.В., Алборова М.Б. Социально-гуманитарные риски информационного общества и международная информационная безопасность. М., 2021, С. 87.

Таким образом, на современном этапе развития МИБ следует прийти к выводу об актуальности вопроса обсуждения на международном уровне с участием экспертного и научного сообщества правил поведения государств в информационном пространстве в условиях вооруженного конфликта. Весьма действенным в этом вопросе может быть использование механизмов регионального взаимодействия в рамках ОДКБ, ШОС, БРИКС и иных объединений.

Список литературы:

1. Бирюков А.В., Алборова М.Б. Социально-гуманитарные риски информационного общества и международная информационная безопасность : монография / А.В. Бирюков, М.Б. Алборова ; М., 2021.
2. Бойко С.М. Новые стратегические ориентиры России в области международной информационной безопасности // Международная жизнь. 2021. № 6. С. 52-56.
3. Бутрим И.И. Правовые аспекты информационной безопасности в военной области (сравнительно-правовой анализ) // Цифровая трансформация: вызовы праву и векторы научных исследований : коллективная монография, под общ. ред. А.Н. Савенкова; отв. ред. Т.А. Полякова, А.В. Минбалеев. М., Институт государства и права РАН, 2021. С. 179-188.
4. Запивахин В.О. Милитаризация киберпространства – главная угроза международной информационной безопасности / Сборник докладов участников четырнадцатого международного форума «Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности» (7-9 декабря 2020 г.). С. 37-39.
5. Зиновьева Е.С. Международная информационная безопасность : монография /Е.С. Зиновьева М., 2014.
6. Зиновьева Е.С. Международное сотрудничество по обеспечению информационной безопасности: субъекты и тенденции эволюции. Дис. … д-ра полит. наук. М., 2019.
7. Козик А.Л. Защита гражданской инфраструктуры и международное гуманитарное право // Сборник докладов участников четырнадцатого международного форума «Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности» (7-9 декабря 2020 г.). С. 83-84.
8. Костенко Н.И. // Теоретические проблемы формирования права МИБ. М., 2019.
9. Крутских А.В. Современные вызовы международной информационной безопасности // Международная информационная безопасность: новая геополитическая реальность монография / под ред. Е.С. Зиновьевой, М.Б. Алборовой. М., 2021. С. 9-14.
10. Международная информационная безопасность: Теория и практика: В трех томах. Том 1: Учебник для ВУЗов / под общ. Ред. А.В. Крутских. М., 2019. С. 229.
11. Новиков В.К. Информационное оружие-оружие современных и будущих войн – 3-е изд., испр. и доп. – М., 2020.
12. Полякова Т.А. Теоретико-методологические проблемы цифровизации и трансформация информационного права // Третьи Бачиловские чтения. Цифровая трансформация: вызовы праву и векторы научных исследований : материалы Международной научно-практической конференции. М., 2020. С. 3-27.
13. Полякова Т.А., Шмаков М.А. Развитие конституционных основ обеспечения информационной безопасности: векторы научных исследований в области информационного права // Военное право и современные информационные технологии в сфере национальной безопасности и военно-технического сотрудничества : Сборник докладов международной научно-практической конференции (Москва, 24-25 августа 2020 г.). М., 2021. С. 55-65.
14. Пыхтин С.Н. Информационные войны как угроза национальной безопасности Российской Федерации Информационные войны. 2020, № 2 (54). С. 71-74.

КРУГЛЫЙ СТОЛ № 5
СОТРУДНИЧЕСТВО В ОБЛАСТИ ПРОТИВОДЕЙСТВИЯ ВМЕШАТЕЛЬСТВУ ВО ВНУТРЕННИЕ ДЕЛА СУВЕРЕННЫХ ГОСУДАРСТВ С ИСПОЛЬЗОВАНИЕМ СРЕДСТВ МАССОВОЙ КОММУНИКАЦИИ

Модераторы:
Смирнов А.И., Генеральный директор НАМИБ;
Куракин М.Б., заместитель Главного редактора журнала «Международная жизнь» МИД РФ

А.И. Смирнов
Генеральный директор Национальной Ассоциации международной информационной безопасности, д.ист.н., профессор МГИМО МИД России, Чрезвычайный и Полномочный Посланник РФ в отставке

СТРАТЕГИЧЕСКИЕ КОММУНИКАЦИИ ЗАПАДА КАК ИНСТРУМЕНТ МЕНТАЛЬНЫХ ВОЙН

Человечество переживает тотальную ломку миропорядка. Подрывную роль в данном процессе и десуверенизации государств играют информационно-коммуникационные технологии (ИКТ) и инфогенный нарратив в целом[1]. При этом пандемия COVID-19 стала триггером как многих преимуществ цифровизации, так и угроз, сопоставимых с Великой депрессией и даже с вызовами времен Второй мировой войны.

На смену пятому технологическому укладу – микроэлектронике – драйвером цифровизации пришел шестой уклад: нано, -био, -инфо – и когнитивные технологии, вызвавшие поистине тектонические сдвиги в развитии цивилизации. **По сути, человечество вступило в новый фазовый переход, сравнимый по значению, например, с созданием письменности.** На основе шестого уклада, или Industry IV стремительно развивается цифровая экономика, киберфизические системы, искусственный интеллект, квантовые вычисления, блокчейн, связь поколения 5G и иные прорывные технологии, кардинально меняющие мир.

В данном контексте приобретает особый смысл выражение «история войн – это история технологических прорывов». В этих условиях ведущие страны разрабатывают и реализуют разнообразные доктрины и стратегии по внедрению данных технологий с целью получения решающего геополитического доминирования и десуверенизации противника.

Рассмотрим так называемое когнитивное оружие.

В силу этого неоценимое значение в обеспечении стратегической стабильности имеют новые «Основы государственной политики в области международной информационной безопасности»[2]. Данный документ направлен на продвижение российских подходов к формированию системы обеспечения международной информационной безопасности (МИБ) и российских инициатив в этой сфере, на содействие созданию международно-правовых механизмов предотвращения и урегулирования межгосударственных конфликтов в глобальном информационном пространстве.

Мне очень приятно и вместе с тем ответственно сообщить, что Президент В. Путин при рассмотрении проекта «Основ…» на заседании Совета Безопасности России 26 марта 2021 г. отметил роль нашей Ассоциации: «…в эффективной реализации государственной политики, обозначенной в новой редакции «Основ», надо активнее использовать возможности научных и экспертных кругов, делового сообщества, в том числе, конечно, Национальной ассоциации международной информационной безопасности.»

Подчеркну, что согласно Уставу Ассоциации, созданной в 2018 г., одной из важнейших задач является проработка в упреждающем режиме проблемных вопросов обеспечения

1 См. 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.

2 URL: http://www.scrf.gov.ru/security/information/document114/ (дата обращения 23.09.2021)

МИБ в интересах формирования переговорных позиций государственных органов[3].

Наряду со многими международными конференциями по проблематике МИБ члены НАМИБ сделали сотни докладов, опубликовали десятки статей, приняли участие в выпуске учебника «Международная информационная безопасность: теория и практика» в трех томах, который переиздан в 2021 г. и т.д.

Вернемся к Основам госполитики в области МИБ. В Основах 2013 г. на период до 2020 г. основными угрозами использования ИКТ для МИБ были определены следующие четыре[4]:

а) в качестве информационного оружия в военно-политических целях, противоречащих международному праву, для осуществления враждебных действий и актов агрессии, направленных на дискредитацию суверенитета, нарушение территориальной целостности государств и представляющих угрозу международному миру, безопасности и стратегической стабильности;

б) в террористических целях, в том числе для оказания деструктивного воздействия на элементы критической информационной инфраструктуры, а также для пропаганды терроризма и привлечения к террористической деятельности новых сторонников;

в) для вмешательства во внутренние дела суверенных государств, нарушения общественного порядка, разжигания межнациональной, межрасовой и межконфессиональной вражды, пропаганды расистских и ксенофобских идей или теорий, порождающих ненависть и дискриминацию, подстрекающих к насилию;

г) для совершения преступлений, в том числе связанных с неправомерным доступом к компьютерной информации, с созданием, использованием и распространением вредоносных компьютерных программ.

В «Основах», утвержденных указом Президента России 12 апреля 2021 г. № 213, вышеупомянутые угрозы были уточнены и дополнены еще двумя[5]:

- использование отдельными государствами технологического доминирования в глобальном информационном пространстве для монополизации рынка ИКТ, ограничения доступа других государств к передовым ИКТ, а также для усиления их технологической зависимости от доминирующих в сфере

3 URL: https://namib.online/ustav-namib/ (дата обращения 23.09.2021)

4 URL: http://www.consultant.ru/document/cons_doc_LAW_178634/ (дата обращения 23.08.2021)

5 URL: http://www.kremlin.ru/acts/bank/46614 (дата обращения 23.08.2021)

информатизации государств и информационного неравенства.

- использование ИКТ для проведения компьютерных атак на информационные ресурсы государств, в том числе на критическую информационную инфраструктуру.

Особое агрессивное воздействие на Россию и её союзников оказывается со стороны США и их сателлитов. Данный постулат подтверждается, в частности, недавним докладом «НАТО 2030: сделать сильный альянс еще сильнее»[6], который на июньском саммите альянса был нацелен на усиление гибридного воздействия на Россию и её союзников: политико-дипломатического, экономического, военного и информационного. Как уже отмечалось, ключевую роль в манипулировании массовым сознанием в так называемой «ментальной войне» играют центры НАТО в Риге, Таллине, Варшаве. Рассмотрим как данную проблему видит Европейский центр передового опыта по противодействию гибридным угрозам, базирующийся в Хельсинки. Это межправительственный аналитический центр, который занимается анализом реагирования на гибридные угрозы под эгидой Европейского союза и НАТО.

Сами за себя говорят и названия последних «трудов» Центра стратегических коммуникаций НАТО в Риге.

Резюмируя, приходится констатировать, что резко вырос подрывной потенциал прорывных технологий для глобальной стабильности и особенно на треке ментальных войн.

Спасибо за внимание!

6 URL:https://www.nato.int/nato2030/ (дата обращения 23.08.2021)

М.Б. Алборова

К.и.н., доцент, Ведущий эксперт Центра международной информационной безопасности и научно-технологической политики МГИМО МИД Российской Федерации

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В СОЦИАЛЬНЫХ СООБЩЕСТВАХ В СЕТИ ИНТЕРНЕТ

Активное развитие научно-технической революции в области вычислительной техники и связи приводит к возрастающей роли информационной сферы в жизни человека. Все стороны общественной жизни все больше втягиваются в единую цифровую систему, человечество попадает в зону информационно-психологического пространства. Мы живем в условиях формирования новых правил нахождения человека и общества в этом пространстве. Оно, как очевидно, не только дает много возможностей, но и расширяет зону рисков для всей цивилизации.

Еще в 1995 году была создана первая социальная сеть Classmates.com, в этот момент человек получил возможность получать неограниченный объем различной информации, с которой не всегда могло справиться его сознание. С тех пор прошло уже четверть века, наступило время проанализировать ближайшие результаты и посмотреть изменения, проявившиеся в нашей жизни. Необходимо отметить, что социальные сети образовали абсолютно новую среду со своими правилами и требованиями. Возникла полноценная комплексная структура информационного поля, которая действует непосредственно на сознание человека и затрагивает все сферы его жизни[1].

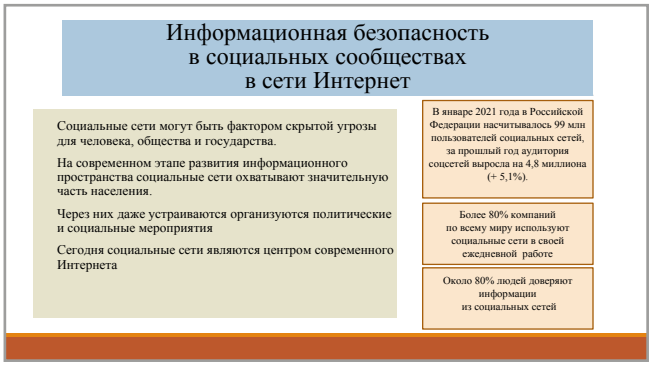
Актуальность и своевременность обращения к данному вопросу обусловлена тем, что на сегодняшний день Интернет, как форма представления и распространения информации используется большинством граждан разного возраста и социального положения. При этом информация, распространяемая в Интернете, доходит до целевой аудитории без необходимой «фильтрации» со стороны государственных органов, что позволяет ее распространителям практически бесконтрольно влиять на сознание общества, и во многом определять правила участия в информационном пространстве.

На современном этапе риски с которыми человечество сталкивается в связи с активным развитием Интернета крайне разнообразны. Это и взлом электронной почты, и кража личных данных, и опасности, связанные с использованием WI-FI, это и проблема травли в Интернете и втягивание в группы экстремистского характера.

В последнее время разработан ряд механизмов, защищающих население от доступа к основному противоправному контенту. Но обеспечить 100%-ную безопасность как самого человека, так и его личных данных при широком использовании социальных сетей практически невозможно. При этом сегодня влияние нового информационного пространства на человека через социальные сети практически безгранично. Более того, человек сам открывает все свои данные, ведь уровень цифровой грамотности по-прежнему очень невысок.

В настоящее время в России наиболее популярными социальными сетями остаются: «Вконтакте», «Одноклассники», «Facebook», «Twitter» и «Instagram». Все они сформированы, структурированы и практически созда-

1 А.В. Бирюков, М.Б. Алборова. Социально-гуманитарные риски информационного общества и международная информационная безопасность. М:. Аспект Пресс, 2021.



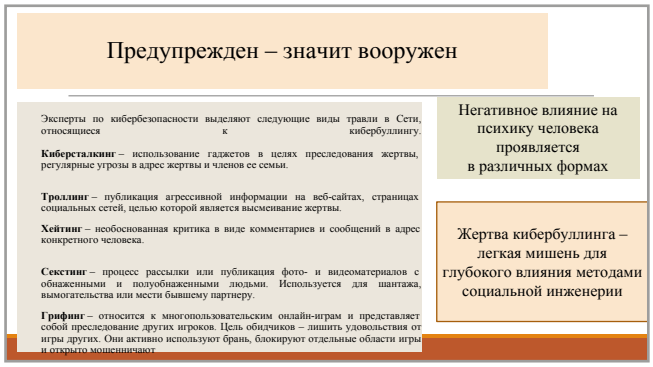
ны по единому принципу, подразумевающему обязательную процедуру регистрации, при которой пользователь вводит в установленную форму свои персональные данные, после чего у него появляется личная виртуальная страница, с использованием которой он и осуществляет взаимодействие с другими пользователями социальных сетей.

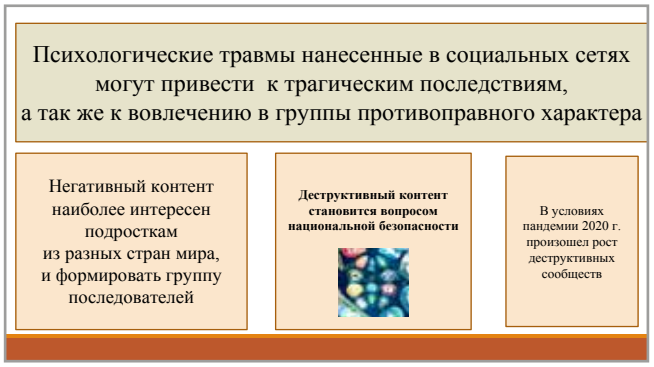
В рамках социальных сетей формируются внутренние виртуальные сообщества, которые объединяют людей по интересам, при этом каждая группа управляется администратором. Именно администраторы в первую очередь определяют запрос на актуальную тему и далее формируют подборку материала, которая была бы интересна широкому кругу подписчиков. Зачастую администраторы становятся своеобразными «лидерами мнений», они выступают в качестве экспертов, участники группы невольно становятся почитателями мнения компетентного специалиста в той или иной области, при этом позиция подобного эксперта мало подвергается сомнению[2].

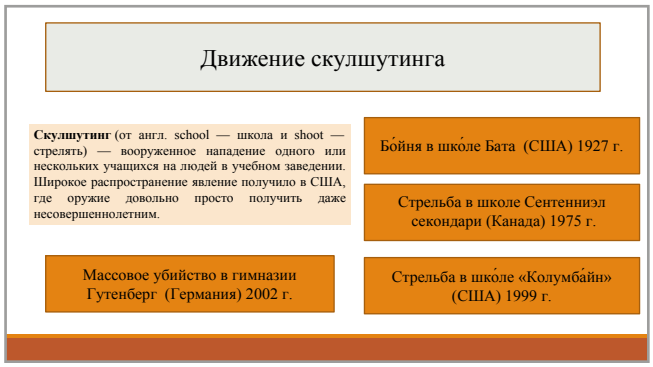
К сегодняшнему дню выросло целое поколение, которому не уделялось значительное внимание, многие не смогли стать носителями морально-нравственных ценностей, а некоторые из его представителей целенаправленно отказываются от общепринятых норм. Уровень личной безответственности растет, а стремление побыть наедине с гаджетом увеличивается. Нельзя не заметить общего морально-нравственного спада ценностей в современном обществе, причем в большей степени это затронуло именно технологически развитые страны, поскольку новые технические возможности обеспечили вовлечение юного поколения в мир технологий и тем самым стимулировали грандиозный отрыв одного поколения от другого. Отсутствие живого человеческого общения в большинстве семей привело к замене этой коммуникации на социальные сети, а отсутствие друга-родителя – к поиску доверенного и компетентного друга в Интернете.

С. Гринфилд, английская ученая, писательница и член палаты лордов, специализирующаяся в области физиологии мозга, доказала, что дети, воспитанные в социальных сетях, теряют способность к сопереживанию. Жизнь для них — как на картинке мобильного телефона, интересная, но чужая, ее всегда можно «перелистнуть». Человек, слишком много времени проводящий в социальных сетях, с трудом может формировать свой окружающий мир. В социальных сетях, если не нравится комментарий, можно просто заблокировать оставившего этот комментарий

2 Булва В.И. Манипулирование общественным сознанием – вызов информационного общества / Международная информационная безопасность: Новая геополитическая реальность / Под ред. Е. С. Зиновьевой, М. Б. Алборовой. — М.: Издательство «Аспект Пресс», 2021. — с.23.







человека, при этом пользователя особенно не волнует, что человек может переживать, ему не будет стыдно за то, что он причинил боль другому, поскольку никакого личного контакта, по сути, не было, следовательно, нет и ответственности. Не надо разбираться в людях, грамотно строить свой диалог и подбирать слова, чтобы никого не обидеть, появляется привычка игнорировать мнение.

При анализе вопросов прямого и косвенного влияния социальных сетей на сознание и подсознание молодежи определенно можно сказать, что социальные сети – это отражение всего нашего общества, своеобразный показатель нравственного здоровья. Если будут сформированы правильные смысложизненные ориентиры, то у общества есть шанс на выживание и прогресс, если будут преобладать негативные установки, то при таком глобальном влиянии это может привести к необратимым последствиям.

Особенно важно акцентировать внимание на влиянии социальных сетей на подростков в возрасте от 14 до 18 лет. Именно этот возраст наиболее сложный, поскольку максимализм этого периода и характерная восприимчивость к информационно-психологическому влиянию наиболее активны. Ценности семьи в этот период начинают смешиваться с ценностями окружающего общества, а в большинстве случаев происходит полное замещение семейных ценностей на приоритетное мнение

среды, а на современном этапе – информационной среды. Отсюда и актуальность этого вопроса, и стремление авторов привлечь внимание к этой сфере взаимодействия общества. Нахождение человека в новом информационном пространстве, сегодня во многом предопределяет дальнейшее становление и развитие как личности, так и общества в целом.

Современное киберпространство, сформированное вследствие развития научно-технического прогресса, действительно проникло в жизнь каждого из нас, создав особую окружающую реальность, породив новую кибер-культуру со своими ценностями, понятиями, образом мысли и своеобразным языком.

