Специальное издание Connections

Connections
Ежеквартальный журнал

Последствия концепции устойчивости для безопасности

Редакторы: Филипп Флури,
Тодор Тагарев

Консорциум «Партнерство ради мира» военных академий и институтов по изучению вопросов безопасности

Осень 2020

Консорциум „Партнерство ради мира" военных академий и институтов по изучению вопросов безопасности

Это издание осуществляется при поддержке Правительства Соединенных Штатов. С изданиями Консорциума можно бесплатно ознакомиться на сайте http://connections-qj.org. Если Вы желаете заказать экземпляр журнала для Вашей библиотеки или если у Вас есть вопросы, связанные с публикациями этой серии, Вы можете обратиться в Оперативный отдел ПРМ по электронной почте: PfPCpublications2@marshallcenter.org.

ISSN 1812-1101, e-ISSN 1812-2973

CONNECTIONS

THE QUARTERLY JOURNAL

том 19, № 4, осень 2020

Консорциум оборонных академий и институтов по изучению безопасности в рамках программы «ПрМ»

Connections: The Quarterly Journal
ISSN 1812-1101, e-ISSN 1812-2973

https://doi.org/10.11610/Connections.rus.19.4

Содержание

Том 19, № 4, осень 2020

Рецензированные статьи

Connections: The Quarterly Journal
ISSN 1812-1101, e-ISSN 1812-2973

Георги Шарков, *Connections QJ* 19, № 4 (2020): 5-28
https://doi.org/10.11610/Connections.rus.19.4.01

Рецензированная статья

Оценка зрелости национальной кибербезопасности и устойчивости

Георги Шарков

Министерство обороны, Республика Болгария, https://mod.bg/

Европейский институт программного обеспечения – Восточной Европы, София, Болгария, https://esicenter.bg/

Резюме: В этой статье представлен обзор уровней зрелости и методологий оценки кибербезопасности и устойчивости с точки зрения их применимости и полезности на секторном и национальном уровнях. Сравниваются и анализируются эталонные модели зрелости и рамки для оценки, такие как Модель менеджмента устойчивости CERT, Модель зрелости способностей для обеспечения кибербезопасности для стран, C2M2 (Модель зрелости способностей для обеспечения кибербезопасности), на предмет их применимости при разработке и реализации национальных стратегий и программ кибербезопасности для достижения киберустойчивости. Дано описание также показателей кибер-готовности с точки зрения их использования для идентификации возможных улучшений. Автор исследует развитие национальных стратегий кибербезопасности с акцентом на киберзрелость и приводит примеры. Также описан подход, основанный на зрелости, для болгарской дорожной карты киберустойчивости в контексте развивающихся гибридных угроз, связанных с кибердоменом, и потребность в институциональной совместной государственно-частной устойчивости.

Ключевые слова: киберустойчивость, модели зрелости способностей, оценка зрелости кибербезопасности, показатели зрелости, гибридная устойчивость.

Введение

Современные цифровые общества и экономики глобально взаимосвязаны и становятся все более взаимозависимыми в результате глобальной цифровой связи и зависимости от цифровой инфраструктуры, цифровых коммуникаций и цифровых систем. Анализ этих взаимозависимостей и возникающих сложных уязвимостей и угроз требует целостного подхода, который выходит далеко за рамки личных, корпоративных или секторальных мер кибербезопасности. Повышение кибербезопасности и защита критически важных инфраструктур требует скоординированных усилий на национальном, региональном и международном уровнях. Кроме того, из-за многоуровневой «кибертерритории» (термин, введенный Министерством обороны США, МО, и подробно описанный Шоном Райли [1]) и сложной системной взаимозависимости, новые риски и угрозы становятся «неизвестными неизвестными» и требуют модернизации устоявшихся веками принципов устойчивости общества до совершенно нового уровня зрелости «киберустойчивости».

