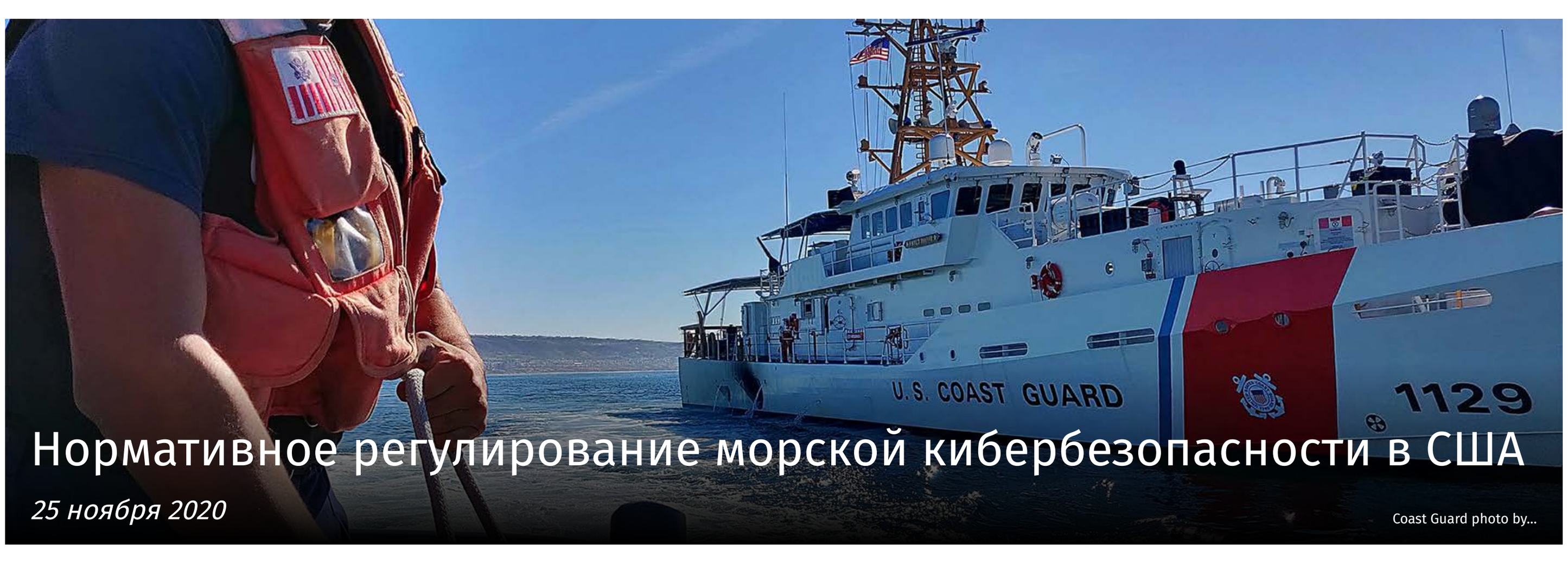


Нормативное регулирование морской кибербезопасности в США

25 ноября 2020

Coast Guard photo by...

0 919 В ридер Распечатать

Тема: Безопасность, Технологии
Регион: Северная Америка
Тип: Экспертные колонки - Киберколонка

Сергей Семенов
Начальник ФБУ «Служба морской безопасности»

КРАТКАЯ ВЕРСИЯ СТАТЬИ | **ПОЛНАЯ ВЕРСИЯ СТАТЬИ**

Ранее в экспертной колонке на сайте РСМД я обозначил важность скорейшего нормативно-правового регулирования морской кибер- и/или информационной безопасности в Российской Федерации, обратив внимание на отсутствие отраслевого регулирования в указанной сфере в нашей стране.

На этом фоне представляет интерес опыт других государств, который можно изучить и использовать в практической деятельности.

В данной статье рассмотрим опыт Соединенных Штатов Америки.

Порты в фокусе внимания

Резолюция Комитета по безопасности на море Международной морской организации (ИМО) *MSC.428(98)* «Управление морскими киберрисками в системах управления безопасностью» призывает не только обеспечить учет киберрисков в системах управления безопасностью судов после 1 января 2021 г., но и признает, что порты и портовые сооружения должны ускорить работу по защите судоходства от текущих и возникающих киберугроз и уязвимостей.

Сергей Семенов:
Морская кибербезопасность — ситуация, проблемы и риски

Необходимо отметить, что с момента принятия резолюции в 2017 г. каких-либо значимых кибератак на морские суда, приведших к серьезному ущербу, зафиксировано не было. В тоже время порты и портовые средства неоднократно подвергались масштабным по своим последствиям кибератакам.