Внимание как психологов, так и психоневрологов сейчас особенно обращено к подростковой группе. Именно подростки находятся в зоне риска, психика в этом возрасте неустойчива, ценности еще окончательно не сложились. Сегодня, к сожалению, актив-

но развивающаяся семья с многопоколенными ценностями – это редкость, подростку просто неоткуда получить необходимые морально-нравственные приоритеты и сформировать гражданские позиции. Напротив, в глобальных интернет-сообществах он попадает под влияние различных социальных групп, в том числе противоправных. Постоянная критичность и максимализм приводят к полному отрицанию общепринятых в реальном обществе норм, замещению их нормами, навязанными социальными сетями.

Одной из наиболее распространенных проблем современного информационного пространства становится кибербуллинг[3]. Важно помнить, что кибербуллинг – это скорее общее определение для разных видов травли в Интернете, и его не стоит путать с кибермоббингом и кибертравлей. Иногда кибербуллинг может переходить в оффлайн. Многие блогеры и публичные личности сталкиваются с киберсталкингом. Это вид насилия, когда подписчики выслеживают инфлюенсеров и начинают их преследовать за пределами социальных сетей. Кибербуллинг может нанести значительную психологическую травму человеку, особенно если это касается подросткового периода. Важно отметить, что жертва кибербуллинга или иного вида травли становится легкой мишенью для глубокого влияния методами социальной инженерии, что может привести к крайне негативному результату, а также к вовлечению в группы противоправного характера.

В социальных сетях, человек с неустойчивыми общечеловеческими ценностями попадает под влияние групп экстремистского характера. Одним из примеров являются группы скулшутинга. Напомним, что скулшутинг – это вооруженное нападение, осуществляемое в учебном заведении. Это явление впервые появляется еще в 1927 году в США и с тех пор нашло свое отражение во многих странах. Это и события в школе Сентенниэл секондари (Канада) 1975 г., и Стрельба в школе «Колумбайн» (США) 1999 г., и массовое убийство в гимназии Гутенберг (Германия) 2002 г. Информация об этих событиях транслируется как в СМИ, так и в социальных сетях, но именно социальные сети позволяют создавать группы как для обсуждения проблемы, так и для формирования группы подражания.

С 2014 года впервые проявляются подобные трагедии и в России, сначала это события в Москве в 2014 году, потом в Ивантеевке в 2017 году. Важно отметить, что если до трагедии в Ивантеевке было 10 групп по данной тематике, то после это количество дошло до 45. Потом, произошли тяжелые события в Керчи. К сожалению, условиях пандемии[4] 2019–2020 года молодежь еще глубже погрузилась в социальные сети, которые предоставили широкое поле для размышления и создали базу для объединения в различные группы и публикацию своей жизненной позиции. После выхода из пандемии и начала учебного периода произошло за один год сразу две трагедии в Казани и Перми в 2021 году. В большинстве случаев социальные сети были использованы как для поиска информации, так и для трансляции своих действий,

Подводя итог, хотелось бы еще раз отметить, что глобальное интернет-пространство – это большие возможности, но и большие риски. Социальные сети можно использовать во благо или во вред. Современные технологии, с одной стороны, создали для человечества уникальную среду, которая может ускорить диалог культур, обеспечить условия для успешного взаимодействия людей, повысить уровень жизни человека, с другой стороны, тонкая грань между реальным и виртуальным миром может быстро стереться и привести к необратимым негативным последствиям. Многие представители современной молодежи переносят сформированные в социальных сетях ориентиры в реальную жизнь, что не всегда приводит к качественному изменению в социальной жизни общества, а порой порождает и тяжелые многопоколенные риски.

3 Булва В.И. Манипулирование общественным сознанием – вызов информационного общества / Международная информационная безопасность: Новая геополитическая реальность / Под ред. Е. С. Зиновьевой, М. Б. Алборовой. — М.: Издательство «Аспект Пресс», 2021. — с.27.

4 Юдина, Ю. А. Угрозы информационной безопасности Российской Федерации в период пандемии COVID-19 / Ю. А. Юдина // Тамбовские правовые чтения имени Ф.Н. Плевако : Материалы IV международной научно-практической конференции. В двух томах, Тамбов, 22–23 мая 2020 года. – Тамбов: Издательский дом «Державинский», 2020. – С. 371-374.

А.Н. Курбацкий
Председатель Экспертного Совета Парка высоких технологий, профессор Белорусского государственного университета (Республика Беларусь)

О СОХРАНЕНИИ СУВЕРЕНИТЕТА В МОЛОДЫХ НЕБОЛЬШИХ СТРАНАХ В ЭПОХУ ЦИФРОВИЗАЦИИ И БЕСКОНТРОЛЬНОГО РАЗВИТИЯ ИКТ

Мы по-прежнему плохо прогнозируем, куда нас заведет практически бесконтрольное развитие ИКТ. Мы постоянно запаздываем в восприятии угроз, порождаемых развитием ИКТ. Появление потенциальных угроз от ИКТ только ускоряется, а мы мало восприимчивы к прогнозам. Медленно воспринимаются экспертные оценки – переход с экспертного уровня на правительственный уровень длится крайне долго. Вспоминаю, как в 2009–11 годы в Москве, в Гармише-Партенкирхене мы активно обсуждали проблему необходимости постоянной оценки угроз, которые несут новые ИКТ. В частности, мой доклад в 2010 году назывался: «Значение экспертизы и прогнозирования влияния развития информационно-коммуникационных технологий на информационную безопасность общества».

Функциональность новой ИКТ, как правило, гораздо более очевидна, чем ее влияние на безопасность. Часто функциональность лежит на поверхности, понятна и поэтому сразу же включается маховик раскручивания потребительских свойств, основанных на функциональности, извлечения из этого прибыли, а какие последствия могут быть у такой массовой бизнес-раскрутки мало кто задумывается.

Появились новые ИКТ – появляются новые угрозы, новые проблемы в информационном пространстве, появляются новые возможности для киберконфликтов, кибертерроризма, киберпреступности. А сейчас при быстрой цифровизации нашей жизни приставку кибер можно и убрать.

При этом нельзя сказать, что и мирового сообщества нет опыта прогнозирования и контроля над новыми технологиями.

Если разработчики новых ИКТ будут понимать, что существует последующая экспертиза, то они, возможно, будут более ответственно относиться к своей продукции.

Нужно формировать ответственность бизнеса, который сейчас существенно опережает государства, за свою ИКТ-продукцию. Хотя бы с помощью таких подходов как с лекарствами или атомными технологиями – возьмем хотя бы пример МАГАТЭ.

Я по сути привел выдержки из своего доклада в 2010 году.

Все это актуально и сегодня.

Приведу примеры из жизни Беларуси: как недостаточное прогнозирование угроз, связанных с развитием ИКТ, влияет на стабильность страны и ее суверенитет.

Я не апологет цифры, хотя всю сознательную жизнь занимаюсь программированием, информационными технологиями, компьютеризацией, информатизацией, цифровизацией, информационной безопасностью и т.д. Просто многие процессы происходят не зависимо от того, согласны мы с ними или нет. В разумных пределах цифровизация процесс интересный и полезный, вот только как определить эти разумные пределы. Чтобы понимать, что нас ожидает, приходится все время наращивать свои компетенции. Резюмируя, если в небольшой стране цифровизацией самим не заниматься, то нас оцифруют без нас. И, естественно, о цифровом суверенитете можно вообще забыть, как и суверенитете вообще.

Поделюсь своим опытом. Я сам активно принимал участие в создании белорусско-

го ИТ-бренда – Парка высоких технологий (ПВТ). Реализация идеи по созданию особых условий для развития ИТ-индустрии Беларуси началась в конце 90-х по инициативе выпускников факультета прикладной математики и информатики БГУ, и в уже далеком 2001 г. появился Указ Главы государства, обеспечивающий движение в этом направлении. Это стало предпосылкой создания в 2005 г. Парка высоких технологий, что явилось значимым событием. ПВТ, однако, воплотил в жизнь практически только аутсорсинговую модель разработки софта – промышленный конвейер по разработке программного обеспечения. Массовый отток ИТ-мозгов мы остановили, но не остановили отток наиболее талантливых и ярких.

К 2015 г. стало понятно, что для дальнейшего продвижения необходима более прогрессивная модель развития ПВТ. В итоге был принят в 2017 г. Декрет Президента Республики Беларусь, создавший новые предпосылки для рывка в развитии ИТ-сферы. У нас в стране открылись новые возможности для приложения талантливых умов. Еще больше притормозился процесс бесповоротного отъезда кадров за пределы Беларуси. Тогда же стало окончательно очевидно, что необходимо создать качественно новое ИТ-образование, соответствующее самым современным мировым тенденциям и вызовам.

К сожалению, возможности появились, но от промышленного конвейера разработки программного обеспечения(ПО) мы далеко не ушли. Большая часть компаний работает по следующей схеме. Заказы поступают в основном из стран Северной Америки и Западной Европы, равно как и спецификации на разработку ПО и информационных систем (ИС), т. е. у нас, по-прежнему, массово формируются центры разработки. При этом зарплата программистов в такой модели существенно выше, чем на внутренних проектах. Но в последнем случае поддерживаются все этапы жизненного цикла разработки ПО и ИС, тогда как во многих зарубежных проектах – лишь некоторые, причем чаще всего самые простые и не наукоемкие. Соответственно, под эту же схему стала подстраиваться и отечественная система ИТ- образования, а это как раз и опасно для страны. Мы потихоньку скатываемся к образованию по подготовке кодировщиков, тестировщиков, специалистов по эксплуатации ПО и соответствующих систем.

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 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. 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.

Построили своего рода идеальный конвейер для разработки софта по модели аутсорсинга и разрушили качественное ИТ образование и как следствие начали разрушать и цифровой суверенитет, еще толком и не создав его.

В мире идет всеобщая цифровизация, которая требует разработки все еще большого количества софта. Правда, есть нюанс. В Беларуси «айтишники» – это единое понятие, которое объединяет тестировщиков, кодировщиков, специалистов по искусственному интеллекту, анализу больших данных, архитекторов систем и т. д. В мировой практике, а особенно в передовых странах, этой цельности нет – все это разные категории специалистов. И если кадры в области искусственного интеллекта, системные архитекторы, бизнес-аналитики, получившие серьезное образование, будут востребованы, то профессии тестировщика и кодировщика (а таких «айтишиков» в Беларуси большинство) могут быстро исчезнуть. Я предполагаю, что в ближайшие годы

искусственный интеллект сможет выполнять их функции.

Таким образом в Беларуси появился весьма условный квази-средний класс с заработками существенно более высокими, чем в среднем по стране. В силу ориентации аутсорсингового конвейера на Запад – это и постоянные контакты с западными заказчиками и поездки на запад (не постоянная жизнь, а только краткосрочные командировки и отдых). Конвейер образования, включающий университеты, колледжи, массу краткосрочных курсов по подготовке айтишников-лайт постоянно пополнял этот квази-класс. Появилась целая индустрия по обслуживанию этого класса (кафе, рестораны, барбершопы, и т.д.). Для молодежи сложилась очень притягательная картинка. И здесь вдруг ковид с жесткими ограничениями, через полгода выборы с резким всплеском информационного потока, совсем не развлекательного – притягательная картинка резко поблекла, иллюзорность начала разрушаться. Естественная реакция такой молодежи - протестность.

Таким образом мы в Беларуси видели в бурном развитии ИКТ в первую очередь финансово-экономические выгоды без оценки социальных последствий. Можно сказать даже сами подталкивали молодежь становиться гражданами мира. А следствие этого – безразличие к судьбе страны. Образование, достаточное для того чтобы стать для Запада вполне востребованным айтишником, молодежь получала в своей стране и в основном за бюджет. Затем эту же страну и начала сбрасывать, как архаичный балласт.

Многие тренды глобальной цифровизации (особенно негативные) в небольшой стране можно раньше заметить, чем в больших традиционных странах – у нас меньший запас прочности по многим параметрам, мы более чувствительны к угрозам. Но для анализа таких тенденций нужна хорошая экспертиза, профессиональное экспертное сообщество. И здесь начинаются проблемы. Мы часто в дискуссиях говорим: вот нужно собрать экспертов, пообсуждать, чтобы не попасть под фейковую волну СМИ, которые, стали ведущей движущей силой, за которой выстроились традиционные руководящие силы. Что мы можем противопоставить фейковой волне – в первую очередь, мнение экспертов. А где взять экспертов? Система образования, университетская среда все меньше справляется с их подготовкой. Потенциальные эксперты массово уходят в бизнес – особенно цифровой и не сильно стремятся работать на страну. Относительно независимое экспертное сообщество резко сокращается. В небольшой стране, как Беларусь, это особенно заметно.

Не способствуют развитию экспертного сообщества обожаемые чиновниками регламенты и стандарты. Во многих сферах деятельности, включая образование, науку и работу над диссертациями, чиновники, исходя из собственных, отнюдь не государственных целей, с помощью стандартов и регламентов возводят преграды между специальностями, направлениями научных исследований и т.п. Порой складывается впечатление о целенаправленности их усилий. В последующем, порождаемая таким процессом «армия контролеров» следит за тем, чтобы границы были нерушимы, и экспертов успешно загоняют в расставленные «силки». В итоге вполне естественно хочется спросить: где в такой ситуации междисциплинарность, межпредметность, системность аналитического мышления? Каким образом при таких искусственных ограничениях можно подготовить молодежь к экспертной деятельности?

В заключении приведу пример из опыта преподавательской деятельности в университете, когда опять же плохо прогнозируем, как новые ИКТ могут разрушать традиционную университетскую культуру образования (из-за ограничений по времени воздержусь от подробной оценки). Быстро нарастает проблема пока может быть и не столь заметная. Возможности социальных сетей, мессенджеров приводят к тому, что у студентов появляется возможность шантажировать преподавателей. Особенно это становится характерным для дистанционного образования, Молодые люди могут выложить в соцсети кадры с лекции, семинара, вырывая фразы из контекста. С нашей точки зрения, преподавательская деятельность должна быть инновационной. На лекциях мы часто импровизируем, чтобы донести информацию, которой еще нет в учебниках. Но если преподаватель будет понимать, что его рассуждения могут быть выложены в интернет, раскритикованы, экспериментировать он не захочет.

Е.С. Зиновьева
Д.полит.н., доцент, заместитель директора Центра международной информационной безопасности и научно-технологической политики МГИМО МИД России

АКТУАЛЬНЫЕ ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ ЦИФРОВОГО СУВЕРЕНИТЕТА В КОНТЕКСТЕ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Изучение проблем государственного суверенитета занимает политологов достаточно давно. Одним из первых государственный суверенитет изучал Жан Боден в XV веке, который понимал под суверенитетом абсолютную власть суверена, верховного власти правителя внутри своей страны, и его независимость на международной арене. В более поздних работах исследователи стали выделять суверенитет внутренний (то есть верховенство власти внутри страны) и суверенитет внешний (то есть независимость государства на международной арене).

По мере того, как развивались информационно-коммуникационные технологии, появляется новая аналитическая категория «цифрового суверенитета» (иногда также используется термин «информационный суверенитет»). Несмотря на то, что категория цифрового суверенитета на сегодняшний день используется в официальных документах ряда стран, в академической науке не существует единого подхода, как определять и изучать цифровой суверенитет.

В связи с этим хотелось бы предложить авторское понимание данной проблемы. Прежде всего, цифровой суверенитет можно рассматривать как суверенитет внутренний (полнота власти внутри государственных цифровых границ в информационной сфере) и внешний (независимая внешняя политика государства в глобальном информационном пространстве). Таким образом, цифровой суверенитет можно определить как полноту государственной власти и контроль над информационным потоками и информационной инфраструктурой внутри своих границ и независимость государства в своей информационной политике на международной арене.

Различными странами международного сообщества накоплен достаточно большой опыт реализации программ, направленных на обеспечение цифрового суверенитета, а сама эта проблематика стала особенно актуальной после событий «арабской весны», когда стало очевидно, что контроль над информационными потоками является важной составляющей национальной безопасности каждого государства. Если же говорить о фактическом наполнении цифрового суверенитета, то для его обеспечения важно не только обеспечение безопасности критических информационных инфраструктур, но и развитие национальных поисковых систем и социальных сетевых сервисов, а также вопросы контроля над потоками трафика. Следует отметить, что первоначальная большая часть инициатив в данной области касалась вопросов внутреннего цифрового суверенитета, однако в последнее время наметилось растущее внимание к проблематике внешнего цифрового суверенитета. Как представляется именно признание цифрового суверенитета на международном уровне как основы международного режима информационной безопасности может способствовать развитию мирного и демократичного глобального информационного пространства, что выгодно всем участникам международного сообщества.

Остановимся чуть более подробно на эволюции практики обеспечения цифрового суверенитета. В Китае, первом государстве, проводившем политику, направлен-

ную на укрепление цифрового суверенитета, в 2010 году в «Белой книге» были зафиксированы положения о необходимости обеспечения цифрового суверенитет, позднее идеи цифрового суверенитета и цифровых границ получили развитие в исследовательских работах китайских ученых. Однако по мере развития информационных технологий актуализировались внутренние и внешние угрозы информационной безопасности в большинстве стран, и тема обеспечения цифрового суверенитета привлекает к себе все большее внимание и выходит на передний план международной повестки дня, а также становится одним из приоритетов во внутренней политике большинства стран мира. Нужно отметить, что подход Китая в данной области также претерпевает определенные трансформации, и помимо внутреннего цифрового суверенитета растущее внимание получает категория внешнего суверенитета в цифровом пространстве. Так, в сентябре 2020 года МИД КНР опубликовал документ «Глобальная стратегия в области безопасности данных», в котором особый акцент делается на признании цифрового суверенитата как важного элемента международного режима информационной безопасности и защиты данных.

Однако, обеспечение цифрового суверенитета на уровне отдельных государств затрудняется в силу особенностей современной системы международного управления интернетом, в которой лидирующую роль (пусть и опосредованно, при помощи некоммерческих организаций ICANN и PTI) играют США. Желая сохранить сложившуюся модель международного управления интернетом и укрепить свое лидерство в сфере информационных технологий, США не заинтересованы в обсуждении на международном уровне вопросов цифрового суверенитета и проведении подобной стратегии государствами. Во внешнеполитической риторике США всегда выступали в поддержку безопасности трансграничных потоков данных, а не безопасности политических государств и политической стабильности внутри их границ, то есть обеспечения цифрового суверенитета. Это связано с тем, что США стремятся сохранить лидирующие позиции в международной системе и не заинтересованы в том, чтобы «связывать себе руки» международными обязательствами, касающимися невмешательства во внутренние дела других государств в информационной сфере.

Вместе с тем, актуализация угроз международной информационной безопасности трансформирует подходы ключевых союзников США по НАТО – а именно, государств-членов ЕС. В феврале 2020 года была принята Стратегия ЕС в области данных, направленная на укрепление лидерства ЕС в цифровом обществе. И хотя стратегия ставит перед собой преимущественно экономические цели, проблема обеспечения цифрового суверенитета в контексте информационной безопасности также занимает важное место. Следует отметить алармизм ряда европейский исследователей проблемы цифрового суверенитета в ЕС, которые выделяют в своих работах вызовы, стоящие перед ЕС в цифровой сфере, среди которых снижающееся влияние европейского бизнеса в ИТ сфере, угрозы информационной безопасности (кибер-преступность, кибер-терроризм, а также использование государствами ИКТ в военно-политических целях). При этом, они считают, что адекватный ответ на эти вызовы позволит ЕС сохранить своё влияние в цифровую эпоху и должен быть основан на укреплении цифрового суверенитета.

Таким образом, на международном уровне наметилось формирование дискурса о цифровом суверенитете, который может стать основой для формирования международного режима информационной безопасности.

В России также данная проблематика занимает существенное место и во внешнеполитической и во внутриполитической повестке дня. Особенно следует отметить внешнеполитические инициативы России в данной области. В апреле 2021 года была принята новая редакция важнейшего документа – «Основ государственной политики Российской Федерации в области международной информационной безопасности». В соответствии с документом недопущение использования ИКТ во враждебных целях, в том числе в целях ущемления государственного суверенитета – важнейший приоритет внешней политики.