Достижение кибербезопасности и устойчивости на национальном уровне – общая ответственность всех заинтересованных сторон: правительства, частного сектора и гражданского общества. Для разработки и реализации национальных стратегий и планов по кибербезопасности требуются скоординированные действия и скоординированный подход с участием многих заинтересованных сторон. Различные методологии, руководящие принципы и рамки для определения хорошо структурированных и всеобъемлющих национальных или секторальных стратегий кибербезопасности предоставляются всемирными организациями, такими как МТС, ОЭСР, АКБ ЕС (ENISA), ОБСЕ, органами по стандартизации и академическими исследованиями. Большинство из них уже постулировали «киберустойчивость» как новую главную цель повышения «кибербезопасности». Стратегии также находят отражение в дорожных картах, в которых излагаются шаги и цели, которых необходимо достичь на различных этапах планов улучшений. Проблема состоит в том, как оценить уровень достижений, эффективность и действенность мер, и в более общем плане, как оценить общий уровень готовности, потенциала и объективно оценить способности для обеспечения безопасности и устойчивости на секторальном и национальном уровне. Также существует потребность в единой методологии для мониторинга прогресса и сравнения достигнутого статуса между организациями, секторами, странами и обществами.

На протяжении десятилетий подход, основанный на моделях зрелости, широко использовался в ИТ-компаниях и технологических секторах, а также в государственных закупках, начиная с обороны, для оценки готовности и

[1] Shawn Riley, “Cyber Terrain: A Model for Increased Understanding of Cyber Activity,” 2014, accessed September 15, 2020, https://www.linkedin.com/pulse/20141007190806-36149934--cyber-terrain-a-model-for-increased-understanding-of-cyber-activity/.

способности организаций предоставлять высококачественные продукты и услуги в рамках требуемого объема, времени и бюджета. С другой стороны, организации, сообщества и страны должны жить и соблюдать постоянно увеличивающееся количество правил, стандартов и требований, таких как Рамка по кибербезопасности NIST[2] и соответствующие стандарты NIST и правила ЕС, например, «Закон о кибербезопасности»[3] с ожидаемой схемой сертификации кибербезопасности, «Директива NIS»[4] и другие. Чтобы справиться со всем этим и в то же время достигать конкретных бизнес-целей организации, модели и методы оценки зрелости оказались наиболее действенным и эффективным способом для больших и малых организаций.[5]

В этом обзоре мы охватываем несколько наиболее популярных примеров огромного разнообразия моделей зрелости кибербезопасности и даем краткий анализ их пригодности для применения на более высоком уровне для целей оценки зрелости кибербезопасности сообщества, сектора или страны, и для обеспечения национальных стратегий кибербезопасности хорошо структурированными программами улучшения, такими как «дорожная карта до зрелости».

Модели зрелости и цифровое общество

Происхождение и типы моделей зрелости

Концепция моделей зрелости для индустрии программного обеспечения/ИКТ была первоначально спонсирована военными США, которые хотели разработать метод объективной оценки способностей и зрелости процессов субподрядчиков по программному обеспечению/ИКТ.[6] Из-за различных появляющихся технологий, стандартов, различных размеров и возможностей поставщиков возникла необходимость в объективной единообразной оценке уровня надежности, доверия и рисков, связанных с качеством услуг

---

2 "Cybersecurity Framework," ver. 1.1., 2018, NIST, USA, по состоянию на 10 октября 2020, https://www.nist.gov/cyberframework.

3 "EU Cybersecurity Act," Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019, https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-act.

4 "The Directive on Security of Network and Information Systems (NIS Directive)," Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016, ongoing consultations for update in 2021, https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive.

5 Doug Hudson, Jason Macallister, and Mandy Pote, "A Guide to Assessing Security Maturity," White paper, Carbon Black, 2019, по состоянию на 15 сентября 2020, https://www.carbonblack.com/resources/a-guide-to-assessing-security-maturity/.

6 Richard Caralli, Mark Knight, and Austin Montgomery, "Maturity Models 101: A Primer for Applying Maturity Models to Smart Grid Security, Resilience, and Interoperability," White paper (Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2012), https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=58916.

по программному обеспечению/ИКТ. Модели зрелости также предусматривают измеримый переход между разными уровнями (или шагами, стадиями). Они позволяют сравнивать организации по их «уровням зрелости» и обеспечивают структурированный и дающий приоритеты подход к планам улучшений.