Поэтому рассматриваемые нормативно-правовые документы США в большей степени касаются именно портов и портовых средств.

Морская кибербезопасность в повестке дня высшего руководства США

Высшее руководство Соединенных Штатов постоянно уделяет внимание растущему числу киберугроз морской отрасли страны.

Так бывший президент США Барак Обама в указе 2013 г. констатировал, что «киберпреступления в отношении критической инфраструктуры говорят о необходимости повышения уровня кибербезопасности». По его мнению, «число киберугроз критической инфраструктуре растет, что представляет собой одну из самых серьезных проблем национальной безопасности».

Четыре года спустя, 30 октября 2017 г., Комитет Палаты представителей США по национальной безопасности провел полевые слушания, посвященные изучению физической безопасности и кибербезопасности портов США. Председатель Комитета Майкл МакКол во время слушаний заявил: «К сожалению, противники Америки постоянно ищут способы нанести удар по нашей стране с помощью кибератак. Поскольку наши портовые системы все больше выигрывают от новых технологий и передовых компьютерных систем, они также оказываются в перекрестье прицела международных хакеров и хакеров государств-изгоев. В июне порт (порт «Лос-Анджелес» — прим. автора) был ненадолго закрыт из-за кибератаки, которая обошлась почти в 300 млн долларов экономического ущерба. Это неприемлемо. Мы должны сделать больше для укрепления кибербезопасности этих важнейших морских узлов». Также он объявил, что Конгресс принял закон, обязывающий министра внутренней безопасности внедрить модель оценки рисков в американских портах, которая сфокусировалась бы на уязвимостях и рисках кибербезопасности.

В июне текущего года сенатор Эдвард Марки, член коммерческого подкомитета по безопасности внес законопроект Об усилении морской кибербезопасности на море. Законопроект предписывает Морской администрации США взаимодействовать с Береговой охраной и Министерством внутренней безопасности для обеспечения ресурсами, которые могут помочь морским операторам (к их числу законопроект помимо прочего относит собственников и операторов портовых терминалов — прим. автора) идентифицировать, защищать, реагировать и восстанавливаться после киберинцидентов.

«По мере того, как морской сектор все активнее использует технологии, связанные с Интернетом (электронные карты и виртуальные средства навигации) угроза кибератак продолжает расти, — сказал сенатор Марки. — Морским транспортом перевозится подавляющее большинство грузов в рамках внешней торговли США, и он может быть особенно привлекательной мишенью для киберпреступников. Мой законопроект направлен на активное противодействие этой угрозе путем укрепления морской кибербезопасности и совершенствования координации между соответствующими федеральными ведомствами».

Мнения высшего морского руководства США

Высокопоставленные морские чиновники США полностью согласны с законодателями и считают, что портовые сооружения остаются уязвимыми и недостаточно неподготовленными к киберугрозам.

Так, командующий Береговой охраной США адмирал Карл Л. Шульц в уведомлении Федерального регистра от марта 2020 г. определяет кибербезопасность как «один из самых серьезных вызовов экономической и национальной безопасности в морской отрасли».

Совсем недавно, в сентябре 2020 г., во время вебинара по безопасности на море, руководитель Морской администрации США контр-адмирал Марк Х. Бузби отметил: «За последние несколько лет стало совершенно очевидно, что необходимо сфокусироваться на морской кибербезопасности… [морская кибербезопасность] как очень неприятная и растущая проблема действительно нуждается в стратегическом подходе. Решение проблемы обеспечения морской кибербезопасности абсолютно жизненно важно не только для нашей экономической безопасности, но и для национальной безопасности в целом».

Киберстратегия Береговой охраны США

В июне 2015 г. Береговая охрана США приняла Киберстратегию, в которой она констатирует, что кибербезопасность — это одна из самых серьезных проблем экономической и национальной безопасности США. Правительственные системы, включая системы Береговой охраны, сталкиваются с растущим массивом возникающих киберугроз, которые могут серьезно скомпрометировать и ограничить способность службы выполнять основные задачи. Данные угрозы создают значительные риски для национальной морской транспортной системы (МТС) и критической инфраструктуры. Имея около 360 морских и речных портов, которые обрабатывают грузы на сумму более 1,3 трлн долл. в год, США критически зависят от безопасной, надежной и эффективной МТС. Чтобы справиться с огромным количеством проблем в цифровую эпоху, американская Береговая охрана, прежде всего, должна полностью охватить киберпространство как оперативную область.