В докладе группы правительственных экспертов 68-й сессии Генеральной Ассамблеи ООН от 2013 год фиксируется, что на поведение государств в информационном пространстве распространяется государствен-

ный суверенитет и международные нормы, вытекающие из принципа государственного суверенитета. Согласно документу, суверенитет также распространяется на юрисдикцию государств над ИКТ-инфраструктурой на их территории. В докладе РГОС от 2020 года также упоминается возможность использования ИКТ во враждебных целях как угроза государственному суверенитету.

Как представляется, в настоящее время формирование безопасного глобального информационного общества может быть основано только на уважении государственного суверенитета в цифровом пространстве. Одним из дипломатических лидеров в области кибер-дипломатии является Российская Федерации и широкая поддержка наших внешнеполитических инициатив в области международной информационной безопасности в рамках ООН показывает своевременность и востребованность формирования международного режима в области информационной безопасности, основанного на таких основополагающих принципах Устава ООН как невмешательство во внутренние дела, недопустимость использования силы или угрозы силой в информационном пространстве.

Д.Б. Фролов
К.ю.н., д.полит.н., директор Департамента информационной безопасности ФГУП «Российская телевизионная и радиовещательная сеть». И.о. зав. каф. Организации технической эксплуатации сетей телерадиовещания

АКТУАЛЬНЫЕ ВОПРОСЫ ЗАЩИТЫ ИНФОРМАЦИИ В СФЕРЕ ТЕЛЕРАДИОВЕЩАНИЯ

Недавно в нашей стране завершилась федеральная целевая программа перевода российского телевизионного вещания на цифровые технологии. Программа стала первым в России – и успешным – опытом перевода целой индустрии на цифровые технологии. Следует также отметить, что возможности создания инфраструктуры информационного общества в эпоху глобального развития информационных технологий разнообразны и многогранны и они напрямую связаны с вопросами доверия и информационной безопасности.

В соответствии с 187-ФЗ, РТРС является субъектом критической информационной инфраструктуры, что требует повышенного внимания к вопросам информационной безопасности. В составе РТРС – 78 филиалов, это одна из самых больших сетей телерадиовещания в мире.

Угрозы информационной безопасности в РТРС условно можно разделить на традиционные – которые характерны для многих объектов связи и телекоммуникаций. Это вирусы, атаки типа «отказа в обслуживании», фишинг и тому подобное. Хотелось обратить внимание на актуальные в связи с пандемией угрозы: это кража авторизационных данных (креденшл стаффинг). Данные похищаются преимущественно через фишинговые формы, которые пользователи получают через мошеннические письма, маскирующиеся под письма технической поддержки. Нередки случаи, когда распространение таких писем идет через уже зараженные почтовые сервера, пользователи которых были взломаны аналогичным способом. Вторая актуальная угроза – это домашние устройства пользователей, через которые они осуществляют удаленный доступ. Неизвестно, с т.з. информационной безопасности, что на них находится и зачастую они своевременно не обновляются. Кроме того, остаются риски, связанные с использованием одного устройства членами семьи сотрудника. Также зафиксирован рост нагрузок на каналы связи, что в некоторых случаях может привести к прерыванию услуг оператора, а также участившиеся случаи DDoS-атак и количество программ-вымогателей. И, конечно, утечки данных. Сейчас ценятся любые данные: всему найдется применение. Утечка может произойти как непосредственно из организации, так из смежных сетей, либо через подрядчика и иные возможности.

Отдельно можно выделить специфичные угрозы – атаки, направленные на подмену контента, когда, образно говоря, подменяется или искажается видеопоток, либо генерируется видеопоток, похожий на исходный – но с определенным отличием. Его также можно назвать своеобразной технологией для создания фейк-ньюс.

Для борьбы с «традиционными» угрозами, РТРС реализовало разработку комплекта необходимой организационно-распорядительной документации, централизовало политики средств защиты. Построило свой центр мониторинга и реагирования на инциденты ИБ, наладило процессы резервного копирования и восстановления, а также анализа инцидентов ИБ и корректировку процессов обеспечения ИБ по результатам анализа инцидентов.

Подмена же контента при передаче подразумевает уже атаку на инфраструктуру телеком-оператора, обеспечивающего доставку контента от студии вещания до абонента или иных провайдеров услуг. В качестве примера можно привести операцию израильских структур во второй Ливанской войны в 2006 году. Тогда удалось подменить вещание арабского телеканала, перехватив сигнал, транслируемый со спутника, и заменив контент государственного канала анти-ливийской пропагандой. 7 сентября 2012 года, когда была осуществлена подмена контента канала Disney, передаваемого оператором Dish Network через спутниковую трансляцию, 6-минутным жестким порнографическим роликом. 11 марта 2016 года, когда осуществлена подмена контента развлекательного канала в Израиле пропагандистским роликом от Хамас в течение 3,5 минут. Имеются и другие примеры подобных действий.

Мы уже вступили в эру цифровую развития, которая несет как множество преимуществ, так и множество возможностей для манипулирования сознанием слушателя, т.е. потребителя контента. Отсюда – новая угроза, о которой мы уже упоминали, это – искажение контента, или фальсификация. Сейчас это называют «дипфейком». Суть – особое искажение видеопотока, когда зрителю не показывают откровенную ложь, но делают ее максимально правдоподобной. Это достигается, например, когда известный, публичный человек что-то рассказывает «своим» голосом. Только делает это не он, а искусственный интеллект, «подгоняя» интонацию и мимику к произносимым словам. И зритель верит. В отличие от текстового контента, который используется в качестве дезинформации, видеоконтент воспринимается большинством как нечто трудно модифицируемое – и, следовательно, истинное. Поэтому, для видеоконтента нужно найти новые способы авторизации, либо должна измениться сама парадигма информационной безопасности, которая будет учитывать сложность или вообще невозможность отличия реального события от виртуального.

В наш век происходит быстрое развитие «интернета вещей», к которым относятся, в частности, умные телевизоры (смарт-тв). Поэтому не обязательно для генерации фейкньюс и дипфейков взламывать вещателя или телеком-оператора: достаточно взломать смарт-тв, вопросам обеспечения информационной безопасности которого обычно не уделяется должного внимания, после чего транслировать подмененный контент конкретному абоненту, например, в качестве шутки, или целенаправленно, как дискредитацию конкретной личности.

К сожалению, действенных методов противодействия в настоящее время не существует, они только разрабатываются. Что же можно сделать? Можно попытаться применить технологию блокчейна, представив видеопоток соответствующим образом. Можно осуществлять мониторинг источников видеопотока, сделать некий анализатор аномалий видеопотока. Основная проблема заключается в том, что используя методы криминалистического анализа, дипфейк определить можно. Но для этого нужно время, чего нет при онлайн-трансляции. Нужно проводить этот анализ так сказать «на лету» и в доли секунды. Сейчас таких технологий нет.

Каковы же перспективы? Мы будем видеть дальнейшее увеличение и разнообразие числа дипфейков. Это – элементы новых информационных воздействий, которые 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.

Но данную тему нельзя оставлять без внимания. К сожалению, мы сегодня запаздываем с решением этой серьезной и непростой проблемы. Она требует не только осмысления но и обмена опытом как на национальном, так и международном уровне, включая разработку соответствующих стандартов и нормативной базы, препятствующих использованию данных технологий во вред людям.

В.А. Романовский
Белорусский Институт стратегических исследований (Республика Беларусь)

ПРОТИВОДЕЙСТВИЕ РАСПРОСТРАНЕНИЮ ФЕЙКОВЫХ НОВОСТЕЙ» КАК ЭЛЕМЕНТ ПРЕДУПРЕЖДЕНИЯ ПРОТИВОПРАВНЫХ ДЕЯНИЙ В ИНФОРМАЦИОННОМ ПРОСТРАНСТВЕ (НА ПРИМЕРЕ РЕСПУБЛИКИ БЕЛАРУСЬ)

Здравствуйте уважаемые участники форума, коллеги!

В правовом поле Республики Беларусь понятие «фейковые новости» не является правовым термином. При этом в Концепции информационной безопасности Республики Беларусь, утвержденной в 2019 г., указывается, что «все большее беспокойство вызывает активное распространение в информационном пространстве фальсифицированной, недостоверной и запрещенной информации. Снижение критического отношения потребителей информации к фейковым сообщениям новостных ресурсов, в социальных сетях и на других онлайн-платформах создает предпосылки преднамеренного использования дезинформации для дестабилизации общественного сознания в политических, социально-опасных, иных подобных целях». С учетом данного положения, представляется возможным рассматривать «фейковые новости» именно как фальсифицированную, недостоверную и запрещенную информацию, а также дезинформацию.

Необходимо подчеркнуть, что в соответствии с Концепцией национальной безопасности Республики Беларусь, утвержденной в 2010 г., «распространение недостоверной или умышленной искаженной информации, способной причинить ущерб национальным интересам страны», является одним из источников угроз национальной безопасности в информационной сфере, т.е. для Республики Беларусь вопрос противодействия распространению дезинформации – это вопрос национальной безопасности.

Предупреждение противоправных деяний в информационном пространстве в аспекте противодействия распространению «фейковых новостей» и/или дезинформации включает в себя, во-первых, социальные меры, направленные на минимизацию причин и условий, способствующих распространению дезинформации; во-вторых, специально-криминологические меры, направленные на устранение причин и условий, способствующих распространению дезинформации, а также выявление и пресечение деятельности причастных к этому виду деяний организаций и физических лиц.

Социальные меры по профилактике правонарушений в аспекте противодействия распространению дезинформации могут включать в себя:

a. Повышение медийной и информационной грамотности населения с акцентом на формирование навыков критического мышления. При разработке соответствующих программ необходимо изучить подходы ЮНЕСКО и Международной Федерации библиотечных ассоциаций и учреждений (IFLA), а также привлекать представителей ведомств, специализирующихся в области профилактики преступлений экстремистской направленности.
b. Использования международного опыта по противодействию дезинформации с учетом интересов национальной безопасности и специфики правоприменительной практики в отдельно взятом государстве.

c. Создание специализированной научно-исследовательской площадки с целью обмена информацией и личным опытом по противодействию дезинформации и экстремизму. Ключевая роль в работе площадки отводится совершенствованию методов предупреждения противоправных деяний в информационном пространстве в аспекте противодействия распространению «фейковых новостей» и/или дезинформации и обмену опытом между профильными специалистами.
d. Создание специализированной государственной межведомственной структуры по противодействию дезинформации, ключевой задачей которой будет является оперативное информирование внутренних и внешних аудиторий о случаях дезинформации в отношении деятельности государственных структур.

Возможные специально-криминологические меры по профилактике преступлений экстремистской направленности в аспекте противодействия распространению дезинформации включают в себя:

a. Повышение скорости реагирования на инциденты, связанные с распространением дезинформации экстремистской направленности. Крайне важным является увеличение скорости обмена данными между специализированными ведомствами и интернет-провайдерами, банками и СМИ.
b. Создание единой системы верификации информации. Необходимо изучить возможность сочетания уже существующих в специализированных ведомствах инструментов с инструментами и платформами, используемыми в других странах и регионах.
c. Активное использование актуальных программных продуктов для противодействия дезинформации и обнаружения, фиксации и изъятия следов подобного рода деятельности при производстве следственных действий и проведении оперативно-розыскных мероприятий.
d. Специальная подготовка, переподготовка и повышение квалификации лиц, занимающихся вопросами противодействия дезинформации с учетом положений документов стратегического планирования в области информационной безопасности.

Очевидно, что при разработке соответствующих подходов и программ каждое государство осуществляет юрисдикцию в отношении информационного пространства в пределах своей территории в соответствии со своим внутренним правом. При этом необходимо разрабатывать общие стандарты правоприменительной практики в рамках противодействия использованию информационно-коммуникационных технологий в преступных целях.

Необходимо учитывать потенциальную опасность неправомерного использования новейших технологий, включая искусственный интеллект и блокчейн.

Важно развивать региональные системы обеспечения международной информационной безопасности. Необходимо поощрять меры по укреплению доверия, повышению транспарентности и распространению передового опыта в целях обмена данными для проведения расследований и судебного преследования в рамках интеграционных и региональных объединений.

Благодарю за внимание.

И.Ю. Тарасова
Помощник сенатора Комитета Совета Федерации Российской Федерации по экономической политике

СПОСОБЫ И ФОРМЫ ВМЕШАТЕЛЬСТВА В ИЗБИРАТЕЛЬНЫЙ ПРОЦЕСС ПОСРЕДСТВОМ ИКТ-ТЕХНОЛОГИЙ

Вмешательство в избирательный процесс (ИП) представляет собой противоправное явление, направленное на подрыв политической стабильности и изменение расклада политических сил в государстве. Цели могут быть разные: от устранения нежелательного кандидата, получения конкурентного преимущества в избирательной гонке до полной смены власти и государственного строя.

Современные ИКТ технологии создают практически неконтролируемые возможности для информационного воздействия на потенциальных избирателей. За последние два-три года центр тяжести электоральной проблематики с обеспечения явки населения на избирательные участки переместился в другую плоскость – в плоскость обеспечения информационной безопасности избирательных кампаний и признания действительности их результатов. Возникло понятие «электоральный суверенитет», которое подчеркивает значимость защиты избирателей от противоправного влияния и подразумевает право государства самостоятельно, без влияния извне, реализовывать любую модель политической системы и порядок ее формирования, которые поддерживает народ и которые не противоречат взятым международным обязательства. Вмешательство в ИП как политико-правовое явление существует еще с тех времен, когда люди стали выбирать своих вождей. При этом предлоги для вмешательства всегда выбирались самые благозвучные: «содействие интересам населения», «необходимость обеспечения стабильности», «координирующее вмешательство государства», «продвижение демократии» и т.п.

Можно выделить внутреннее и внешнее вмешательство в выборы. **Внутреннее** вмешательство (совокупность несанкционированных законодательством действий органов государственной власти, местного самоуправления, должностных лиц и граждан) направлено на установление контроля над политической ситуацией, получение конкурентных преимуществ в ИП и/или полную смену власти. **Внешнее** политическое вмешательство (заранее спланированные несанкционированные действия иностранного государства/группы государств, международных организаций, иностранных юридических или физических лиц), имеет целью дестабилизацию внутриполитической обстановки в суверенном государстве, изменение конкурентного политического ландшафта, установление контроля над действующей властью и/или государственный переворот. Формы вмешательства могут быть как явными, так и скрытыми.

Явное вмешательство – это целенаправленная, несанкционированная деятельность субъектов ИП или иных лиц, направленная на изменения результатов выборов, дестабилизации политической ситуации в стране. Например, нападки на кандидата на выборную должность в социальных сетях, клеветнические обвинения в адрес кандидата и т.п. Так, во время выборной кампании Президента Бразилии в октябре 2018 одному из кандидатов (Ж. Болсонару) Высший избирательный суд Бразилии предписал удалить со своей страницы в Facebook и канала в YouTube 6 ложных публикаций. Они были направлены против Аддада – соперника Болсонару во 2-ом туре. В одном из постов утверждалось, что на посту министра образования в 2005–2012 гг.

«Аддад пытался с помощью особых брошюр изменить ориентацию 6-ти летних детей на гомосексуальную»[1].

Скрытое вмешательство – тайные спланированные действия политических акторов, направленные на оказание несанкционированного влияния на ИП суверенного государства или достижение иной, в том числе – корыстной, цели. Формами скрытого вмешательства выступают работа с оппозиционными элементами (инструктаж), незаконное финансирование участников избирательных кампаний, подкуп избирателей и т.д.

Один из примеров скрытого вмешательства – электоральная коррупция. Под ней понимают:

- подкуп, получение или дачу взятки, иные коррупционные преступления, совершенные в рамках избирательной кампании;
- любое, связанное с выборами, незаконное использование лицом своего публичного статуса, сопряженное с получением для себя или аффилированных лиц (например, родственников) материальной (имущества, услуг или льгот) и нематериальной выгоды, вопреки законным интересам общества и государства;
- влияние на результаты выборов с помощью незаконного финансирования текущей деятельности партий, кандидатов и третьих лиц, аффилированных с ними, оказывающее влияние на итоги избирательных кампаний и конкуренцию на политическом рынке. Кандидат может оплатить расходы на избирательную кампанию средствами не со счета кандидата, а из собственного кармана.

Также, имея ресурс административного давления, коррумпированный кандидат может добиться преимуществ в доступе к СМИ, распространять клеветническую информацию об оппонентах и т.д., влиять на ИП посредством противоправного информационного обеспечения выборов как через «традиционные», так и Интернет-СМИ, социальные сети, блоги итд.

Другая разновидность скрытого вмешательства в ИП – деятельность оппозиции, которой оказывают финансовую и консультативную помощь иностранные агенты. Оппозиция использует, в частности, такие формы вмешательства, которые реализуются через социальные сети и Интернет-сообщества, с целью получения конкурентных преимуществ в борьбе за общественное сознание. Опасность таких информационных акций состоит в их безграничном и фактически неконтролируемом воздействии на аудиторию. Это могут быть «фейки» (подделки), номинация, дефейс, провокационные вбросы дезинформации, информационные «ловушки», троллинг, кибербуллинг, астротурфинг, словесное манипулирование итп. Фейки – специально сконструированные (ложные) свидетельства о вымышленных событиях. Фейк часто содержит визуальный материал- фотографии или видеоролики, снятых вообще в другом месте и другое время. Это фальшивые аккаунты, мошеннические сайты с «комментариями» несуществующих экспертов, псевдоновости, фотоподделки и др. Так, во время избирательной кампании Президента России в 2018 г. электронное издание «MK.ru» сфабриковало информационный вброс о «креативных» способах повышения явки избирателей на выборы в регионах: якобы священнослужители пообещали жительницам г. Орла за явку на избирательные участки… «отпустить грех аборта». Информация оказалась фейком: покаянный молебен проходил в стандартный день воскресной службы и к выборам не имел совсем никакого отношения.

Пример словесного манипулирования: номинация – использование слов-классификаторов, позволяющих повесить «ярлык» на кандидата или событие. Это такие определения, как «отщепенцы», «жулики», «фашисты», которые могут выполнять функции психологического программирования, вырабатывая у избирателей те или иные электоральные установки.

Одна из форм вмешательства, появившихся благодаря развитию ИКТ, – астротурфинг (англ. astroturfing) – способ управления общественным мнением посредством создания видимости социального эффекта. Астротурфинг – маскировка искусственной общественной поддержки под общественную инициативу. Распространен в Интернете и на-

1 Особенности избирательной кампании в Бразилии: фейки вместо дебатов [Электронный ресурс] // URL: http://amp.dw.com/ru/особенности-избирательной-кампании-в-бразилии-фейки-вместо-дебатов/a-45940910 (дата обращения: 24.09.2021).

правлен на имитацию широкой общественной поддержки людей, организаций или их деятельности. Технически этот метод держится на вытеснении сообщений реальных людей (на веб-форумах, в соцсетях) «замещающими» их фальшивками. Реализуется при помощи программного обеспечения либо нанятых оплачиваемых пользователей. Создаются якобы «случайные» и «независимые» протестные группы, волны «стихийной поддержки» кандидата. Так, в марте 2014, во время присоединения Крыма к России, в русскоязычном интернете публиковались посты и комментарии, подписанные от имени жителей Крыма, выступающих против его выхода из состава Украины. Как выяснилось впоследствии, значительная часть таких комментариев публиковалась совместными усилиями украинских и американских военных, к которым Минобороны Украины обратилось за помощью. Еще примеры распространенных ИКТ вмешательств – троллинг – метод целенаправленной провокации в социальных сетях, часто с публичными оскорблениях либо ином «хамском» поведении в Интернете; кибербуллинг – травля в интернете; дефейс – замена изображения , «изменение лица», размещение ложной информации на сайте «жертвы» как бы от ее имени. На Украине в период президентства Петра Порошенко сформировалась сеть заказных троллей и ботов, которые распространяли с поддельных учётных записей позитивную информацию о действующем президенте и чиновниках из власти, а в 2019 году, во время предвыборной кампании, вели работу по дискредитации других кандидатов. В обиходе эти тролли назвали «Порохоботы».