Модели зрелости можно разделить на три типа:

- *Модели прогресса зрелости,* часто иллюстрируемые «путешествием», представляют собой простую прогрессию или масштабирование определенного атрибута, характеристики, индикатора, паттерна, где движение вверх по уровням зрелости указывает на прогрессирование в зрелости соответствующего атрибута. Уровни описывают следующие «более высокие состояния» достижений, продвижения или «шагов» в эволюции и обеспечивают четкую дорожную карту преобразований. Однако, на практике они не измеряют ни зрелость процесса, ни способности;
- *Модели зрелости способностей (CMM):* оцениваемые параметры представляют возможности организации по набору характеристик, показателей или шаблонов, часто выражаемых как «практики». Их обычно называют «моделями процессов». Типичные уровни моделей CMM названы в зависимости от зрелости процессов, например:

  ад-хок → управляемый → определенный → количественно управляемый → оптимизированный

- *Гибридные модели зрелости* сочетают в себе характеристики моделей прогресса с атрибутами способностей из моделей зрелости способностей и отражают переходы между уровнями, связанными со зрелостью способностей, при этом используя архитектуру атрибутов, индикаторов и паттернов модели развития. Они относительно просты в использовании и понимании, особенно в конкретных предметных областях.

Модели зрелости, независимо от их типа, имеют аналогичную структуру, которая обеспечивает согласованную связь между целями, передовым опытом и оценками, а также облегчает определение дорожных карт улучшений между текущими и целевыми способностями в контексте бизнес-целей, стандартов и специфичных для предметной области характеристик. Типичная структура включает:

- *Уровни зрелости:* представляют собой переходные состояния (также этапы); в гибридном подходе они также могут быть картографированы как «уровни способностей»;
- *Домен модели:* группы атрибутов и деятельностей в областях, обычно называемых «областями процесса»;

- *Атрибуты:* основное содержание модели, сгруппированное по областям и уровню, на основе практики, предписаний, знаний, стандартов;
- *Методы оценки:* унифицированные оценки, позволяющие получать сопоставимые и содержательные баллы (больше, чем просто чекбоксы). Основное использование – объективная оценка соответствия модели, предоставление измеримых показателей достижений и прогресса, а не сравнение организаций. Оценка может быть официальной (под руководством экспертов) и неофициальной (включая самооценку);
- *Планы улучшений (дорожные карты):* методы оценки обеспечивают оценку текущего состояния, анализ пробелов в достижении целевого уровня, определение объема и приоритетов улучшения, планирование улучшений и проверку результатов (достижение следующего или поддержание текущего уровня).

Модели зрелости для цифрового общества и цифровой экономики

Внедрение и раннее использование моделей зрелости произошло в индустрии программного обеспечения и информационных технологий. После первого использования модели поэтапной зрелости Ричардом Л. Ноланом в 1973 году и следующей работы Уоттса Хамфри, первоначально в IBM, а после 1986 года в Институте программной инженерии (SEI), Университета Карнеги-Меллона (CMU), Департамент обороны США запросил у SEI формализованную структуру зрелости процессов, чтобы иметь возможность оценивать подрядчиков по программному обеспечению. В начале 1990-х годов SEI представила формализованную модель зрелости способностей (CMM) с пятью уровнями зрелости. Впоследствии, в 2002 году, была опубликована гораздо более полная и интегрированная модель, интеграция моделей зрелости способностей (CMMI) с самой популярной версией 1.3 2010 года. Она применяется к разработке программного обеспечения, системной инженерии, приобретению программного обеспечения и систем, а также при предоставлении обслуживания в качестве разных приложений с общим ядром. CMMI в дальнейшем перешла в ведение Института CMMI (дочерняя компания CMU), которая была приобретена в 2016 году ISACA. Новая версия 2.0 была выпущена в 2018 году. CMMI определяет пять уровней зрелости, которые отражают зрелость установленных и институционализированных процессов:

Начальный -> Управляемый -> Определенный -> Количественно управляемый -> Оптимизированный

С тех пор модели зрелости способностей были широко внедрены в таких областях, как инфраструктура ИКТ, все виды разработки программного обеспечения, управление услугами, управление бизнес-процессами, произ-

водство, гражданское строительство и кибербезопасность. В 2018 году Институт CMMI опубликовал «Платформу киберзрелости CMMI» для проведения оценок киберустойчивости.