Доля киберрисков в общем объеме уязвимостей, с которыми сталкивается МТС, постоянно растет. Операторы судов и объектов используют компьютеры и киберзависимые технологии для навигации, связи, проектирования, перевозки грузов, балласта, обеспечения безопасности, экологического контроля и многих других целей. Эти киберсистемы как создают преимущества, так и увеличивают риски. Три четверти национальной торговли США проходит через порты и водные пути, поэтому даже временное прекращение деятельности МТС может иметь серьезные последствия для местной, региональной, национальной и даже глобальной экономики.

Для устранения этих рисков Береговая охрана США, морская отрасль и другие заинтересованные стороны будут работать над определением соответствующих киберстандартов и включением их в существующие мероприятия по обеспечению безопасности судов и объектов.

Владимир Васильев:
Автономный рейс: перспективы использования судов без экипажей

Совершенствование законодательства в области морской безопасности

В октябре 2018 г. в США принят Закон о совершенствовании морской безопасности (*MSIA*). Законом дополнены действующие акты о морской безопасности в части обеспечения морской кибербезопасности. Уточнены компетенции субъектов, задействованных в ее обеспечении, введена обязанность проведения анализа киберугроз в рамках оценки охраны судна или портового средства. План охраны судна или портового средства должен быть дополнен положениями, касающимися обнаружения киберугроз, которые могут привести к инцидентам транспортной безопасности, реагирования на них и восстановления после них.

Необходимо отметить, что за нарушение данных требований предусмотрен гражданский штраф в размере не более 25 тыс. долл. за каждый день, в течение которого продолжается нарушение. Однако при этом максимальная сумма не должна превышать 50 тыс. долл.

Нормотворчество Береговой охраны США

1. Кибербезопасность портовых средств США

В марте 2020 г. Береговая охрана США выпустила циркуляр NVIC 01-20 Руководящие принципы в отношении киберугроз объектам, регулируемым Законом о безопасности морского транспорта (*MTSA*) 2002 года — *Guidelines for Addressing Cyber Risks at Maritime Transportation Security Act (MTSA) Regulated Facilities*.

Данный циркуляр содержит рекомендации владельцам и операторам портовых средств по соблюдению требований оценки, документирования и устранения уязвимостей компьютерных систем или сетей. В соответствии с частями 105 и 106 раздела 33 Кодекса федеральных нормативных актов (*CFR*), которые реализуют Закон о безопасности морского транспорта (*MTSA*) 2002 г., регулируемые им объекты (включая объекты на внешнем континентальном шельфе) обязаны оценивать и документировать уязвимости, связанные с их компьютерными системами и сетями, в рамках Оценки охраны объектов (*FSA*). Выявленные уязвимости должны быть учтены в соответствующих разделах Плана охраны объекта (*FSP*) в соответствии с частями 105.400 и 106.400 раздела 33 *CFR*. Указанные части содержат общие требования к кибербезопасности объектов, позволяя их владельцам и операторам по своему усмотрению определять детали того, как они будут соблюдать их требования. Эти правила также наделяют Береговую охрану полномочиями проверять их соответствие требованиям и утверждать *FSA* и *FSP*. Таким образом, владельцы и операторы несут ответственность за оценку киберуязвимостей и обеспечение кибербезопасности своих объектов под надзором и руководством Береговой охраны.

Хотя правила *MTSA* являются обязательными для владельцев объектов и операторов, настоящий циркуляр не содержит каких-либо обязательных положений. Он представляет собой добровольное руководство, предназначенное для оказания помощи владельцам и операторам объектов, регулируемых *MTSA*, в понимании и соблюдении обязательных правил. Они имеют право по своему усмотрению определять, как лучше всего выявлять, оценивать и устранять уязвимости компьютерных систем и сетей своих объектов.

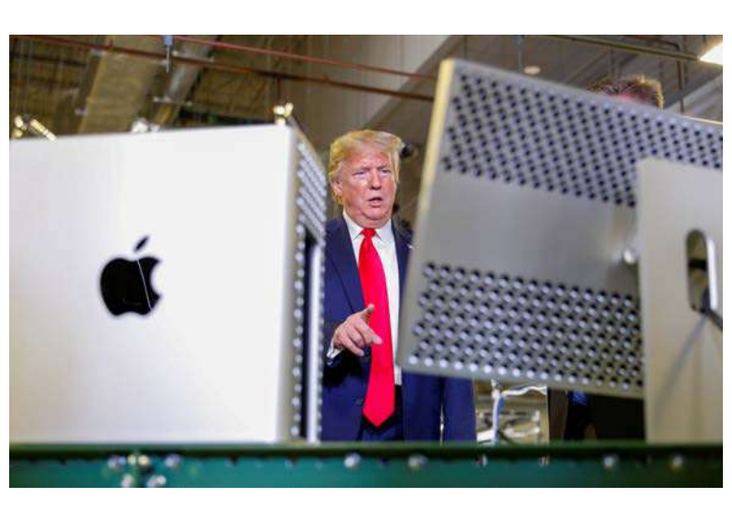
Несмотря на то, что данный циркуляр вносит определенную ясность в вопрос обеспечения морской кибербезопасности, в США он является объектом критики.