На днях завершились выборы в Государственную Думу Федерального Собрания Российской Федерации VIII Созыва, которые ознаменовались беспрецедентным уровнем вмешательства со стороны коллективного Запада[2].

Фейки о выборах в ГосДуму активно распространялись с начала лета 2021 г., первые из них зафиксировали с территории ЕС. С июля по август порядка 4,8 тысяч таких фейков обнаружила Лига безопасного интернета (например, что будут вакцинировать на участках)[3]. Был запущен фейк о том, что якобы отменяют видеонаблюдение на выборах. На деле же количество участков, которые были оснащены системой видеонаблюдения все 3 дня голосования, в том числе, в ночное время увеличилось до 50 тысяч в 2021 г. Оппозиция, иноагенты делали огромную ставку на использование видеонаблюдения в провокационных целях, они рассчитывали использовать видеоролики для подделок и провокаций – и просчитались. Видеонаблюдение закрыли для всеобщего обозрения, его организовали только на служебный портал. Тут же запустили фейк, что этим возмущены избиратели. Вброс сразу опровергла Председатель ЦИК Элла Памфилова. В ЦИК, наоборот, было больше обращений от тех, кто не хочет, чтобы их «транслировали» на весь мир. Избиратели расценивали это как вмешательство в их личную жизнь. Возмущались именно те, кто был жестко ориентируем именно на страны Запада, кому прекрасно известно, что там этого видеонаблюдения нет в первую очередь потому, что западные сообщества расценивают это как вторжение в их частную жизнь. В Канаде, например, просто запретили фото и видео съемку. Журналистов там вообще не пускают на участки (они через щелку в двери смотрят)[4]. Россияне запустили в соцсетях ироничный хэштег «#этодругое», как показатель двойных стандартов в отношении России.

В ЦИК РФ ежедневно сообщали о неоднократных попытках дискредитации и круглосуточных массовых кибератаках на систему федерального дистанционного электронного голосования (ДЭГ), которое применялось на данных выборах сразу в семи регионах РФ. Основной проблемой были кибератаки, обрушившиеся на сайт Центризбиркома. По Москве только хакерских атак было до 47 000 запросов в секунду. А всего за время голосования было заблокировано около 246 000 запросов. «Это просто катастрофа. У нас такого никогда не было», – сказала Памфилова, уточнив, что мощные атаки осуществлялись в том числе из США (50%), Германии (25%), России (10%) и Китая (5%). Это не только Dos-атаки,

2 https://iz.ru/1224179/2021-09-20/v-op-zaiavili-o-bespretcedentnom-urovne-vneshnego-vmeshatelstva-v-vybory-rf (Дата обращения 21.09.2021)

3 https://vk.com/wall618472499_630 (Дата обращения 21.09.2021)

4 https://rg.ru/2021/09/15/ella-pamfilova-ob-osobennostiah-izbiratelnoj-kampanii-2021.html (Дата обращения 20.09.2021)

это и попытки агитации через иностранные цифровые платформы. Много специально изготовленных фейков – новостей с заведомо ложными данными. Они распространялись в западных СМИ, через СМИ-иноагенты, в русскоязычном сегменте Интернета. Поток негативной информации в иностранных медиа увеличился в разы. Со стороны коллективного Запада она ретранслировалась в наше информационное пространство уже в переводе и на русском языке». Атаковались порталы ЦИК, Выборов, Госуслуги, ЕСИ и т.д. Среди тезисов: «выборы стали самыми грязными и нелегитимными в РФ», «многодневные выборы были созданы специально для фальсификации результатов», «всем достойным кандидатам отказали в регистрации», «массово применялась технология двойников»[5]. Системы защиты успешно справились с подобным воздействием на ДЭГ и сайт ЦИК. Для участия в ДЭГ зарегистрировались более 2,5 млн человек, что говорит о доверии населения к этой системе. В течение всего выборного процесса велись массированные информационные нападки и в регионах, в частности в Крыму. Вот ответ Министра иностранных дел России Сергея Лаврова по голосованию на территории Крыма на Пресс-конференции по итогам недели высокого уровня 76-й сессии Генеральной Ассамблеи ООН: «Сейчас ухватились за «крымскую тему», включая лихорадочный созыв т.н. Крымской платформы в Киеве, шум по поводу голосования. Думаю, это попытка отвлечь внимание от того, что Киев во главе с Президентом Зеленским позорно провалил свои обязательства по Минским договоренностям относительно преодоления внутриукраинского конфликта на востоке страны. Вот и стали разыгрывать «крымскую тему». «Вторая причина, почему они это делают, – это дипломатический непрофессионализм. Профессионалы прекрасно понимают, что вопрос с Крымом закрыт раз и навсегда»[6].

Атака на российские выборы велась и на территориях за рубежом, где голосовали российские граждане. Так, Посольство России в США заявило о беспрецедентном числе кибератак на выборах. О недопустимости вмешательства на избирательный процесс российские дипломаты говорили в Белом доме и Госдепе. Посол РФ в США Анатолий Антонов заявил, что Вашингтон запросил данные о вмешательстве в российские выборы с американской стороны и обещал провести соответствующее расследование. Вместе с тем глава дипмиссии отметил, что американцы уклонились от обещаний принять меры в отношении информационных компании Google и Twitter, аргументируя это якобы невозможностью повлиять на их политику. При этом в 2017 году, когда США активно обвиняли Россию во «вмешательстве» в президентские выборы, представителей интернет-гигантов неоднократно вызывали на слушания в сенат, где расспрашивали по поводу российского «влияния»[7]. Очевидно, что американские власти пытаются снять с себя ответственность за действия корпораций и самоустраниться от этой темы на фоне других проблем. Фейки особенно часто встречались в социальных сетях TikTok, YouTube, Facebook и Telegram. В ходе предвыборной кампании в Госдуму у российских властей были претензии к компании Google, которая владеет сервисом YouTube. Так, 20 августа Роскомнадзор потребовал удалить приложение «Навальный» из онлайн-магазинов Apple и Google, как используемое для продолжения деятельности признанной экстремистской и запрещенной на территории России организации «Фонд борьбы с коррупцией» (признан в России иноагентом). Позже «Яндекс» сообщил, что удалил ссылки на «Умное голосование», однако поисковик Google по-прежнему выдавал ссылку на сайт «Умного голосования». В то же время представители американской корпорации Apple заявили, что «правовые тонкости» не позволяют материнской компании удалить приложение «Навальный» из App Store. Представителей американских компаний Apple и Google пригласили 16 сентября в Совет Федерации, и они не смогли объяснить, почему приложение «Навальный» не было удалено. Тогда глава комиссии Госдумы по расследованию фактов вмешательства иностранных государств во внутренние дела России Василий Пискарев заявил, что попытки корпора-

5 https://iz.ru/1223530/2021-09-18/tcik-otrazil-krupnuiu-ddos-ataku-na-resursy-izbirkoma-v-subbotu (Дата обращения 21.09.2021)

6 https://www.mid.ru/press_service/video/-/asset_publisher/i6t41cq3VWP6/content/id/4898861(Дата обращения: 27.09.2021)

7 https://iz.ru/1224651/2021-09-21/posolstvo-rf-v-ssha-zaiavilo-o-bespretcedentnom-chisle-kiberatak-na-vyborakh (Дата обращения 23.09.2021)

ций Apple и Google вмешиваться в российские выборы могут повлечь за собой последствия, в том числе уголовного характера. В результате приложение «Навальный» было удалено из магазинов Google Play и App Store 17 сентября после целого ряда мероприятий, в частности бесед с послом США в Москве.

Другой вопиющий пример применения коллективным Западом политической цензуры и политики двойных стандартов: 28 сентября 2021 г. видеохостинг YouTube запретил пользователям 1) размещать контент, оспаривающий итоги всех прошедших выборов в США; 2) выражать любые сомнения в результатах состоявшихся в воскресенье парламентских выборов в Германии. Администрация YouTube сообщила, что нарушающий правила контент будет удаляться, его владелец – получать предупреждения. После третьего «страйка» канал-нарушитель может быть заблокирован. Новое правило действует в отношении всех прошедших выборов в США и парламентских выборов 2021 г. в Германии. При этом YouTube не заблокировал **ни один** недостоверный ролик о выборах в Госдуму. Таким образом, неправомерные действия, запрещенные под угрозой крупных санкций в других странах, безнаказанно могут совершаться данной платформой на территории России. YouTube фактически заявил приверженность политической позиции США и государств Евросоюза. «Эта дискриминации в отношении пользователей других стран приведет к тому, что количество опасного контента, в том числе фейков и недостоверной информации, на этой платформе будет только расти»[8]. (К слову, активная политическая ангажированность хозяев глобальных Интернет-сетей вообще представляет крайне тревожную мировую тенденцию. Достаточно вспомнить, что на прошедших в США выборах президента в 2020 г. она показала себя реальной третьей силой, наряду с производственным и финансовым мировым олигархатом).

Западные «технологи» пытались воздействовать на российских избирателей через информационные кампании, условно «разделив» российскую аудиторию на несколько «адресатов». В первую очередь это политические и бизнес – элиты страны, часть которых, по мнению Запада, могла принять его сторону. Санкционные войны – это один из примеров действий, направленных на государственный переворот через раскол элит (Расчет на раскол элит, чтобы часть их поддержала западных провокаторов – это один из шаблонных методов «цветных революций»).

Параллельно шла обработка других групп общества – молодёжь (в том числе из неблагополучных семей, из молодых инвалидов и сирот, из маргинальной молодежи, ассимилирующихся в России этнических иностранцев и др) и представителей определенных регионов, которые Запад рассматривает как потенциально «слабые» и восприимчивые звенья. Далее предполагалось воздействие на всех граждан нашей страны в целом. Антироссийская пропаганда в Интернет – СМИ и всех возможных площадках велась на определенные возрастные, географические, профессиональные, социальные, религиозные группы.

Были намечены главные тактические линии для дискредитации данного избирательного процесса. Во-первых, обвинения в массовых фальсификациях, во-вторых, обвинения российской власти в недопуске оппозиционеров на выборы, и далее – утверждения, что вся российская власть нелегитимна.

Первый, предварительный этап включал «наступательную» деятельность иностранных фондов, выступления в СМИ и блогосфере западных журналистов, политиков, любых «экспертов» и российских иноагентов, с использованием агрессивных информационных кампаний и лозунгов о непризнании выборов. По их задумке, надо было создать общественное мнение, что выборы пройдут с нарушениями и будут нелегитимны.

Параллельно активизировались официальные лица и ведомства иностранных государств. На **втором** этапе, начиная с лета 2021 г., подтянулась «тяжелая артиллерия», в лице ведущих западных институтов. Так, 13 августа шведский депутат Ханс Валльмарк предложил главе МИД Швеции и ЕС дать понять России, что фальсификация выборов будет чревата последствиями. Депутат заявил, что выборы не смогут быть справедливыми, так как многим кандидатам мешают принимать в них участие и политические движения

8 https://vz.ru/news/2021/9/28/1121317.html (Дата обращения 29.09.2021)

не могут быть свободны в России[9]. А задолго до начала выборов ОБСЕ подготовила предварительный доклад, в котором раскритиковала российский закон о том, что в России могут быть избраны депутатами лица с двойным гражданством. «Следующим шагом» БДИПЧ ОБСЕ впервые с 2007 года отказалось прислать своих наблюдателей на осенние выборы в Госдуму. Свое решение там объяснили введенными в России ограничениями. Всего организация хотела направить в Россию более 500 наблюдателей. В Москве же это количество сочли чрезмерным, в ситуации с пандемией коронавируса. Россия предложила ОБСЕ ограничить это количество шестидесятью сотрудниками наблюдательной миссии. ОБСЕ анонсировала, что не сможет выполнять в таких условиях свою работу «четко и эффективно». Со стороны организации непринятие коронавирусных ограничений выглядело особенно фальшиво, когда множество стран уже прошли через эту практику. Так, российских болельщиков не пустили на заключительный матч группового этапа Чемпионата Европы в Дании. Беспрецедентно жесткие меры предпринимались при организации и проведении Олимпийских игр в Токио, где вакцинировали более 80% резидентов Олимпийской деревни и аккредитованные СМИ. На протяжении двух пандемийных лет у ОБСЕ был выработан алгоритм проведения миссий в усеченном виде. Кстати, после решения об отказе направлять миссию в Россию ОБСЕ объявила о решении направить крайне малочисленные группы экспертов в Канаду и Чехию; в Норвегию и Исландию не направлять **никого** вообще, и **четыре** наблюдателя в Германию на выборы в Бундестаг. Например, на выборах в России международных наблюдателей было в 10 раз больше, чем в США, при этом количество избирателей там лишь в 1,5 раза превышает число российских. В США иностранцам вообще запрещено приближаться к избирательным участкам. Однако там ОБСЕ это не смущает.

Глава комиссии Совфеда по защите госсуверенитета Андрей Климов: «Это решение было ожидаемо... БДИПЧ рассматривало несколько вариантов в плане наблюдения за выборами в России, в итоге был выбран путь лобового скандала. Решение чисто политическое… им было понятно, что они не найдут нарушений на парламентских выборах в России»[10].

Для справки: В России выборы в Государственную думу 2021 г. мониторили 245 международных наблюдателей из 59 стран мира, 10 международных организаций и 57 дипломатов из аккредитованных в Москве диппредставительств. В общей сложности более 380 международных наблюдателей и экспертов из 80 стран мира следили за ходом голосования на площадках центров общественного наблюдения, работали миссии по линиям СНГ, ПАСЕ, ОДКБ.

На **третьем**, кульминационном этапе дискредитации думских выборов за день до голосования российских избирателей Европарламент принял резолюцию, где 3/4 голосов заранее объявил грядущие результаты выборов сфальсифицированными. В этом же документе было сказано, что ЕС должен осудить любую попытку президента Владимира Путина остаться у власти после окончания его нынешнего мандата, на основании поправок в Российскую Конституцию, которые ЕС также признал нелегитимными. В одной связке с непризнанием парламентских выборов Европарламент выразил готовность осудить намерение Президента Путина баллотироваться на следующий срок.

И, наконец, «вершина кульминации»: 20 сентября Госдеп США заявляет что выборы в России не были легитимными, и один из аргументов – потому что не пустили миссию БДИПЧ ОБСЕ, а также не допустили других кандидатов. США не признало выборы на территории России и двух субъектах федерации – Крым и Севастополь.

Надо ли говорить, что доклад Европарламента по России, в котором говорится о возможности непризнания выборов в Госдуму РФ, как и последующее заявление Госдепа, являются образцом неприкрытого вмешательства во внутренние дела суверенного государства. Итак, был заранее подготовлен сценарий: сначала отказ БДИПЧ ОБСЕ под

9 https://www.mk.ru/politics/2021/08/13/v-shvedskom-parlamente-predosteregli-rossiyu-ot-falsifikacii-vyborov.html (дата обращения 15.09.2021)

10https://iz.ru/1202945/2021-08-05/v-sovfede-obiasnili-otkaz-obse-posylat-nabliudatelei-na-vybory-v-gd?utm_source=yxnews&utm_medium=desktop (Дата обращения 20.09.2021)

надуманным подлогом, чтобы потом на этом основании русофобская резолюция Европарламента и заявление Госдепа обеспечили «международный резонанс», и «коллективный Запад» объявил выборы несвободными и нелегитимными.

Прозападная «коалиция» рассчитывала, что российские избирали «впадут в депрессию» и не придут голосовать, будет низкая явка. Антироссийская пропаганда «била» по двум направлениям – она обращалась к гражданам России и населению за рубежом. В иностранных государствах провокаторам было важно работать с местными гражданами по множеству причин, в том числе в надежде на западное финансирование, международную огласку, на поддержку оппозиции западными государствами в случае своего бегства из страны и т.д.

Когда ангажированные СМИ и иноагенты пугали население на Западе Россией-агрессором и – отравителем, это производило эффект на местное население. Но провокаторы просчитались с менталитетом российских граждан, пытаясь воздействовать на них теми же «страшилками». Наш народ всегда плохо воспринимает давление - он консолидируется. Россияне не поверили лозунгам прозападных пропагандистов про «нечестные выборы». Наоборот, русофобские заявления ОБСЕ, Европарламента, Госдепа и др. привели к прямо противоположному результату: крепче сплотили людей вокруг власти.

Организаторов кампании подвела шаблонность мышления, неумение учитывать различия менталитетов и элементарный непрофессионализм «экспертов».

Целенаправленный сценарий не был полностью реализован: открытые выборы в России состоялись при высокой явке, международные наблюдатели признали их законными. Ниже комментарий Министра иностранных дел России Сергея Лаврова на вышеупомянутой Пресс-конференции по итогам недели высокого уровня 76-й сессии Генеральной Ассамблеи ООН в Нью-Йорке: «Мы не слышали каких-либо оценок от Евросоюза как такового, потому что Европарламент – это не структура, определяющая политику ЕС. Я говорил об этом с Ж. Боррелем…». «Он неловко и невнятно оправдывался…». «У нас сведений о том, что кто-то официально отвергает результаты наших выборов, которые только что были объявлены, нет»[11].

Но не будем забывать, что это была «обкатка» будущей информационной войны, нацеленной на срыв выборов Президента Российской Федерации в 2024 г. «Анализ фейков из-за рубежа о сентябрьских выборах показал, что 90% из них так или иначе касались президента РФ, хотя выборы были в Госдуму…» «Где-то процентов 40 они напрямую касались Президента, в остальном нападки на главу государства шли как фон к основным фейкам. Есть основания полагать, что после того, как улягутся страсти и истерики, они приступят к дальнейшей работе… Системность нападок именно на Президента для дискредитации его авторитета у населения России будет активизирована. В заявлениях Госдепа и Европарламента проводится следующая цепочка: общероссийское голосование по Конституции – выборы депутатов Госдумы – выборы президента России. Тем самым они хотят сказать, что не желают признавать все выборы и голосования, называя их нелегитимными» (Совет Федерации ФС РФ)[12].

При этом, информационные операции по дискредитации Президента России и его ближайшего окружения начались задолго до вышеупомянутого пункта в резолюции Европарламента об осуждении возможности Президента Путина баллотироваться на выборы в 2024 г. и заранее признание незаконным выдвижения его кандидатуры. Ниже приведем несколько примеров.