Модели зрелости способностей для кибербезопасности и киберустойчивости

В течение последнего десятилетия было предложено несколько рамок для кибербезопасности и устойчивости. Недавнее исследование [7] выявило более 25 исследовательских мероприятий в 36 различных секторах, направленных на достижение большей ясности в отношении объема, характеристик, синергии и пробелов, которая будет способствовать продвижению научных исследований в этой области. Техническая карта 2017 года, сравнивающая модели зрелости, используемые в различных секторах, включая образование и осведомленность, стала еще одним источником для нашего исследования.[8] В исследовании рамки классифицируются как стратегические или оперативные, в зависимости от иерархии их влияния на решения, рассматриваемых атак, используемых методов и области реализации. Чтобы определить популярность этих терминов, мы провели простой поиск в Google Scholar, который дал более 10 000 результатов для «модели зрелости кибербезопасности» и около 12 000 результатов для «оценки зрелости киберустойчивости». Для нашего опроса мы выбрали несколько рамок, определенных в предыдущем исследовании, и добавили более новые работы, поскольку мы стремимся определить применимость на более высоком, чем организационный уровень (например, секторы, сообщества, страны), схожесть результатов оценки и возможности для междисциплинарного, межотраслевого и трансграничного применения. В подразделах ниже мы комментируем некоторые популярные показатели кибербезопасности.

Модель управления устойчивостью CERT (CERT-RMM)

CERT-RMM стала эталонной моделью для киберустойчивости, разработанной отделом CERT SEI Университета Карнеги-Меллона. Она оказала сильное влияние на большинство современных методов и рамок оценки зрелости кибербезопасности. Хотя это явно не указано в названии, модель предна-

[7] Daniel A. Sepúlveda Estay, Rishikesh Sahay, Michael B. Barfod, and Christian D. Jensen, "A Systematic Review of Cyber-resilience Assessment Frameworks," *Computers & Security* 97 (2020), 101996, https://doi.org/10.1016/j.cose.2020.101996.

[8] Angel Marcelo Rea-Guaman, Tomás San Feliu, Jose A. Calvo-Manzano, and Isaac Daniel Sanchez-Garcia, "Comparative Study of Cybersecurity Capability Maturity Models," in *Software Process Improvement and Capability Determination,* ed. Antonia Mas, Antoni Mesquida, Rory V. O'Connor, Terry Rout, and Alec Dorling (Cham, Switzerland: Springer, 2017), 100-113, https://doi.org/10.1007/978-3-319-67383-7_8.

значена для достижения операционной устойчивости организаций в цифровом обществе и цифровой экономике, то есть того, что мы в настоящее время подразумеваем под *киберустойчивостью*. Стабильная версия 1.1 модели была опубликована в 2011 году,[9] с обновлением до последней опубликованной версии 1.2 в 2016 году.[10] Модель основана на методе «Оценитель оперативно критических угроз, активов и уязвимостей» (OCTAVE) для управления рисками информационной безопасности и на опыте применения в финансовом и других секторах. Аспекты управления киберрисками были объединены с процессно-ориентированным подходом и общей таксономией, связанной с CMMI, с такими терминами, как «области процесса» и общими целями и методами, введенными вместе с картированием областей инжиниринга, предоставления услуг и непрерывности процессов из CMMI для услуг и разработок.

Модель определяет следующие 26 областей процессов, сгруппированных в 4 категории:

- *Категория «Управление предприятием»*: Коммуникации; Соответствие; Фокус предприятия; Управление финансовыми ресурсами; Управление человеческими ресурсами; Организационное обучение и осведомленность; Управление рисками;
- *Категория «Операционный менеджмент»*: Управление доступом; Экологический контроль; Управление внешними зависимостями; Управление идентичностью; Управление инцидентами и контроль; Управление знаниями и информацией; Управление персоналом; Управление технологиями; Анализ и разрешение уязвимостей;
- *Категория «Инжиниринг»*: определение активов и управление ими; Управление мерами защиты; Разработка требований к устойчивости; Управление требованиями к устойчивости; Разработка технических решений для обеспечения устойчивости; Непрерывность обслуживания;
- *Категория «Управление процессами»*: Измерение и анализ; Мониторинг; Развитие организационных процессов; Фокус организационного процесса.