Прежде всего, циркуляр не вносит никаких изменений в действующее в США законодательство, а представляет собой новое толкование ранее принятых норм в области обеспечения морской безопасности.

Так, с точки зрения Береговой охраны положение части 105 раздела 33 *CFR* о необходимости учитывать «меры по защите радио- и телекоммуникационного оборудования, включая компьютерные системы и сети» является основанием для оценки и учета киберрисков. Хотя указанная часть никаких требований в области кибербезопасности не содержит.

Буквальное прочтение правил части 105 говорит о том, что ее требования распространяются на компьютерные системы и сети, используемые только для радио- и телекоммуникации. То есть можно обоснованно заключить, что лицо, ответственное за охрану, должно оценивать уязвимости только в киберсистемах, используемых для связи, исключая киберсистемы, используемые в других критических *IT* и ОТ (*Operational Technology*) системах морских объектов.

Согласно циркуляру, хотя лицо, ответственное за охрану, должно оценивать и устранять уязвимости кибербезопасности, субъект имеет право по своему усмотрению решать, как он выявляет, оценивает и устраняет эти уязвимости. Учитывая это, можно констатировать, что, по существу, отсутствует нормативная база, которая служила бы основой для единообразного правоприменения. Также, по сути, циркуляр требует, чтобы оценка и устранение киберугроз морских объектов осуществлялись с момента принятия части 105, то есть с 2003 года.



Анастасия Толстухина:
«Коллективная кибероборона» по-американски

Циркуляр не устанавливает никаких явных требований. Нет никаких уникальных кибертребований, связанных с обязанностями персонала (например, обязанностями *IT* или *OT* персонала по обеспечению кибербезопасности), не существует четких требований к кибербучению или киберзнаниям (например, требования к лицам, ответственным за охрану, быть знакомым с *IT* и ОТ терминологией или пройти базовый курс компьютерной гигиены). Отсутствуют конкретные правила, связанные с кибертренировками и киберучениями. В отличие от систем, используемых для обеспечения физической безопасности морских объектов, в настоящее время нет специальных требований к техническому обслуживанию или тестированию *IT* или *OT* систем в целях кибербезопасности.

Но самая главная проблема обеспечения морской кибербезопасности заключается в том, что в отличие от четкого управления компонентами, лежащими в основе физической безопасности (например, контроль доступа, запретные зоны, досмотр персонала), в части 105 ничего не говорится о компонентах программ кибербезопасности.

По мнению капитана 2 ранга Береговой охраны США Майкла С. Петта, заместителя директора по морским операциям и профессора Стоктонского центра международного права при Военно-морском колледже США, Береговая охрана США могла бы использовать внутренний процесс нормотворчества для внедрения четкого, единообразного и более строгого режима кибербезопасности.

2. Кибербезопасность и портовый контроль США

Управление Береговой охраны США 27 октября 2020 г. выпустило рабочую инструкцию *CVC-WI-027* «Управление киберрисками судов», которая содержит руководство для морских инспекторов Береговой охраны (MI) и должностных лиц Государственного Портового Контроля (*PSCO*) по оценке кибергигиены на борту судов, а также варианты действий при обнаружении недостатков.

В ходе инспекции/освидетельствования судна, подпадающего под действие Международного кодекса управления безопасностью (МКУБ) *MI PSCO* должен оценить, является ли событие кибербезопасности фактором отказа системы, необходимой для безопасного плавания или эксплуатации судна. В качестве примера в руководстве приведен отказ электронной картографической навигационно-информационной системы (ЭКНИС), возможно, вследствие плохой кибергигиены на судне. По мнению авторов руководства, в данном случае не выполняется правило *V/27* Конвенции СОЛАС, которое требует, чтобы все морские карты, необходимые для предполагаемого рейса, были адекватными и актуальными. Приводимая в качестве примера гипотетическая ситуация, по мнению Береговой охраны, содержит четкие основания для проведения более детальной проверки судна и его системы управления безопасностью (СУБ), в том числе в части, касающейся управления кибербезопасностью.