Цепочка «новейшей истории отравлений» началась в 2006 г. с «дела Литвиненко» и обвинений в его преднамеренном убийстве сотрудников ФСБ, то есть фактически «ближнего круга» Президента России. Спустя 10 лет в 2016 г британское расследование пришло к выводам, что операция по убийству Литвиненко вероятно («универсальное» highly likely) проведена с одобрения Президента Путина. В феврале 2020 в Британии в графстве Саррей выходит театральная постановка «Жизнь и смерть Александра Литвиненко». А сра-

11 https://www.mid.ru/press_service/video/-/asset_publisher/i6t41cq3VWP6/content/id/4898861(Дата обращения: 27.09.2021)

12https://iz.ru/1224979/2021-09-21/v-sovfede-obiasnili-popytki-inostrannogo-vmeshatelstva-v-rossiiskie-vybory (Дата обращения: 22.09.2021)

зу на следующий день после состоявшихся в России выборов ЕСПЧ вынес обвинительное решение по делу Литвиненко, признав Россию ответственной за убийство, «утяжелив» таким образом обвинения в нелегитимности действующей власти. Фактически уже много лет западными спецслужбами разрабатывается операция «Путин травит политических оппонентов». Последовательно развивается цепочка «Литвиненко - Скрипали - Навльный». В нее же можно добавить историю с задержанием в 2020 г. в Чехии представителя Россотрудничества с якобы «ядом рицин» с целью «отравления из мести» за снос памятника Коневу в Праге. Меняются имена «жертв», оттачиваются формы и методы, например:

- шантаж: международные санкции (из новейших – «санкции Навального»), массовые высылки российских дипломатов, невыдача виз;
- ультиматумы: угрожающие заявления Терезы Мэй в адрес российских властей относительно «отравления Скрипалей», а также ультиматум созданной Америкой международной коалицией с Великобританией или, например, блокировка международной коалицией выдвижения российского кандидата А. Прокопчука на пост главы Интерпола в 2018 г, с навешиванием на Прокопчука «ярлыков»-номинаций «шпиона и преступника». При этом раскрученный до глобального масштаба инцидент со Скрипалями повлек за собой очередной информационный вброс накануне выборов главы Интерпола: «всех, кто проголосует за российского кандидата, КГБ потом отравят, как Скрипалей»
- Дискредитация Прокопчука как «человека Путина» и «агента КГБ, связанного с Петровым и Башировым» – это в том числе попытка «выманить» на определенные действия самого Президента. Такая «приманка» однажды сработала, когда Владимир Путин был вынужден лично поручиться за Петрова и Баширова на Восточном Экономическом Форуме в 2018 г.
- «Аргентинское кокаиновое дело 2018» – другой пример информационного вброса путем контролируемой утечки в СМИ, когда в нужный момент «засветили» партию кокаина и стали ждать ответной реакции на «приманку» от главы МИД России, Совета Безопасности, то есть прослеживалась та же цель – компрометация ближайшего окружения Президента. Обвинение руководства страны в транзите наркотиков также продолжалось по цепочке: перехват крупной партии кокаина из Бразилии с маркировкой «Единой России» в Бельгии, когда от лица ЕР вынужден был объясняться Евгений Ревенко; потом перехватили аналогичные партии в Кабо-Верде на судне с российским экипажем в 2019.
- пример глобально раздутого скандал с WADA – прием, когда Российское руководство ловят «на лжи» и заставляют страну публично покаяться.

Можно вспомнить «дело Марии Бутиной», провокацию с захватом 33-х человек из ЧВК Вагнер в Белоруссии… Подобные операции имеют целью спровоцировать руководство страны на ответные действия и становятся все многочисленнее и изощреннее по мере приближения президентских выборов.

Схема новых вбросов происходит по цепочке путем контролируемых утечек. Так, сразу же после выборов 2021. «вспомнили и обновили» дело Скрипалей[13] (которое на время заглохло из-за пандемии и выборов в США), «вытащили из забвения» тему Литвиненко.

Пожалуй, провалом на этом фоне выглядит операция «Навальный». Сначала была ставка на будущего оппозиционного кандидата в президенты, но операция неожиданно «сорвалась». Классическая провокация с отравлением Навального шла по «шаблону Скрипалей». Потом в качестве «приманки» его возвращают в Россию. Хозяева Навального уверены, что его не посмеют лишить свободы в России, – вспомним фразу Навального в интервью после лечения в Германии «это невозможно, чтобы меня в России посадили». В результате он «выбыл из игры», провалился как единственный оппозиционный кандидат, а другого не нашли. Западу осталась надежда на ультиматумы, санкционный шантаж –

13 https://ria.ru/20210923/britaniya-1751338413.html (Дата обращения: 24.09.2021)

но в общем-то пока операция «Навальный» провалена: он жив, здоров и долго не выйдет из мест лишения свободы. В качестве альтернативы, развернули кампанию по делигитимизации выборов, которая тоже не достигла своей главной цели.

При этом все же определенную «пользу» наши западные политические оппоненты из своей русофобской информационной компании извлекли. Они учтут слабые места своих технологий и будут их корректировать и модифицировать, исправят все выявленные уязвимости в информационных системах. Будут развивать новые информационные атаки, часть которых привяжут к уже раскрученным старым операциям – такой эффект снежного кома, доводящего до критической массы (синергетический эффект). Целью таких провокаций будет максимальная дестабилизация социально-политической ситуации в стране перед выборами 2024, формирование установки на необходимость активных действий, участие в протестных акциях. Далее последует мобилизация протестных групп после соответствующей информационной накачки; после заявлений о нелегитимности выборов организуются протестные акции, направленные на совершение государственного переворота, свержение власти и государственного строя.

Все операции будут нацелены на конкретных руководителей государства, лиц, принимающих решения. Поэтому под ударом будет Президент и институт президентства как основа власти. Таким образом, со стороны «коллективного Запада» и его оппозиционной «пятой колонны» внутри страны это игра «в долгую» на разрушение политической системы государства и России в целом.

С.П. Юниченко
Эксперт Министерства обороны Российской федерации

О ВООРУЖЕННОМ ВМЕШАТЕЛЬСТВЕ ВО ВНУТРЕННИЕ ДЕЛА ДРУГИХ ГОСУДАРСТВ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ[1]

Уважаемые коллеги!

Общеизвестно, что вмешательство во внутренние дела других государств запрещено Уставом ООН. Однако история полна примерами постоянного нарушения этого основополагающего общепризнанного принципа международного права в угоду национальным интересам отдельных членов мирового сообщества, как правило, весьма развитых и могущественных.

Вмешательство во внутренние дела других государств может осуществляться вооруженным путем или без применения оружия. В рамках выступления я остановлюсь на вооруженном вмешательстве, которое Генеральной ассамблеей ООН в 1965 году признано синонимом агрессии[2] .

Данное положение позволяет определить основное содержание «вооруженное вмешательства во внутренние дела других государств с использованием информационно-коммуникационных технологий», опираясь на существующее определение понятия «агрессия»[3].

Напомню, что под агрессией понимается «применение вооруженной силы государством против суверенитета, территориальной неприкосновенности или политической независимости другого государства, или каким-либо другим образом, несовместимым с Уставом ООН, как это установлено в настоящем определении»[4].

Нарушение государственного суверенитета, территориальной неприкосновенности или политической независимости другого государства осуществляется в конкретных физических средах (земном, морском и воздушном пространствах). В отличие от них информационное пространство не имеет явно выраженных государственных границ. Вместе с тем, в последнее время мировое экспертное сообщество постепенно приходит к пониманию того, что понятие государственный суверенитет имеет такое же прямое отношение к информационному пространству, как и к геофизическим видам пространства. Все информационно-коммуникационные технологии (ИКТ), используемые для формирования информационного пространства, имеют своих национальных владельцев и размещены в пределах суверенных границ конкретных государств. Поэтому трансграничное нарушение их нормального функционирования (уничтожение, вывод из строя, подавление), которое может осуществляться с использованием вооруженной силы, основанной на использовании традиционного оружия, может квалифицироваться как нарушение суверенитета, территориальной неприкосновенности или политической независимости другого государства, т.е. как агрессия.

Вместе с тем, еще не сложилась практика применения ИКТ в качестве оружия против

1 Выступление подготовлено коллективом экспертов Минобороны России в области международной информационной безопасности в составе: Дылевский И.Н., Базылев С.И., Запивахин В.О., Комов С.А., Юниченко С.П., Шевченко А.Л., Завьялов Е.К., Каргин М.Н.

2 Седьмой абзац преамбулы «Декларации о недопустимости вмешательства во внутренние дела государств, об ограждении их независимости и суверенитета», Принятой резолюцией 2131 (XX) Генеральной Ассамблеи от 21 декабря 1965 года.

3 Определение агрессии. Утверждено резолюцией 3314 (XXIX) Генеральной Ассамблеи от 14 декабря 1974 года.

4 Статья 1 «Определение агрессии». Утверждено резолюцией 3314 (XXIX) Генеральной Ассамблеи от 14 декабря 1974 года.

таких объектов, результаты которого были бы соизмеримы с ущербом от традиционных видов оружия. Однако уже есть пример, подтверждающий наличие у отдельных видов ИКТ таких трансграничных возможностей, которые позволяют квалифицировать их реализацию как акт вооруженной агрессии. Например, компьютерная атака с использованием программного вируса Stuxnet на иранские ядерные объекты была номинирована в качестве одного из знаменательных военных событий по итогам 2010 года[5].

В ст.3 «Определения агрессии» закреплено положение о том, что акты агрессии могут совершать только государства с использованием вооруженных сил. Что касается иных физических и юридических лиц, то они могут считаться источником агрессии лишь в том случае, если действуют по заказу государственных структур.

Лица, которые осуществляют трансграничные нападения, руководствуясь террористическими, экстремистскими или корыстными мотивами, не могут рассматриваться в качестве источника агрессии. В этом случае информационные атаки должны квалифицироваться как террористические, экстремистские или иные уголовные преступления. Эти преступления имеют антиобщественный характер и поэтому различные государства, как правило, осуществляют совместное уголовное преследование виновных лиц в рамках международной правовой помощи.

Государства, с территории которых осуществляются трансграничные преступления, должны нести за них международную ответственность, т.к. они обязаны обеспечивать правопорядок на своей территории. Однако эта ответственность не имеет отношения к агрессии, которая по своей природе связана с военной политикой государства и ее прямой или косвенной реализацией в незаконной военной деятельности.

В ст. 2 «Определения агрессии» указывается, что «применение вооруженной силы государством первым в нарушение Устава является свидетельством акта агрессии, хотя Совет Безопасности может в соответствии с Уставом сделать вывод, что определение о том, что акт агрессии был совершен…». При проведении международно-правовой квалификации какого-либо конкретного акта трансграничного военного применения ИКТ данное положение следует интерпретировать с точки зрения необходимости учета двух основных факторов. Во-первых, агрессором может быть признано то государство, которое первым применило ИКТ в качестве оружия для решения своих военно-политических задач. Этот временной фактор в соответствии с резолюцией свидетельствует в пользу признания акта агрессии. Однако для вынесения окончательного вердикта Совет Безопасности ООН должен оценить наступившие последствия. В том случае, если последствия будут признаны серьезными, информационная атака может быть квалифицирована как акт агрессии.

Перечень возможных актов агрессии, приведенный в статье 3 резолюции, применительно к использованию ИКТ в качестве оружия выглядит следующим образом:

а) нападение на информационную инфраструктуру критически важных объектов на территории другого государства;

б) нападение на информационные объекты сухопутных, морских или воздушных сил другого государства;

в) действие государства, позволяющего, чтобы его территория, которую оно предоставило в распоряжение другого государства, использовалась этим другим государством для совершения акта агрессии с использованием ИКТ против третьего государства;

г) засылка государством или от имени государства банд, групп, иррегулярных сил или наемников, которые осуществляют акты применения ИКТ в качестве оружия против другого государства, носящие столь серьезный характер, что это равносильно перечисленным выше актам.

В ст. 4 «Определения агрессии» указывается, что «вышеприведенный перечень актов не является исчерпывающим и Совет Безопасности может определить, что другие акты представляют собой агрессию согласно положениям Устава». Поэтому конкретные крите-

5 Виктор Мясников Десять главных военных событий 2010 года, НВО, 24.12.2010; Top Military Developments of 2010, StrategyPage, January 14, 2011.

рии квалификации агрессии с использованием ИКТ могут быть дополнительно сформулированы в явном виде.

По нашему мнению, во всех перечисленных случаях ключевым признаком серьезности последствий использования ИКТ в качестве оружия следует считать их соответствие результатам применения традиционных видов оружия (гибель людей, физическое разрушение инфраструктуры, техногенные катастрофы и т.п.).

В заключение следует отметить, что приведенный подход может быть использован для выработки понятия «вооруженное вмешательство во внутренние дела других государств с использованием ИКТ» и его закрепления в итоговых материалах новой профильной Рабочей группы открытого состава ООН, начинающей работу в декабре этого года.

Благодарю за внимание!

Т.Н. Аитов
Кандидат физико-математических наук, Совет ТПП РФ по финансово-промышленной и инвестиционной политике

ТРУДНОСТИ ПЕРЕХОДА. О ПРОБЛЕМАХ ИМПОРТОЗАМЕЩЕНИЯ В ИТ

Тема импортозамещения острая, волнует всех- правительство, граждан, СМИ о ней много пишут. И, конечно, все происходящее большой интерес вызывает у разработчиков ПО и оборудования. Время от времени выходят очередные директивы – свежая появилась этим летом и установила, что 60% потребностей российских предприятий в необходимом для их работы ПО должны покрывать российские разработчики. Все это к 2024 году.

До нее мы часто цитировали директиву 91-Р, выпущенную Минфином – так называемый «список Силуанова», в котором перечислены крупнейшие госкомпании и дан другой ориентир – 50% ПО госкомпаний должно быть российским к 2022 году. То есть цифры ориентиров таковы 60% к 2024 году, 50% к 2022-ому году.

Появятся ли еще какие-то новые ориентиры? Выполним ли мы намеченное? Здесь мнения экспертов разделились. Одни считают, что намеченное выполнимо, другие (это скептики) выражают сомнения и напоминают, что по итогам 2020 года уровень проникновения российского ПО, увы, не превышает 10%. Однако, и пессимисты, и оптимисты единодушны в одном, что импортозамещение идет не так быстро, как бы нам всем хотелось…

Почему импортозамещение «буксует»? Почему идет не так быстро, как хочется?

Ответ очевиден: до сих пор в важной работе нет должной системности.

Вместо коротких списков компаний правильнее разрабатывать серьезные системные проекты, нацеленные на перевод конкретных госпредприятий на российское ПО. В проектах уже и предусматривать – кто именно? В какие сроки? И что будет выполнять?

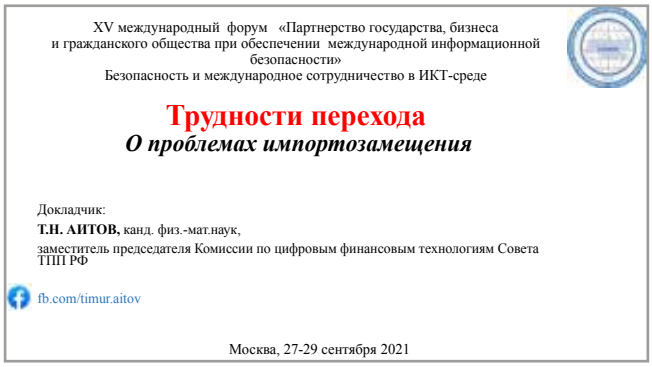
Каждый проект должен учитывать как реальные возможности игроков и иерархию построения ИТ-систем, так и совместимость ИТ-продуктов. Важно предусмотреть для каждого проекта финансирование. Необходим и компетентный организатор.

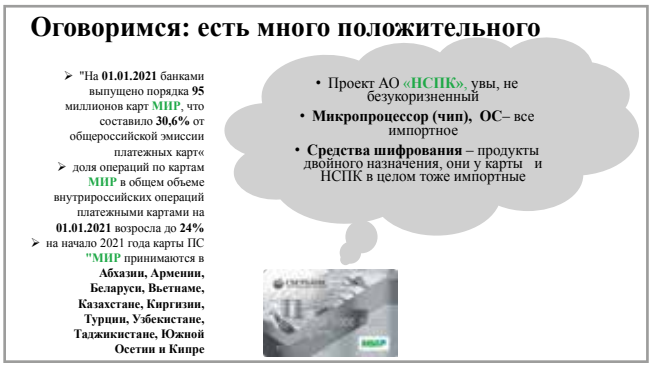
Проблем в импортозамещении много, конкретные примеры далее…

Сразу оговоримся, есть положительные примеры. Хорошо известен всем проект карты Мир – это успешный проект по импортозамещению. Сегодня 30% всего количества карт российских банков-эмитентов это карты Мир с их долей 24% по общему объему операций с картами.

Тем не менее, и проект Мир, увы, не безукоризненный в части импортозамещения. Микропроцессор (чип карты), и ОС карты – импортные. Средства шифрования – как у карты, так и НСПК в целом – тоже импортные. Про эти средства известно, что это продукты двойного назначения. Поэтому они в первую очередь подпадают под санкции. Тем не менее, проект Мир сможет работать даже если международные платёжные системы объявят о санкциях: наша НПСК сможет обслуживать карты Visa и MasterCard, эмитированных российскими банками на территории РФ без согласия МПС. Другое дело, что нельзя будет выпустить новые карты при завершении срока их эксплуатации. Но с теми что есть, НСПК сможет работать и остроту проблемы внезапного отключения карт внутри страны этим снимет. Это то, что касается розницы.

Что касается межбанковских расчетов, импортозамещения ЦБ пока не демонстрирует. Напомню, пару лет назад ЦБ и банки перешли на Перспективную платежную систему





(ППС), заменившую БЭСП. Но и в ППС остались «царствовать» IBM и ORACLE – два крупнейших мировых вендора.

Выключат ли IBM или ORACLE наши межбанковские расчеты при конфликтах? Думаю, вряд ли вендоры допустят полное отключение. Но вот замедлить работу своих систем – это они смогут и это реальный сценарий санкционного воздействия.

Завершая тему финансов, упомянем SWIFT, который политики всех мастей постоянно грозят нам отключить, выдвигают ультиматумы. Я в свое время даже написал специальную статью на тему отключения SWIFT и опубликовал в своей авторской колонке в FORBES. В статье подробно обосновал, почему SWIFTне отключат для России. Все причины там перечислил: и что, Россия входит в 20-ку крупнейших пользователей, и то, что наши представители есть в Совете директоров SWIFT и так далее. Но, конечно, на 100% я гарантировать то, что SWIFT не отключат, или, по крайней мере, не замедлят его работу (также, как в отношении межбанковских платежей), я не могу.

Наверное, правильно, что ЦБ запустил СПФС – Систему передачи финансовых сообщений – которую изображают сегодня в виде этакого символического «щелчка» по SWIFT. Однако, адекватной замены SWIFT наш проект пока не дал.

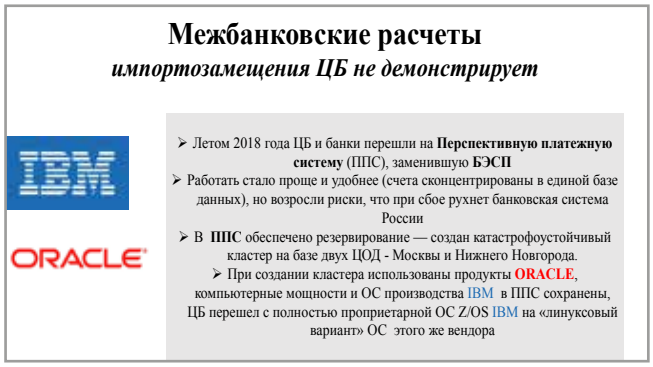
Примеры непростых задач замещения можно продолжить …

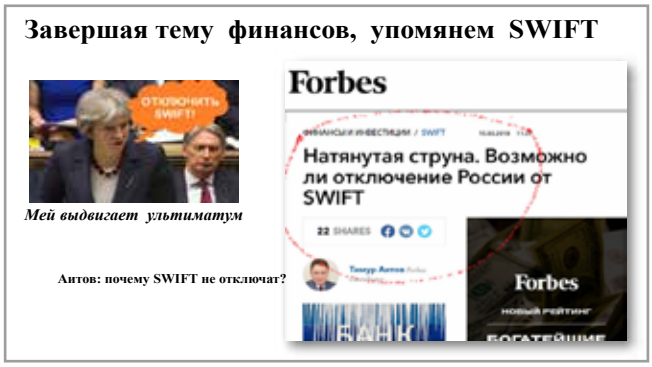
Приведу еще пример из сферы авиаперевозок. Существуют так называемые инвенторные системы, обеспечивающие решение задач бронирования и продажи авиаперевозок, а также, регистрации на рейс. У всех крупнейших наших авиаперевозчиков эти системы импортные. И даже если вы, скажем, летите в Челябинск или в Семипалатинск, и еще даже не взлетели, но ваша PNR (passenger name record) уже «улетела» в США – если это система Сайбор и перевозчик Аэрофлот. По этой PNR хорошо видно, кто вы, в каком кресле сидите, кто ваш попутчик, сидящий рядом и как вообще часто вы летаете в Семипалатинск или Челябинск.

Авиаперевозчикам были даны ориентиры для перехода с 1 января 2020 года на бронирование внутрироссийских авиаперевозок средствами отечественного ПО, но по разным причинам этого не произошло.

В чем основная причина и основная ИТ-проблема импортозамещения? Почему все ПО сразу заменить непросто? Ведь много разных продуктов уже выпущено, и много выпускается российскими разработчиками? Тот же «Мой офис»?