«Стратегия устойчивости» основана на достижении устойчивости четырех основных активов: *людей, информации, технологий и сооружений*. Таким образом, «устойчивость» «переводится» в действия, которые будут защищать и поддерживать меры в отношении активов. Структура модели соответствует классической архитектуре CMMI. Для каждой из 26 областей

---

[9] Richard A. Caralli, Julia H. Allen, and David W. White, *CERT Resilience Management Model: A Maturity Model for Managing Operational Resilience*, CERT-RMM Version 1.1 (Boston, MA: Addison-Wesley, 2011).

[10] Richard A. Caralli, Julia H. Allen, David W. White, Lisa R. Young, Nader Mehravari, and Pamela D. Curtis, "CERT Resilience Management Model. Version 1.2," Technical Report, Carnegie Mellon University, 2016, https://resources.sei.cmu.edu/library/asset-view.cfm?assetID=514489.

процессов определен набор конкретных целей (всего 94), которые должны быть достигнуты путем внедрения конкретных практик (251, обычно с несколькими вспомогательными практиками), модель предписывает использование трех общих целей и 13 общих практик для измерения уровня зрелости. Для облегчения оценки впоследствии были введены более детализированные уровни показателей зрелости (MIL). Сопоставление уровней способностей с уровнями показателей зрелости показано ниже:

- *Уровень способностей 0: незавершенный* - MIL0: незавершенный;
- *Уровень способностей 1: выполненный* - MIL1: выполненный;
- *Уровень способностей 2: управляемый* - MIL2: запланированный; MIL3: управляемый; MIL4: измеряемый;
- *Уровень способностей 3: Определенный* - MIL5: Определенный и новый MIL6: Общий (рассматривает зрелость для целостного улучшения сообщества).

Модель зрелости способностей для кибербезопасности (C2M2) для критически важных инфраструктур

Модель зрелости способностей для кибербезопасности (C2M2) [11] была введена в 2014 году Министерством энергетики (МЭ США) в качестве обновления более ранней версии C2M2 для подсектора электроэнергетики (ES-C2M2) путем удаления ссылок по конкретным секторам и их преобразования в более широко применимые к критическим инфраструктурам. Ее поддержала инициатива Белого дома, возглавляемая Министерством энергетики, Министерством внутренней безопасности (DHS) и SEI, CMU. C2M2 состоит из 10 доменов (перечисленных в таблице 1) и набора практик для каждого домена, которые представляют способность в данном домене. Практики сгруппированы по целям и упорядочены по четырем уровням показателей зрелости (от MIL0 до MIL3).

«Цели» разделены два типа: *цели подхода* (одна или несколько для каждой области, уникальные для областей), поддерживаемые последовательностью конкретных практик, и *цели управления* (по одной для каждой области), поддерживаемые последовательностью «общих» практик, описывающие институциональную деятельность. Прогресс измеряется набором практик, характеризующих *уровни показателей зрелости*, применяемых для оценки подхода к прогрессу и оценки прогресса институционализации. Как и в моделях CMMI и CERT-RMM, MIL являются «кумулятивными». Модель сопоставлена с большинством известных моделей и рамок в области информационной безопасности и кибербезопасности, таких как ISO/IEC 27001/2, структуры NIST по кибербезопасности, критическим инфраструктурам, цепочкам поставок. Примечательно, что все 10 доменов с целями и

[11] Cybersecurity Capability Maturity Model (C2M2) Program, US Department of Energy, по состоянию на 30 сентября 2020, www.energy.gov/ceser/activities/cybersecurity-critical-energy-infrastructure/energy-sector-cybersecurity-0.

практиками соответствуют подмножеству CERT-RMM.[12] В настоящее время обсуждается новая версия 2.0.[13]

Таблица 1. Области в C2M2, новая версия 2.0 (в процессе консультаций).