Иностранное судно может быть задержано в случае выявления объективных доказательств того, что оно не выполнило предусмотренные СУБ меры по обеспечению кибербезопасности (если управление киберрисками не было включено в СУБ судна до первой ежегодной проверки документа компании о соответствии после 1 января 2021 г., или если объективные доказательства указывают на наличие серьезного сбоя в реализации СУБ по обеспечению кибербезопасности, который привел к инциденту, влияющему на работу судна).

В иных случаях *PSCO* должен зафиксировать ошибки в эксплуатации недостаток и нарушение требований МКУБ и потребовать от судна исправить его до отправления, а также провести внутренний аудит обеспечения кибербезопасности в течение 3 месяцев или до возвращения в порт США после плавания за границу.

Можно констатировать, что критерии проверки вопросов обеспечения кибербезопасности судна крайне размытые. Вероятно, выводы по каждой проверке будут зависеть от субъективного взгляда конкретного инспектора.

В завершение мне хотелось бы отметить, что законодательство США, регулирующее вопросы морской кибербезопасности, не ограничивается исключительно приведенными в статье документами. При этом, надеюсь, что мне удалось показать, какое серьезное внимание уделяется в США вопросам защиты судов, портов и портовых средств от киберугроз. Показанные в статье положительные примеры и проблемные зоны нормативно-правового регулирования морской кибербезопасности в США можно использовать при определении российского отраслевого подхода к обеспечению кибербезопасности морского транспорта.

СЛЕДИТЬ ЗА СОБЫТИЯМИ

Проект
Международное измерение информационной безопасности

Автономный рейс: перспективы использования судов без экипажей
Автономизация морских перевозок в ближайшее время возможна только в пределах территориальных морей и внутренних вод прибрежных государств

Бизнесу тоже нужен киберкодекс
Обзор бизнес-инициатив по формированию правил ответственного поведения в цифровом пространстве

«Коллективная кибероборона» по-американски
Комиссия по киберпространству предполагает реконфигурацию государственно-частного партнерства в вопросах кибербезопасности

Морская кибербезопасность — ситуация, проблемы и риски
У российских судов в иностранных портах могут возникнуть риски санкций за невыполнение рекомендаций Международной морской организации по кибербезопасности

Кибербезопасность, Флот, Кибератаки, Морская кибербезопасность, Транспорт

Выбор читателей Скрыть
Сделать Америку снова нормальной?
Отношения России и США на перепутье
Сирийский Идлиб: что дальше?
Как молоды мы были...
Саммит АТЭС: тяжелая неделя для США и для Трампа

Возврат к списку

Издания РСМД
Политика санкций: цели, стратегии, инструменты
Армии и безопасность на Ближнем Востоке и в Северной Африке
Глобальный прогноз РСМД 2019–2024

Теги
Арктика АТР Безопасность Ближний Восток Великобритания Выборы Германия Дональд Трамп ЕАЭС Европа Европейский союз Запад Индия Иран Китай Миграция НАТО Образование ООН Россия Санкции Сирия США Турция Украина Украинский кризис Франция Экономика Ядерное оружие Япония

Полезные материалы
Справочник экспертов и организаций — «Международные исследования в России»
Статистика и индексы — Статистические данные по международной проблематике
Базы данных — Электронные журналы и библиотеки

Библиотека
Сталин и судьба Финляндии — Киммо Рентола
Экономический рост в странах Востока: тенденции, неравномерность, неравенство социального развития — Ирина Дерюгина, Александр Филоник, Гурген Гукасян, Иван Бочаров, Наталья Замараева
Теория метафоры и политические институты — Кирилл Коктыш

ТВИТТЕР FACEBOOK ВКОНТАКТЕ
Твиты от @Russian_Council
Russian Council @Russian_Council
RIAC & @ispionline presents joint report "After the Storm: Post-Pandemic Trends in the Southern Mediterranean". Authors: Andrey Kortunov, @paolo_magri, @Ruslan_CL, @Ivonbocharov, @emmevilla, @ElenaCorradi, @ChiaraLovotti, Andrey Chuprygin, @InesAbdelrazek russiancouncil.ru/en/activity/pu…
After the Storm: Post-Pandemic Trends in t…
RIAC and ISPI Joint Report This Report bring…
Встроить Показать в Твиттере

О СОВЕТЕ ЧЛЕНЫ РСМД ЭКСПЕРТЫ НОВОСТИ АНАЛИТИКА И КОММЕНТАРИИ ПУБЛИКАЦИИ БИБЛИОТЕКА ТЕМЫ РЕГИОНЫ ПРОЕКТЫ ДЛЯ СМИ БЛОГИ СЮЖЕТЫ