Дело в том, что «кусочками» на мировом рынке давно ничего не продаётся, вместо этого предлагается вертикально-интегрированный софт – экосистема ПО – этакая стена из «кирпичиков», на вершине которой ОС, ниже





СУБД, прикладные программы, программы безопасности и др.

Вся экосистема ПО работает как единое целое – и, если вам надо что-то поменять, вы вытаскиваете такой «кирпичик», вставляете на его место другой, и все продолжает работать. И вот подобных бизнес-экосистем российского производства у нас, скажу аккуратно, не хватает для реализации полноценного импортозамещения. Их практически нет. Разработчики опасаются, что они не «отобьют» затраты на разработку этих «стен»

Еще похожая проблема – существенные части крупных ИТ-систем вычленить и заменить невозможно. Как пример приведу ActiveDirectory (AD- «Активный каталог») – службу каталогов MS. AD используют все крупнейшие российские компании независимо от отраслевой принадлежности. AD позволяет сетевым администраторам быстро разворачивать ПО на миллионах компьютеров, отказываться от этого ПО никому из крупных компаний не собирается.

Отечественных аналогов AD пока нет. Есть одна российская компания, не буду ее назвать, она собирается в декабре этого года выпустить «российский AD» пока на 100 тысяч объектов. Как он будет работать? Примут ли его как стандарт все остальные мировые производители ПО и оборудования? Этот вопрос пока открыт.

Упомяну еще проблему.

Нет должной координации работ разработчиков.

Например, в реестр российского ПО сегодня попало около 60 операционных систем. Они все узкоспециализированные, немного отличаются друг от друга. Зачем их столько? Отобьют ли разработчики расходы на разработку? Думаю, вряд ли. Разработчикам даже банк не даст кредит на доработку систем, потому что будет опасаться излишне жесткой конкуренции и отсутствия спроса на ПО…

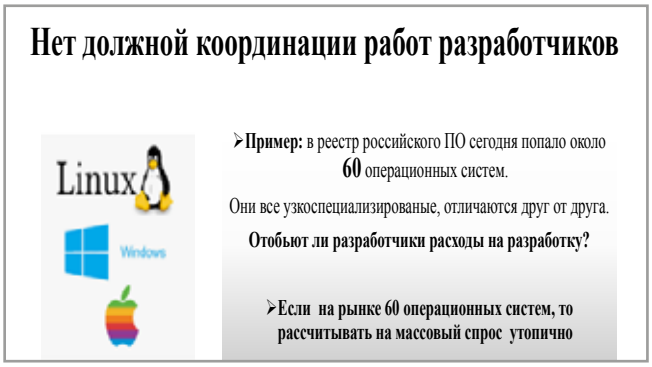
Хотя конечно и в части производства ОС есть удачные примеры.

Так, ГК Astra Linux сертифицировала свою ОС для всех используемых в России процессоров, как зарубежного производства, так и наших отечественных – «Эльбрус» и «Байкал Т1» … Я упомянул здесь «Эльбрус», но ведь и он не без проблем – для него есть ОС, это хорошо. Но под него нет прикладного ПО. А известные западные вендоры палец о палец не ударят, чтобы адаптировать свой софт под архитектуру Эльбруса.

Смогут ли сегодня наши предприятия полноценно перейти на отечественную ИТ-инфраструктуру? Увы, нет.

Это еще одно подтверждение отсутствие системности в работе

Еще важная причина (или отговорка?) чтобы не переходить на российское ПО. Например, некоторые банки считают, что риски, связанные с нарушением непрерывности работы



бизнеса (при массовой кампании по замене ПО), значительно превышают санкционные риски отключений. Да, если из-за санкций пропадает техподдержка, это плохо, говорят они, но если есть лицензия, то ПО всё равно будет работать. Можно подстраховаться и купить «ключи» для ПО на несколько лет вперед и проблем не будет

В завершение об акцентах, которые, на мой взгляд, надо правильно расставить в теме импортозамещения.

Во-первых, основной акцент должен делаться не на принуждении покупателей, а на координации работ и стимулировании производителей.

Это гораздо важнее.

Конечно, необходима системная работа, которой до сих пор нет в достаточном объёме.

И, наконец, главное. Задача импортозамещения никак не связана с выгодой – особой выгоды российское ПО не дает: оно как правило, дороже и менее функционально.

Цели важнее: импортозамещением необходимо обеспечить должную безопасность страны.

А.В. Бирюков
К.и.н., доцент, ведущий научный сотрудник и ведущий эксперт Центра международной информационной безопасности и научно-технологической политики МГИМО МИД Российской Федерации

О ГУМАНИТАРНЫХ АСПЕКТАХ ИНФОРМАТИЗАЦИИ И МЕЖДУНАРОДНАЯ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

В связи с проектом Конвенции об обеспечении международной информационной безопасности хотелось бы высказать ряд соображений, касающихся гуманитарных аспектов информатизации.

В цифровую эпоху в контексте научно-технического прогресса усиливается видение будущего человечества, связанного с симбиозом человека и машины. В ряде стран реализуются конкретные проекты в данной области. А уж рассуждения на эту тему доминируют в интеллектуальном дискурсе, чему способствует быстрое практическое развитие искусственного интеллекта и других цифровых технологий в круге NBICS. Появилась и набирает «вес» идея технологической гегемонии, которая открывает столбовую дорогу к эпохе технологической сингулярности.

По оценке футурологов, технологическая сингулярность может стать реальностью к середине XXI века, когда разум человека намного отстанет от искусственного интеллекта. Это верная оценка с точки зрения умения просчитывать варианты с помощью алгоритмов. В этом смысле искусственный интеллект становится важным помощником человека[1]. При этом вовсе не исключено, что гегемония искусственного интеллекта не трансформируется в главную угрозу человечеству[2].

Наращивание потенциала искусственного интеллекта происходит на фоне относительно слабого понимания возможностей мозга человека, особенно в части, касающейся творчества и созидания. Между тем в данном аспекте образованный и творческий человек превосходит искусственный интеллект. Важно подчеркнуть, что российская научная школа проводит углубленные исследования естественного интеллекта, результаты которых будут во все большей степени востребованы[3].

В настоящее время активно развивается концепция трансгуманизма, которая превращается в мировоззрение, своеобразное политическое движение и медиа-платформу. Эта концепция представляет собой попытку преодолеть Человека, отринув в нем все человеческое и создав кибернетическое пост-человечество. Трансгуманизм получает поддержку западных ученых и специалистов. Данная тема внимательно изучается в России[4].

Все перечисленное означает, что на Западе готовятся к апофеозу доминирования технологий в гибридном мире цифровой эпохи и по мере развития НТП рассматривают перспективу вытеснения Человека разумного на обочину цивилизационного развития на Земле. Между тем большинство стран считает, что в XXI веке и в будущем человек дол-

1 Рэй Курцвейл. Эволюция разума. М.: ЭКСМО, 2015

2 Nick Bostrom. Superintelligence: Paths, Dangers, Strategies. www.amazon.com

3 Ларина Е.С. Человеческое мышление и искусственный интеллект: российский аргумент в международном сотрудничестве. В кн. Международная информационная безопасность: новая геополитическая реальность. М:. Аспект Пресс2021

4 Виталий Аверьянов, Игорь Шнуренко, Михаил Делягин, Максим Калашников, Елена Ларина, Сергей Баранов. Трансгуманизм: цифровой левиафан и голем-цивилизация. М:. Книжный мир, 2021.

жен стоять в центре системы национального роста и международных отношений, увеличивая долю знаний и творческого компонента в постиндустриальном способе производства, усиливая роль социально-гуманитарных аспектов и значимость морально-нравственных основ развития.

Как представляется, в подходе к международной информационной безопасности следует исходить из особой ценности Человека разумного. В связи с этим было бы правильным в международных основополагающих документах или официальных комментариях к ним подчеркивать особую роль человека в стиле формулы, предложенной Всемирной комиссией по этике научных знаний и технологий, которая в свое время была создана при ЮНЕСКО. В одном из докладов этой комиссии акцентируется внимание на том, что благополучие и интересы человека приоритетны по отношению к науке и технологиям[5]. В нашем случае речь идет о проекте Конвенции ООН об обеспечении международной информационной безопасности. Преамбула этого документа прописана замечательно, однако в ходе обсуждения проекта в стенах ООН можно было бы подчеркнуть актуальность МИБ с точки зрения продвижения гуманитарных аспектов человеческой цивилизации.

Если продолжить рассмотрение гуманитарного контекста международной информационной безопасности современного общества, то представляется важным отметить парадоксальную тенденцию – деградацию человека цифровой эпохи, прежде всего в духовно-нравственном отношении. Озабоченность по этому поводу уже высказывалась в России на солидном уровне. Однако подобная негативная оценка вызывает споры.

Прежде всего необходимо отметить, что научно-технический прогресс может стать источником угрозы развитию человечества. Эта мысль все чаще обсуждается учеными и специалистами. Об этом говорилось, в частности, на проводившейся Институтом сложности в Санта-Фе и Академией АНБ США конференции по наиболее сложным вопросам современности[6]. Опасность цифровых технологий рассматривается в качестве всадника Апокалипсиса. Подобная оценка прозвучала из уст генерального секретаря ООН. При этом, однако, на данном этапе основную проблему представляет неадекватное управление НТП, осуществляемое людьми. Следовательно, в дихотомии человек-машина опасность исходит в первую очередь от неправильных решений человека, который организует работу с использованием машины.

Самое главное обстоятельство, наблюдаемое всеми, заключается в том, что человечество в буквальном смысле захлестнула информационная лавина. С 2015 года в мире было произведено столько же информации, сколько за всю историю существования письменности[7]. И каждый последующий год объем информации удваивается. Накапливаются и обрабатываются большие данные, которые все чаще рассматриваются в качестве важнейшего сырья XXI века. Эффективно работать с таким массивом информации можно только с опорой на достижения НТП.

Многие используют потенциал цифровых технологий и одновременно приходят к пониманию, что человек «захлебывается» в информационном море, не может сориентироваться и найти востребованные им качественные объективные данные. У людей не развиваются аналитические способности обработки информации и развивается её поверхностное восприятие. К информационной передозировке добавляется цифровая зависимость.

Выросло целое поколение людей, привыкшее опираться на технические средства и не считающее нужным обрабатывать информацию с помощью интеллектуальных методов человеческого разума и хранить такой способ в памяти. По этой причине количество лиц, обладающих долговременной памятью – базой креативности, стремительно снижается[8] .

5 Бирюков А.В. Этика как инструмент обеспечения стабильности в контексте международной информационной безопасности. Выступление на 12-м форуме «Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности». Специальный выпуск журнала «Международная жизнь» Россия и глобальные вызовы в области информационной безопасности, с.115-118 https://interaffairs.ru/virtualread/garmish2018/publication.pdf

6 Елена Ларина и Владимир Овчинский. «Черный шар» и глобальная инквизиция Ника Бострома. Наш Современник. 2019, №2.

7 См. Климович А. Вопросы философии Больших данных. Pdf.

8 Курпатов А. Современный человек страдает от информационного ожирения // Вместе-РФ, 12.02.2020 – URL: https://vmeste-rf.tv/news/joyce-brothers-here-a-modern-person-is-suffering-from-information-obesity/ (дата обращения: 05.10.2020)

Возник и развивается новый тип мышления, которое «потребляет» упакованную нужным образом информацию и не нацелено на творческий процесс. На передний план выходят клиповое мышление, цифровое слабоумие и информационное оглупление. Эти явления охватывают представителей всех возрастов и прежде всего поколения XXI века.

К социальной дифференциации, которая усиливается в цифровую эпоху, добавляются интеллектуальный и образовательный разрыв в информационном обществе. Значительная, если не большая часть населения абсолютизирует пользу стереотипного поведения, что сужает возможности исследовательского подхода и критической оценки собственных ошибок, а также создает условия для возникновения отношений зависимости. В обществе развивается когнитивный диссонанс у людей, вынужденных жить в долг, не уверенных в завтрашнем дне, подверженных страху выпасть на обочину культивируемого образа жизни, ощущающих давление паноптикума, не согласных с насаждаемыми ценностями.

Все перечисленное является нам в разных странах и имеет глобальный характер. Именно в таком гуманитарном контексте на передний план общественной информатизации и международной безопасности выдвинулись поведенческие технологии, когнитивное противоборство и ментальное воздействие, ставшие одним из важнейших фронтов противостояния[9]. Основная его идея – воздействовать на сознание, разум и волю человека, социальных групп и больших масс людей таким образом, чтобы «зомбировать» эти объекты и настроить их на саморазрушительные действия.

Может возникнуть вопрос – а не завиральная ли это попытка переформатировать целый народ и ориентировать его на новые ценности и смыслы? Прямого ответа на этот вопрос пока нет. Опыт Украины, думается, только частично затрагивает тему войны современного типа. Главное состоит в том, что в её основе лежат достижения науки о человеке и его социальной активности[10].

В этом выступлении не рассматриваются конкретные механизмы этой борьбы. Некоторые из них освещены другими участниками форума, поскольку именно в цифровую эпоху происходит стремительное расширение возможностей целенаправленного воздействия на людей со стороны, что связано с международными отношениями и международной информационной безопасностью. Сегодня были затронуты темы пост-правды, углубленного обмана, которые быстро развиваются в условиях информационной революции.

Повторю, что упомянутые особенности работы мозга и социально-психологические процессы протекают повсеместно в условиях глобальной информационной революции, однако в каждом национальном обществе имеется специфика, обусловленная историко-культурным и социально-психологическим контекстом, которая заслуживает внимания.

В современной России, особенно в 90-е годы прошлого века, культивировалась абсолютная ценность зарубежного опыта общественного развития, что частично удалось преодолеть. В ходе поиска оптимальной общественной модели происходило занижение оценки достижений СССР. Такая однобокость в результате привела к забвению даже славных страниц истории Отечества, игнорированию достижений не только Советского Союза, но и Российской империи в области государственности, науки, культуры и просвещения, а также на полях брани. Незнание не только философских и этических основ российской истории и культуры, но и героизма предков ограничивает гражданские горизонты и ответственность тех россиян, кто связывает судьбу со своей родиной.

Давно назрел вопрос формирования паутины смыслов и целей цифрового общества на основе национальной истории и культуры, новых и традиционных ценностей и традиций. Говоря коротко, речь идет об идеологии. Сейчас получила распространение мысль о том, что идеи и ценности надо адаптировать под утвердившиеся реалии в обществе. На наш взгляд, поступать необходимо ровно наоборот. Безусловно учитывать реальность надо, но не идти на поводу у сложившихся негативных явлений. Необходима целостная си-

9 См. А.В. Бирюков, М.Б. Алборова. Социально-гуманитарные риски информационного общества и международная информационная безопасность. М:. Аспект Пресс, 2021.

10 Ларина Елена, Овчинский Владимир. Кибервойны XXI века. О чем умолчал Эдвард Сноуден. М.: Книжный мир, 2014.

стема комплексного воздействия на граждан нашего государства. Причем в первую голову она должна базироваться на справедливых смыслах, разделяемых ценностях и ясных целях. И особенно важно, чтобы идеология была широко растиражирована в обществе, учитывалась в деятельности разных профессий и доминировала бы в средствах массовой информации и социальных сетях. Речь идет о гибких и умных формах, а не о кондовых пропагандистских приемах.

Не менее важный содержательный аспект этой работы связан с выстраиванием этических основ информационного общества в России на базе сочетания традиционных ценностей и новых общественных реалий, обусловленных цифровой эпохой. Адекватная этическая система, думается, должна включать в себя такие компоненты как совесть и лояльность.

Очень важно восстановить целостный механизм мудрой социализации поколений XXI века, с головой погруженных в зарубежные социальные сети и киберпанк, а также испытывающих массированное негативное воздействие со стороны «партнеров». Необходимы мероприятия по противодействию подобному давлению. Не менее существенно вернуть роль семьи в сфере социализации, которая всегда была велика в Российской империи и Советском Союзе. Это сложная задача в условиях, когда разрушение семьи, может быть, не в такой прямой формулировке подпитывается разными идеями и практическими шагами. Общественное движение ЛГБТ, например, относится к подобным деяниям.

Не менее актуальна роль образования и культуры в социализации людей. Чтобы повысить значимость подобной социальной функции, необходимо включение воспитательного компонента по линии образования и культуры в общественную жизнь России и каждого человека буквально с молодых ногтей. Бездуховность значительной части людей просто поражает. Кричащих примеров очень много. Один Алишер Моргенштейн чего стоит. Судя по гонорарам и приглашения на крупные форумы, он стал «героем нашего времени». С такими «героями» России будет чрезвычайно сложно победить в интеллектуальной войне.

В связи с этим подготовка молодежи, в том числе специалистов в области обеспечения международной информационной безопасности, представляет собой суперактуальную проблему. Здесь, пожалуй, было бы полезным перенять опыт нашего соседа Китайской Народной Республики, которые ежегодно готовят 15 тыс. человек. А потребности страны составляют 1.5 миллиона человек.

В заключении хотелось бы особо подчеркнуть, что гуманитарные аспекты информатизации представляют собой не просто контекст международной информационной безопасности России, но и направление вклада МИБ в стратегию организации обороны страны в условиях информационного, психологического и интеллектуального противоборства. И наконец важно сказать, что понимание гуманитарных аспектов информатизации весьма полезно для анализа феномена МИБ и управления им, что будет способствовать повышению качества политики России в данной области.

Бай Яцзе
МГИМО МИД России (Китай)

ЦИФРОВОЙ СУВЕРЕНИТЕТ И СРЕДСТВА МАССОВОЙ КОММУНИКАЦИИ: ВЗГЛЯД ИЗ КНР

В нашем традиционном сознании теория суверенитета включает, например, территориальный суверенитет, суверенитет территориальных вод, валютный суверенитет, экономический суверенитет, культурный суверенитет и т. д. А с развитием шестого технологического уклада (на Западе известен как Industry IV) с нано, био-, инфо- и когнотехнологиями резко ускорило процессы цифровизации, страны также начали задумываться о цифровом суверенитете в киберпространстве. Особенно в контексте пандемии 2020 года, начиная с которой сфера цифровых технологий уже стала ключевым полем битвы в геополитической борьбе. Концепция киберсуверенитета эволюционирует. Эта эволюция фактически является проблемой цифровой безопасности и геополитической проблемой, вызванной цифровой и технологической конкуренцией. Цифровой суверенитет – это концепция, производная от концепции киберсуверенитета.

Таблица 1. Из 30 кейсов, практически половину составили связанные с Россией, Китаем и постсоветским пространством

1	Russian snap exercises in the High North Coercion	Coercion through threat or use of force
2	Confucius Institutes	Government Organised Non-Government Organisations (GONGO)
3	2007 cyber attacks on Estonia	Cyber operations
4	US Transit Center at Manas	Economic leverage
5	The spread of Salafism in Egypt	Political actors
6	Disinformation in Sweden	Media
7	Hamas' use of human shields in Gaza	Lawfare
8	The 2010 Senkaku crisis	Economic leverage
9	Humanitarian aid in the Russo-Georgian conflict	Lawfare
10	Chinese public diplomacy in Taiwan	Exploitation of ethnic or cultural identities
11	Detention of Eston Kohver	Espionage and infiltration
12	Finnish airspace violations	Territorial violation
13	South Stream pipeline	Energy dependency
14	Russian language referendum in Latvia	Exploitation of ethnic or cultural Identities
15	Institute of Democracy and Cooperation	Academic Groups; NGOs; GONGOs
16	Zambian elections 2006	Economic leverage; Political actors
17	Serbian Orthodox Church	Religious groups
18	Communist Party of Bohemia and Moravia	Political actors
19	Bronze night riots	Exploitation of ethnic or cultural identities / Agitation and civil unrest

Таблица 1. Из 30 кейсов, практически половину составили связанные с Россией, Китаем и постсоветским пространством (продолжение)

20	Russiky Mir Foundation in the Baltics	Government Organised Non-Government Organisations (GONGO)
21	Criminal networks in the Donbas	Bribery and corruption
22	Civil disorder in Bahrain 2011	Agitation and civil unrest
23	Pakistani involvement in Yemen	Economic leverage
24	Operation Parakram	Coercion through threat or use of force
25	Snap exercises and Crimea	Coercion through threat or use of force
26	Electronic warfare during Zapad 2017	Territorial violation
27	Russian espionage in Sweden	Espionage and infiltration
28	Religious extremism in the Netherlands	Exploitation of ethnic cultural identities
29	Cyber attacks on ROK & US	Cyber operations
30	Casas del ALBA in Peru	NGO

Концепция «цифрового суверенитета» определена в документе «Цифровой суверенитет для Европы», выпущенном Европейским парламентом 14 июля 2020 года: 'digital sovereignty' refers to Europe's ability to act independently in the digital world and should be understood in terms of both protective mechanisms and offensive tools to foster digital innovation (including in cooperation with non-EU companies). («“Цифровой суверенитет” означает способность Европы действовать независимо в цифровом мире, и его следует понимать с точки зрение как защитных механизмов, так и наступательных инструментов для стимулирования цифровых инноваций.)

Стоит отметить, что определение «цифрового суверенитета» следует понимать двояко: с одной стороны – это механизм самозащиты Европы, а с другой – орудие наступления.

Система Интернета вещей, система блокчейнов и другие новые цифровые технологии, разработанные на основе Интернета, начали процветать повсюду. Цифровой контент, такой как анализ информации на основе больших данных, рекомендации алгоритмов искусственного интеллекта, моделирование, прогнозирование и т.д., распространяется среди разных стран. Ускоренное распространение информации через средства массовой коммуникации способствует усилению глобализации между странами. Однако вытекающая из этого проблема заключается в том, что неограниченное трансграничное распространение средства массовой коммуникации, а точнее, агрессивное трансграничное распространение средства массовой коммуникации оказывает большое вредное влияние на цифровой суверенитет страны.

Здесь это карта распространения пользователей Интернета, видно, что новые средства массовой коммуникации уже популярны по всему миру.

8 сентября текущего года NATO strategic communications center of excellence (Центр передового опыта стратегических коммуникаций НАТО) опубликован новый документ: «Инструментарий гибридных угроз стратегических коммуникаций» (strategic communications hybrid threats toolkit).

В этом отчёте коммуникация поднята до стратегического уровня, и показано, как применять принципы стратегической коммуникации на национальном уровне. В отчёте проанализировано 30 сценариев с гибридными действиями государственных субъектов, разделены на 14 предметных областей угроз. Из 30 кейсов, практически половину составили связанные с Россией, Китаем и постсоветским пространством. Путем сравнения данных в тематических исследованиях выявляются закономерности и тенденции, а также обобщается уязвимость целевой страны, которую можно использовать.

Одним из наиболее типичных примеров являются беспорядки в Гонконге (Китай), в 2019 году. В этих протестах очень важную роль сыграли высокие информационно-коммуникационные технологии. В таких протестах принимают участие в основном молодые люди.

Таблица 2. В последние годы в Китае опубликованы документы о цифрового безопасности

Время	Документы
09.2021	«Киберсуверенитет: теория и практика (версия 3.0)»
04.2021	«Отчёт о развитии цифрового Китая (2020)»
11.2020	«Инициатива действий совместного создания сообщества единой судьбы киберпространства»
11.2020	«Киберсуверенитет: теория и практика (версия 2.0)»
09.2020	«Глобальная инициатива по безопасности данных»
06.2019	«Совместное заявление о развитии отношений всеобъемлющего партнёрства и стратегического взаимодействия, вступающих в новую эпоху»
12.2017	«Реализация национальной стратегии больших данных и ускорение строительства цифрового Китая»
06.2017	«Закон Китайской Народной Республики о кибербезопасности»

В ходе этого протеста социальная сеть Telegram была основным местом общения бунтовщиков, а онлайн-форум «Лянь Дэн» – основной позицией общественного мнения. Протестующие, использовав специально выбранные объекты и контент, злонамеренно создавали постановочные фото и видеофейки, размещали их на социальных платформах для широкого распространения, дискредитируя полицию и даже правительство, чтобы ввести в заблуждение населения, не знающие правды.

Протестующие злонамеренно исказили разумное поведение на политическом уровне через социальные сети. Такое поведение больше подходит понимать как средство «политической пропаганды».

По совпадению, аналогичные ситуации произошли в Беларуси в протестах против президентских выборов в 2020 году

Телеграмм канал NEXTA является основным местом распространения информации о протестах. Каждое воскресенье оппозиция организует масштабные демонстрации в стране через канал Nexta Live в Telegram.

Оппозиция в Беларуси создала радиостанцию в Польше, зарегистрировала аккаунт в Telegram и имеет одноимённый аккаунт в YouTube. Они провели большую пропагандистскую работу с помощью этих средств массовой коммуникации. Эти оппозиционные информационные каналы очень популярны в Беларуси. Население Беларуси составляет 10 миллионов человек, а у оппозиции 2 миллиона подписчиков на аккаунте Telegram. По сравнению с традиционными средствами массовой коммуникации, социальные платформы, такие как YouTube и Telegram, Твиттер, Фейсбук и т.д. невозможно полностью контролировать.

Средство массовой коммуникации усиливает и обостряет политическую борьбу через распространение дезинформации, слухи и разжигания ненависти, потому что это облегчает сбор схожих голосов. Если иностранные силы станут контролировать киберпространство, то оно под руководством будет полно подстрекательских слов, лжи и языка ненависти.

В последние годы Китай продемонстрировать свою решимость защищать цифровой суверенитет в различных областях. Особенно после того, как в Китае произошла санкция США против компании HUAWEI.

В декабре 2017 года Китай выпустил документ «Реализация национальной стратегии больших данных и ускорение строительства цифрового Китая» на национальном уровне.

В марте текущего года, министр иностранных дел КНР Ван И (Wang Yi) заявил, что Китай и Россия должны совместно бороться против «цветных революций» и распространения дезинформации, а также поддерживать свой суверенитет и политическую безопасность; в 3.26 В выступлении президента Путин на конференции Совета Безопасности также подчеркнул важность киберсуверенитета. На вопрос о том, что отстаивать цифровой суверенитет в киберпространстве позиции Китая и России совпадают.

В.В. Щёголев
Советник Заместителя Руководителя Фонда Росконгресс, доктор политических наук

НАСТОЯЩЕЕ И БЛИЖАЙШЕЕ БУДУЩЕЕ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ И СОТРУДНИЧЕСТВА: НАРУШЕНИЯ НАЦИОНАЛЬНЫХ СУВЕРЕНИТЕТОВ ИЛИ БЕСКОНФЛИКТНОЕ ПРОСТРАНСТВО ДОВЕРИЯ И СОДЕЙСТВИЯ РАЗВИТИЮ?

Современные молниеносно развивающиеся киберпроекты и технологии на пороге **второй квантовой революции** при использовании свободно доступных квантовых операций и вычислений, при задействовании квантовых коммуникаций и квантовой метрологии вполне позволяют осуществление **уникально скоростных и крупномасштабных сквозных межотраслевых расчётов и определений алгоритмов жизнедеятельности,** оптимальности производств, усовершенствования процессов и построения многоаспектных рекомендательных матриц и графиков, якобы, абсолютной полезности и единонаправленного существования.

При этом стоит иметь в виду, что **обладание** такими компетенциями в комплексе с наличием квантового компьютера, даёт возможность рассчитать и приступить не к перестройке или структурной реорганизации составных частей систем управления и потребления, а к полному переустройству групп отраслей, оптимальному построению заново и многоструктурированию технологических цепочек, формированию с большой периодичностью **обновляемых приоритетов в исключительно производящих секторах промышленности, в наукоёмких сферах военно-технического строительства, направлениях политико-дипломатической работы, разделах экономического и технологического общественного роста.**

Страна – обладатель таких технологий безапелляционно уходит в самостоятельное плавание и формирует свою повестку индивидуально, не оглядываясь ни на кого, не задумываясь о курсе своей национальной валюты, не ограничивая свою элиту и соотечественников во мнении о собственной привлекательности, и, в конечном итоге, **приступает к предопределению судьбы некоторых соседей.** Все вышеприведённые перспективы неотехнологических конструкций, хоть и утрированы в некотором смысле, но, тем не менее, они значительно расширяют устойчивость политиков, инструментарий дипломатов и несокрушимость арсеналов вооружённых сил страны, нашедшей ресурсы и активы для такого прорыва.

До момента появления такой сверхдержавы, страны, обладающие ядерным оружием вынуждены, каждая по **своим ключевым** направлениям, формировать некоторую международную повестку и вовлекать в круг её политико-дипломатических отношений **как можно больше участников,** особенно из числа членов Совбеза ООН. **До настоящего времени, а это до 2023 года, ведущие кибердержавы едины во мнении** и… намерены, без подписания каких бы то ни было документов, ограничивать действия своих партнёров в виртуальном пространстве, но **не жертвовать своими разработками в кибервызовах,** устраиваемых даже для партнёров по блокам. **Разумеется, это не относится к России!** По этим причинам ожидать в ближайший год каких-то двусторонних, либо иных, соглашений между «владельцами ядерных зонтиков» о нераспространении или контроле за кибервооружениями не приходится.

Слишком привлекательными являются эти новые забавы, которые, в понимании боль-

шинства потребителей сюжетов Тик-Тока, Фэйс-бука и пр., оружием не являются. И прежде чем придет понимание о том, что необходимы «взаимные ограничения», «этика и достоверность преподносимой информации» и «правила игры», в т.ч. для определённых категорий заинтересованных, при пользовании электронным информационным пространством, неизбежны серьезные трансграничные скандалы, социальные происшествия, энергетические веерные и иные кризисные ситуации.

Да и в самом деле, разве мы все – участники Форума всерьёз думаем, что расстрелы в школах одноклассников прекратятся по образу и подобию игры «ГэТэА» и других аналогичных «стрелялок»? Мы же понимаем, что это бизнес запада против стран бывшего социалистического лагеря с целевым подростковым направлением, привязанный к психоневротическим воздействиям на неокрепший мозг школьников и студентов. В Российскую армию такие школьники не пойдут, их прельщает сидячее «стреляние» до изнеможения, да ещё и в группах от 5-ти до 10 человек, фактически «взвод на взвод». Важно отметить, что западная «вакханалия» **в детских сегментах российского интернета,** мешающая нашим подросткам спокойно учиться, **в ближайшее время прекратится.** Президент России Владимир Путин дал поручение рассмотреть вопрос об установлении госрегулирования оборота информации для детей в Интернете. Поручение направлено российскому правительству, а также комиссии Госсовета России. Глава российского государства поручил ответственным лицам подготовить доклад по теме до 1 марта 2022 года. А на российском телевидении, в отличие от европейского и американского, не показывают детям дошкольного и школьного возраста мультфильмы про жизнь «какашек» и «гениталий», к которым, как мы все понимаем, российские хакеры не причастны, хотя глупостей не убавляется.

Такие западные разработки – задачи кибератак общего (широкого) применения социотехники, содержащие **методы социальной инженерии.** С их помощью злоумышленники пытаются убедить человека, выбранного в качестве объекта кибератаки, совершить то или иное действие, приводящее к заражению системы или раскрытию ценной информации. Чаще всего этот метод применяется при промышленном шпионаже и более выверенных и длительных отношениях с объектом. В ходе социотехнической атаки объект атаки не осознает, что его действия являются вредоносными. Методы социотехники основаны на злоупотреблении доверчивостью объекта атаки, а не на использовании его преступных инстинктов. Атаки можно разделить на две категории: **«охота»** и **«животноводство».**

«Охота» предполагает получение информации при минимальном взаимодействии с объектом атаки. При таком подходе взаимодействие, как правило, сводится к одиночному контакту атакующего с атакуемым, и после получения информации атакующий сразу прекращает общение с атакуемым. «Животноводство» предполагает установление продолжительных отношений с объектом атаки с целью его «доения» (т. е. получения информации) на протяжении длительного периода времени.

Социотехнические атаки в категориях «охота» и «животноводство» проводятся, как правило, **в четыре этапа.**

Первый этап – сбор информации. Цель этого необязательного этапа — сбор об объекте атаки информации, которая поможет «зацепить» его: увлечения, место работы, поставщики финансовых услуг и т. п.

Второй этап – «зацепка». Цель «зацепки» – успешно «заговорить» объект атаки, вступив с ним в контакт и создав повод для взаимодействия. Западные психологи выделяют шесть рычагов «зацепки» и влияния на объект:

- **взаимность** (получив что-либо, люди чувствуют себя обязанными и стремятся дать что-нибудь взамен),
- **дефицит** (люди склонны выполнять просьбу, если считают, что речь идет о чем-то редком),
- **последовательность** (если объект атаки пообещал что-то сделать, то он будет стремиться выполнить обещание, чтобы не казаться неблагонадежным),
- **симпатия** (объект атаки охотнее выполняет просьбу, если злоумышленник ему симпатичен),
- **власть** (люди склонны выполнять просьбы, поступающие от представителей власти),
- **социальное доказательство** (склонность выполнять просьбу, если другие

делают то же самое). В российском понимании проблемы – к подчёркнутым добавляются **внезапность** и **убедительность** преступников, подлежащих уголовному преследованию, где бы он не находился, хоть на атоллах Тихого океана.

Третий этап – «разводка». Суть его заключается в выполнении основной части атаки. Это может быть раскрытие информации, переход по ссылке, перечисление денежных средств и т.д.

Четвертый этап – выход, т.е. завершение взаимодействия. Во многих атаках, относящихся к категории «животноводство», злоумышленнику выгодно выходить из игры так, чтобы не вызывать подозрений.

Попытки применения методов социотехники не всегда линейны: та или иная отдельная атака может быть частью более крупной кампании по сбору взаимосвязанных данных. Например, злоумышленники могут провести ряд атак, относящихся к категории «охота», а затем, используя собранную информацию, инициировать атаку, относящуюся к категории «животноводство». Нередко для социотехнических атак используются вредоносные веб-сайты и их операторы, т.е. примерно в **20% атак, проводимых с целью шпионажа, для доставки вредоносного ПО используются механизмы комплексного стратегического взлома веб-сайтов.** Самыми распространенными видами социотехнических атак с использованием электронной почты являются фишинг вообще и целенаправленный фишинг в частности. **Рассылка электронных почтовых сообщений – эффективный метод проведения атаки,** поскольку, по ссылкам в фишинговых электронных сообщениях переходит около 18% пользователей.

Телефон в качестве канала связи пользуется популярностью у информационных посредников. Бывает, что злоумышленники знакомятся и встречаются с объектом лично, тогда они могут принудительно или обманным путем заставить его предоставить информацию. Опасность социотехнических атак крайне серьёзна и чаще употребима по сравнению с другими формами кибервоздействия, если не считать **«закладки»**. С их помощью киберпреступники незаконно получают доступ к информации, используемой в различных вредоносных целях. Для эффективной борьбы с этой проблемой необходимо понимать природу социотехнических атак. Это значит, что необходимо уметь выявлять наиболее вероятные действующие лица, используемые ими методы проведения атак и имеющиеся у них ресурсы, а затем принимать соответствующие меры по снижению уровня риска.

Если пока холодильники, телевизоры, стиральные машины и прочие бытовые приборы не «сбегают» и не устраивают бунты своим владельцам, а мирно стоят и передают хозяевам закладок все оперативные данные о группе владельцев и их кухонных новостях, то вот с телефонами и прочими гаджетами дело обстоит на самом деле очень серьезно. По данным экспертов «Лаборатории Касперского», **ежегодно в 2,5 раза возрастает количество ситуаций, когда фиксируется «удаленный доступ» к телефонам их владельцев. «Стараниями» хакеров телефоны, якобы «сами», включали микрофон** и начинали записывать разговоры, которые вели их владельцы. Еще более тревожные показатели – по кражам с телефонов хранящейся в них информации. Такие случаи возрастают в среднем за год в 5 –7 раз.

В связи с этим мы имеем в виду, что обработка этой информации суперкомпьютерами – дело секундное, с выводами, данными об объектах, их связях и контактах, общественной, государственной, семейной, личной жизни, хобби и интересах, данными по лицевым и оборотным счетам, психосоматическом, физиогномическом и медицинском их состоянии, участии в частных клубах, отношении к генному составу – всё это предметы и направления мобильности объектов, интересующих западную специализированную интернет-сферу, вполне себе покорно выполняющую доктринальную наступательную задачу РУМО, АНБ и их подельников, Комитета НШ НАТО и прочих примкнувших в поисках русского хакерского следа или иного участия российских спецорганов в, различного рода американских, британских, чешских, польских, украинских, немецких и т.д., упущениях, финразборках и разгельдяйстве, особенно если это касается президентских выборов. С той лишь разницей, господа западные участники, что «мы не ваших будем», у нас «чубы не трещат» от ваших разборок, нам те-

перь интересно «кто – кого». И потом – кто же стал инициатором кибернападений, сразу же после возведения монумента на месте башен-близнецов и провозглашения «крестовой войны» с международным и азиатским терроризмом?

Разве не Соединенные Штаты впервые официально обвинили российские власти в организации хакерских атак. **В обнародованном 7 октября 2016г. специальном заявлении Министерства внутренней безопасности США и офиса директора Национальной разведки утверждалось, что российские хакеры взломали почтовые серверы американских граждан, политических организаций и госструктур с целью вмешательства в избирательный процесс в стране.** Спецслужбы считают, что «исходя из масштаба и изощренности таких усилий, только высокопоставленные российские чиновники могли санкционировать такую деятельность». Речь тогда шла, прежде всего, о взломах серверов Демократической партии, при этом несложно определить на фоне или в результате каких событий американская карательная машина решила взяться за «воспитание» российских официальных властей.

До этого дня Вашингтон официально обвинял в причастности к компьютерным диверсиям только власти Китая, КНДР и Ирана. А ещё в **2015 году Обама наделил сам себя правом вводить санкции против киберагрессоров.** Тогда в российском МИДе «отмели подозрения» сказав, что «доказательная база столь серьезных обвинений начисто отсутствует», «Она у Администрации США либо вообще не складывается, либо придумана теми, кто сейчас в Вашингтоне выполняет очевидный политический заказ, продолжая нагнетать беспрецедентную антироссийскую истерию».

При этом с их стороны в российское время не прекращаются поручения своим эмиссарам, в т.ч. через международные, неправительственные и общественные организации, выискивать, «перепрофилировать» вытаскивать из российских ВУЗов молодых ИТ-специалистов, подающих надежды **(б. ТАСИС поучаствовал до 2007 года в делах России и стран СНГ от имени ЕС и их заокеанских партнёров везде, где только мог, и конечно в первую очередь в энергоносителях и образовании; представители ВБРР проникают в университеты для пропаганды и сбора молодёжных проектов, в т.ч. протежируя издания в СКОПУСе; ОЭСР ежегодно (за денежное вознаграждение) запрашивает подробные доклады российских экспертов по вопросам развития отраслей российского хозяйствования, направлениям российского государственного внимания, международного сотрудничества, в т.ч. по проблематике российского СМР (содействия международному развитию) в интересах его системного ограничения; массированная работа по отбору ведётся** через молодёжные и студенческие обмены (особенно на младших курсах бакалавриата), через вторжение на сайты ВУЗов, нечистоплотных педагогов, в т.ч. стажировавшихся за рубежом, вербовочные курсы и сайты зарубежных бизнес-сообществ). И как мы понимаем, отслеживать этот вал крайне сложно, а до сей поры в залах и офисах «силиконовой долины» и довольно многих западных компаний, имеющих отношение к Сети, говорят на русском.

В августе 2016 года НАТО официально признало киберпространство потенциальным **«полем боя». Ранее к таковым альянсам относил сушу, воду, воздух и космос.** Теперь к ним добавилось пространство, созданное человеком.

Впервые виртуальная среда стала объектов стратегического планирования «за семью печатями» в США в мае 2011 г., когда была принята национальная Стратегия действий в киберпространстве, оставлявшая за **Вашингтоном право реагировать на компьютерные диверсии всеми доступными средствами, вплоть до ядерного оружия.** В декабре 2011 года со своим заявлением в ответ на американскую позицию выступила Россия – в подготовленных (открытых) Минобороны РФ **«Концептуальных взглядах на деятельность Вооруженных Сил Российской Федерации в информационном пространстве».**

При всём этом решение НАТО от августа 2016 г. можно считать самым реакционным на ближайшие 30 лет т.к. оно предусматривает распространяющийся на киберпространство (обороты, обмен и участие потребителей и пользователей постоянно растёт) **принцип коллективной обороны (5-ю статью Вашингтонского договора).** По идее это должно означать, что в случае кибератаки на одно

из государств блока, отвечать напавшему будут силы всего альянса, практически одновременно. Но нигде не сказано, при каком уровне ущерба это решение вступает в силу, при соответствии каким критериям или показателям должен вводиться этот принцип и миллионы терабайт направятся в ответ на запрос грин-карты или визы, а главное кто возьмёт на себя ответственность за последствия такого ответа НАТО, если итогом всё равно будут ядерные головки…. Не совсем понятен уровень расчётов или в США уже свободно программируют свои потери в прогнозируемых войнах?

Также нигде не оговаривается, как в НАТО намерены решать проблему атрибуции (а выявить киберагрессора со стопроцентной уверенностью довольно сложно). Т.о. **вопрос – к каким даже гипотетически представляемым последствиям приведет признание пятого измерения еще одним пространством для боестолкновения выглядит не то чтобы глупо,** но я бы сказал повисшим в воздухе надолго без ответа. А последние разногласия внутри НАТО, в т.ч. в контексте унижения Франции и Германии, как основных плательщиков в НАТО, да и в ЕС тоже, вообще, на мой взгляд, вгоняют политико-дипломатическую процедуру США в глубокое пике… А в этом случае – как быть маленьким членам НАТО, как мальтипу (собака весом около 2 кг, а стоимостью, как 1500 порций хорошего российского мороженного – к слову эта порода в Англии распространяется только через закрытые клубы, члены которых под пристальным кибервниманием МИ6) типа Эстонии.

Так многие американские и европейские эксперты до сей поры считают, что кибератака на эстонские ресурсы в 2007 г. (во время скандала с переносом памятника Советскому солдату-освободителю) стала первым примером межгосударственной кибервойны России и Эстонии. Между тем, а разве кто-то доподлинно установил, что вторжение было из России? Или может удалось доказать, что российские госструктуры напрямую причастны к атаке? Да и ущерб был, следует признать, минимальным (сайты ряда госучреждений и банков Эстонии не работали пару часов). Тем не менее, власти Эстонии тогда, не постыдясь разграбления братской могилы и обозначения памятника, как Бронзовый парень (в отдельных источниках солдат), обратились к союзникам по альянсу за помощью. Но Эстония другим членам альянса не нужна – никто не вступился, да и принцип коллективной обороны тогда не распространялся на киберпространство.

С тех пор гонка кибервооружений идет полным ходом. **Спецслужбы запада используют потенциал киберпространства для тайных операций, в том числе в отношении своих союзных государств (всем памятна «прослушка» канцлерины Меркель).** Глобальные корпорации, умелой рукой направляемые против российского потребителя, также якобы терпят огромные убытки из-за промышленного кибершпионажа русских хакеров. Приемы, якобы установленные журналистскими расследованиями заштатных изданий, как средства из арсенала русских хакеров в последнее время стали использоваться повседневно в международной политике – для выставления на показ своего негодования, что, дескать, обидели русские, а на самом деле для достижения властных полномочий, геополитических целей, что связано с финансированием из Госдепа, и для сведения счётов с оппонентами и оппозицией.

На фоне всей этой кибервакханалии все чаще звучат требования в пользу создания некоего «кодекса ответственного поведения государств в киберпространстве». При этом западные политики никогда не вспоминают о том, кто первым выступил с инициативой о предотвращении использования всемирной сети в противоправных целях. Ещё в 1998 г. Россия выдвинула такие предложения на площадке ООН. Однако до 2015 г. члены Совбеза ООН не обращали внимание на инициативу российской стороны, т.е. до принятия Группой правительственных экспертов ООН доклада, в котором впервые перечислены базовые принципы, которых должны придерживаться государства в киберпространстве. В Москве надеялись, что уже в 2017 г. Генассамблея ООН примет специальную резолюцию, в которой будут содержаться эти (и возможно дополнительные) нормы, но Америке это не нужно было. К тому же это в России резолюции ООН – значимый документ, а вот в некоторых западных странах они ни к чему не обязывают и носят рекомендательный характер.

Еще больше вопросов осталось открытыми по сей день, когда речь заходит о при-

менимости существующего международного (прежде всего гуманитарного) права к киберсреде. В 2013 г. Объединенный центр передового опыта по кибероборонe НАТО (NATO CCDCOE, создан в эстонской столице через год после истории с «Бронзовым солдатом»), опубликовал 300-страничный документ под названием «Таллинское руководство по ведению кибервойн». В нем впервые представлены алгоритмы действий государств и военных альянсов на случай масштабных кибератак. Цель документа – доказать, что существующие международные правовые нормы применимы и к киберпространству. А значит, вопреки позиции России и ряда других государств, новые законы не нужны. Это знаковое событие свидетельствует о том, что активно развивающееся с 1990-х гг. киберпространство не стало объединяющей средой и площадкой для практического сотрудничества между ведущими державами, но превратилось в еще одну арену их противостояния. И это касается в первую очередь России и её союзников.

С этим документом стоит ознакомиться, чтобы узнать, как будут выглядеть конфликты будущего из американского угла. Самый большой раздел «Руководства» посвящен кибератакам, сопровождающим традиционные вооруженные конфликты. На них, по мнению авторов документа, распространяются все нормы международного гуманитарного права, вплоть до признания участников и организаторов компьютерных диверсий комбатантами, которые могут быть пленены или физически ликвидированы.

К специфике киберпространства в документе приспособлены и многие другие правовые положения о вооруженных конфликтах. Запрещается проводить кибероперации против гражданских лиц (за исключением участников народного ополчения) и объектов, например больниц. Атаки против плотин и атомных электростанций предлагается проводить «с особой осторожностью», дабы свести к минимуму жертвы среди гражданского населения. Задействуя вредоносные программные средства для сокращения электроснабжения противника путем нарушения работы АЭС, эксперты НАТО рекомендуют особое внимание «уделить обеспечению постоянной целостности системы охлаждения» реактора.

Также подробно объясняется, в каких еще случаях можно атаковать гражданские объекты. Например, завод, производящий компьютерное оборудование или программное обеспечение по контракту с вооруженными силами неприятеля представляет собой, по мнению экспертов НАТО, «военную цель, даже если на нем выпускаются и товары гражданского назначения. А операция против SCADA-системы водохранилища может быть «задействована для спуска воды на область, в которой ожидается осуществление неприятельских военных операций, что предотвратит ее использование противником».

Непросто складывались в единый массив результаты кропотливой работы созданной в 2004 г. Группы правительственных экспертов ООН в сфере международной информационной безопасности (ее первым председателем стал представитель России – Андрей Владимирович Крутских, Спецпредставителя Президента России по вопросам международного сотрудничества в области МИБ). Преодолев терминологические и процессуальные споры, лишь в 2015 г. группа смогла добиться прорыва, представив на рассмотрение Генсека ООН доклад, который гипотетически стал основой для глобального пакта об электронном ненападении.

В соответствии договоренностями, с достигнутыми в рамках группы, государства обязуются использовать кибертехнологии «исключительно в мирных целях». Среди прочего предполагалось, **что они не будут атаковать объекты критически важной инфраструктуры друг друга** (АЭС, банки, системы управления транспортом и т.п.), перестанут вставлять вредоносные «закладки» (вредоносные коды) в производимую ими IT-продукцию, воздержатся от огульного обвинения друг друга в кибератаках и начнут прилагать усилия по борьбе с хакерами, осуществляющими компьютерные диверсии с их территории или через нее. И эта титаническая работ была проведена совершенно вовремя т.к. **на рубеже 2016–2017 годов США практически завершили подготовку к нанесению удара по России и определились со сроками возможного начала войны.** Об этом в январе 2017 года по американскому телевидению заявил известный американский специалист по современной России Стивен Коэн. **Во время**

своего выступления Коэн сказал: «...впервые в своей жизни, начиная с 1960 года, я считаю очень реальной возможность войны между Россией и Соединенными Штатами».

В своем выступлении он обвиняет администрацию США в сложившейся ситуации, говорит «о роковом повороте мировой истории» и подготовке к нанесению американцами начального удара по России с помощью третьих стран - Украины, Турции и Ближневосточных монархий, которых они активно вооружали и готовили. Большое значение в этом первоначальном ударе также придавалось и придается террористическим группировкам ИГ и Аль-Каида (обе запрещены в России). Что касается тогдашнего украинского руководства, он заявил следующее: «Это не демократический режим. ... Если США будут продолжать оказывать поддержку Киеву в таком формате, то мы очень скоро увидим начало войны с Россией».

Далее, Стив Коэн сказал: «Проблема началась еще в 90-х гг., когда администрация президента Клинтона стала считать себя победителем над СССР. Эта же позиция была занята в дальнейшем и в отношениях с Россией. РФ рассматривалась администрацией США как проигравшая сторона. Американская политика руководствовалась девизом: «Россия уступает, мы берем и требуем дальнейших уступок». Главным аспектом этой политики являлось решение считать зоной влияния США весь мир до границ с Россией, включая и бывшие страны СССР. Даже в границах СНГ и соседних государствах, США отказывали России в праве на защиту ее интересов. Украина и Грузия, страны, которые входили в состав России еще во времена, когда США не существовало, были официально признаны сферой американского влияния, откуда Россия должна была быть обязательно выдавлена».

Т.о. мы, уважаемые коллеги, понимаем насколько важен был выход на итоговый проект Концепции Конвенции ООН об обеспечении международной информационной безопасности представляется достаточно приемлемым в сложившейся ситуации и оптимальным, отвечающим ранним резолюциям Генеральной Ассамблеи ООН по данным вопросам.

Вместе с тем, следует постоянно быть на чеку по профилактике обычных мошенничеств в Сети, ввиду того, что эта категория довольно подготовленных людей в полной мере под пристальным вниманием иностранных спецслужб и их взаимоотношения «укорочены» электронным оборотом если в 1990-х хакеры были своего рода «виртуальными романтиками» и по большей части хулиганили безобидно и лишь ради забавы, то уже к началу XXI века преступники поняли, что виртуальное пространство – золотое дно, и начали зарабатывать хакерскими атаками огромные деньги, становясь мегамошенниками. Через десятилетие ряды интернет-мошенников и воров пополнила новая каста – разоблачителей. Это своего рода «робин гуды» виртуального пространства, чьи имена сейчас известны всему миру. Появились и целые группы «кибермстителей» (например, появившийся после Евромайдана в Киеве «КиберБеркут»), которые выводят на чистую воду своих врагов.

Обращает на себя внимание еще одна тенденция последнего времени. На временную службу к преступным кругам нанимаются хакеры и обворовываются промышленные предприятия и банки. Ворует зерно и уголь – вагонами, а бензин – цистернами. Более того: некоторые крупные наркодилеры исхитряются отправлять морским транспортом крупные партии наркотиков. Затем (зная, в каких именно контейнерах и какими судами они должны быть доставлены) хакеры взламывают компьютерные системы портов и делают нужные контейнеры «невидимыми» для досмотра. Борьба с этими тенденциями правоохранительных органов, по словам Касперского, особого успеха не имеет. С одной стороны, вычисление и арест киберпреступников конкретную группу хакеров «гасит», но одновременно способствует расползанию по Сети тех, кого поймать не удалось.

Ведь таких «умельцев» во Всемирной паутине – огромное множество, так что арест двух-трех и даже десяти киберпреступников (которые входили в многочисленную группу) приводит лишь к тому, что распадается именно эта конкретная группа. Другие же ее участники «шифруются» во Всемирной паутине, обучают новых хакеров и создают новые преступные группы.

Эволюция хакеров разумеется на этом не закончилась и следующим качественным дополнением рядов профессионалов информа-

ционного пространства станут представители бизнесс-промышленных кругов, имеющих доверенности на крупные финансовые вложения и обороты, предполагающие получение крупных прибылей на электронных площадках под тем или иным системным форматом. Под этим управлением хакеры будут собираться в крупные закрытые для постороннего внимания, в т.ч. по этнонациональному признаку, организовывать свои финансовые агрегации, начинать активно и открыто пропагандировать надвигающиеся катаклизмы, извлекать прибыли из социальных бедствий. Россия же по многим показателям на верхушке рейтинга стран, чьи пользователи наиболее часто подвергались киберугрозам, а из США, Англии, и теперь и из Австралии, в адрес России будут продолжать слышаться постоянные обвинения обвинения в кибервторжениях.

Когда-то генеральный директор компании Евгений Касперский предупредил общество относительно кибербезопасности не только в России, но и по всему миру: «все плохо, а будет еще хуже». Эксперты прогнозируют, что в следующем году еще больше, чем прежде, атакам будут подвергаться банки. Частные клиенты хакерам уже не интересны, ведь у них много не своруешь. Кроме того, кибермошенники, вероятно, станут «мобильнее» и адресно удалённее.

Однако Указом Президента Российской Федерации от 9 мая 2017 г. № 203 утверждена **Стратегия развития информационного общества в Российской Федерации на 2017–2030 годы.**

«20. Целью настоящей Стратегии является создание условий для формирования в Российской Федерации общества знаний.

21. Настоящая Стратегия призвана способствовать обеспечению следующих национальных интересов:

а) развитие человеческого потенциала;

б) обеспечение безопасности граждан и государства;

в) повышение роли России в мировом гуманитарном и культурном пространстве;

г) развитие свободного, устойчивого и безопасного взаимодействия граждан и организаций, органов государственной власти Российской Федерации, органов местного самоуправления;

д) повышение эффективности государственного управления, развитие экономики и социальной сферы;

е) формирование цифровой экономики.

В связи с этим следует отметить, что на нашем Форуме, помимо слов одобрения текста Концепции Конвенции ООН **об обеспечении международной информационной безопасности, было высказано довольно большое количество предложений относительно мнений российской стороны по поддержанию бесконфликтного пространства доверия и содействия развитию** в электронно-информационной сфере обращения и соцсетях в целях расширения информированности зарубежной среды о российском гостеприимстве, если с «открытой перчаткой», о национальной политике добрососедства, если к нам с «чистой лошадью и полным возом», о миролюбивом социальном участии, если «вошёл в нужду», о доверительном русском слове, если «от души».

С мыслями об этом Фонд «Росконгресс» совместно с национальным брендом «Сделано в России» разработал национальный проект, основанный, в первую очередь, на внешнеэкономическом сопровождении довольно крупной электронной площадки для представления иностранному потребителю товарно-материальных результатов российских производств, российских технологий и услуг.

КОНЦЕПЦИЯ ПРОЕКТА «СДЕЛАНО В РОССИИ»:

1. Торговый Дом «Росконгресс» – цифровой торговый дом, осуществляющий продажу и продвижение товаров и услуг на внутреннем и внешнем рынках. Зарегистрированные на платформе компании получают доступ к информационным сервисам «Сделано в России» и программе лояльности (Торговый дом и цифровая платформа);
2. Медиа-платформа для национально – ориентированного бизнеса. Платформа включает агентство деловой информации «Сделано в России» с официально зарегистрированным СМИ (www.madeinrussia.ru), распространяющим информацию на 12 языках с аудиторией более 50 000 читателей из 114;

3. Клубная платформа – Деловой клуб «Сделано в России», осуществляющая реализацию клубных проектов (обеспечение среды для поддержания контактов между предпринимателями);
- Деловой клуб (реализация клубных карт и клубных продуктов)
- Клубный журнал (реализация рекламы в журнале, размещение материалов);
- Мобильное приложение клуба;
- Клубный интернет телеканал (размещение материалов, интервью, встреч, дискуссий, рекламы).
- Церемония награждения, галерея клуба.
- Мероприятия клуба (клубные, деловые, культурные, спортивные).
- Составными элементами Делового клуба «Сделано в России» (в Московском столичном клубе в здании ЦДЛ) являются:
- Клубная гостиная Делового клуба «Сделано в России», реализованная совместно с Фондом Росконгресс, Московским столичным клубом и Росконгресс спортклубом. Программа клубной гостиной: B2B, B2G, деловые завтраки, презентации, сессии, проведение Road show, шахматная и бильярдная гостиные, сигарная комната, караоке и др.;
- Серия встреч, организация дискуссий с участниками спикеров – представителей ведущих российских компаний-экспортеров, творческих профессий, лидеров мнений для обсуждения вопросов конкурентоспособности на мировой арене;
- Гостиная губернаторов в Московском столичном клубе в ЦДЛ, по согласованию с Фондом «Росконгресс» и согласовании финансовых условий с Московским столичным клубом (продвижение брендов регионов, национальных и региональных брендов);
- Выступления спикеров и лидеров эстрады совместно Московским столичным клубом;
- Клубная спортивная программа с Росконгресс спорт клуб (спортивные мероприятия Делового клуба «Сделано в России», журнал Росконгресс спорт клуб, мобильное приложение Росконгресс спорт клуб, Галерея спортивной славы, Церемония награждения Roscongress sport Awards);
- Журнал Делового клуба «Сделано в России»;
- Мобильное приложения Делового клуба «Сделано в России»;
- Церемония награждения проекта «Сделано в России» – «Национальный Бренд»;

4. Итоговым элементом системы «Сделано в России» – является Международный форум «Национальный бренд», который способствует максимальному привлечению участников, спикеров, партнеров, спонсоров и продвижению медиа – платформы, цифровой торговой платформы, клубной платформы – Делового клуба «Сделано в России» (обеспечение среды для расширения контактов Торгового Дома «Росконгресс», освещения и продвижения инициатив Торгового Дома «Росконгресс»).

Все четыре направления являются средством продвижения Торгового Дома «Росконгресс».

Этой же Стратегией развития информационного общества в Российской Федерации на 2017–2030 годы предусмотрено, что:

«22. Обеспечение национальных интересов при развитии информационного общества осуществляется путем реализации следующих приоритетов:

а) формирование информационного пространства с учетом потребностей граждан и общества в получении качественных и достоверных сведений;

б) развитие информационной и коммуникационной инфраструктуры Российской Федерации;

в) создание и применение российских информационных и коммуникационных технологий, обеспечение их конкурентоспособности на международном уровне;

г) формирование новой технологической основы для развития экономики и социальной сферы;

д) обеспечение национальных интересов в области цифровой экономики.

23. В целях развития информационного общества государством создаются условия для формирования пространства знаний и предоставления доступа к нему, совершен-

ствования механизмов распространения знаний, их применения на практике в интересах личности, общества и государства».

Т.о. разработанный Фондом «Росконгресс» совместно с национальным брендом «Сделано в России» национальный проект в полной мере **соответствует требованиям, отвечающим интересам Российской Федерации, а также Доктрине информационной безопасности Российской Федерации,** утвержденной Указом Президента Российской Федерации от 5 декабря 2016 г. №646:

«28. Стратегической целью обеспечения информационной безопасности В области стратегической стабильности и равноправного стратегического партнерства является формирование устойчивой системы неконфликтных межгосударственных отношений в информационном пространстве».

Для заметок

Для заметок

Для заметок

СБОРНИК ДОКЛАДОВ УЧАСТНИКОВ ПЯТНАДЦАТОГО МЕЖДУНАРОДНОГО ФОРУМА «ПАРТНЕРСТВО ГОСУДАРСТВА, БИЗНЕСА И ГРАЖДАНСКОГО ОБЩЕСТВА ПРИ ОБЕСПЕЧЕНИИ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

Подписано в печать 19.11.2021. Гарнитура Helios.
Формат 60x84/8. Объем 31,16 усл. печ. л.
Тираж 200 экз.