Области	Описание цели
Управление рисками	Создание, использование и поддержка программы управления рисками кибербезопасности предприятия для выявления, анализа и снижения рисков кибербезопасности
Управление активами, изменениями и конфигурациями	Управление ИТ- и ОТ-активами организации, включая аппаратное и программное обеспечение, соразмерно риску для критически важной инфраструктуры и в соответствие с целями организации
Управление идентификацией и доступом	Создание и управление идентификации субъектов, которым может быть предоставлен логический или физический доступ к активам организации. Контроль доступа к активам организации
Менеджмент угроз и уязвимостей	Создание и поддержка планов, процедур и технологий для обнаружения, идентификации, анализа, управления и реагирования на угрозы и уязвимости кибербезопасности
Ситуационная осведомленность	Организация и поддержка деятельностей и технологий для сбора, анализа, оповещения, представления и использования оперативной информации и информации о кибербезопасности, информации о состоянии и сводной информации от других доменов для обеспечения ситуационной осведомленности об оперативном состоянии и состоянии кибербезопасности
Реагирование на события и инциденты	Создание и поддержка планов, процедур и технологий для обнаружения, анализа, смягчения последствий, реагирования и восстановления после событий и инцидентов в области кибербезопасности
Управление цепочкой поставок и внешними зависимостями	Создание и поддержание контроля для управления рисками кибербезопасности, связанными с услугами и активами, которые зависят от внешних субъектов, соизмеримым с риском для критически важной инфраструктуры и в соответствие с целями организации
Управление персоналом	Создание и поддержание планов, процедур, технологий и средств контроля для создания культуры кибербезопасности и обеспечения постоянного соответствия и компетентности персонала

[12] Cybersecurity Capability Maturity Model (C2M2), Version 1.1, February 2014, https://www.energy.gov/sites/prod/files/2014/03/f13/C2M2-v1-1_cor.pdf.

[13] Cybersecurity Capability Maturity Model (C2M2), Version 2.0, June 2019, https://apps.dtic.mil/sti/pdfs/AD1078768.pdf.

Архитектура кибербезопасности	Создание и поддержание структуры и поведения средств управления кибербезопасностью организации, процессов и других элементов
Управление программой кибербезопасности	Создание и поддержание корпоративной программы кибербезопасности, которая обеспечивает управление, стратегическое планирование и спонсирование деятельности организации в области кибербезопасности таким образом, чтобы цели кибербезопасности согласовывались со стратегическими целями организации и рисками для критически важной инфраструктуры

Трехмерная модель зрелости кибербезопасности сообщества (CCSMM)

Чтобы справиться с проблемой, заключающейся в том, что большинство государственных учреждений, отраслевых партнеров, операторов критически важной инфраструктуры, школьных систем, некоммерческих и других организаций существуют и действуют на локальном уровне, и не в одинаковой степени готовы к защите от киберугроз, которые могут повлиять на все сообщество, Центр сертификации и безопасности инфраструктуры (CIAS) Техасского университета в Сан-Антонио (UTSA) создал модель зрелости кибербезопасности сообщества (CCSMM).[14] Была разработана программа, чтобы помочь сообществам (и штатам) реализовать модель, и она была опробована в семи штатах, помогая им начать разработку своих собственных программ,[15] поскольку кибербезопасность общества, возможно, является слабым звеном в цепочке кибербезопасности страны. «Уровни» в CCSMM менее формальны и определяются как «уровни улучшения»:

- *Уровень 1 – Начальный*: некоторые процессы или программы могут существовать, но сообщество не имеет всех программных элементов для базовой программы;
- *Уровень 2 – Установленный*: была разработана базовая программа с элементами и процессами для всех четырех измерений;
- *Уровень 3 – Самооценка*: реализована минимальная жизнеспособная и устойчивая программа;

[14] "Community Cyber Security Maturity Model (CCSMM)," Center for Infrastructure Assurance and Security (CIAS) at The University of Texas at San Antonio (UTSA), по состоянию на 15 сентября 2020, https://cias.utsa.edu/the-ccsmm.html.

[15] Natalie Sjelin and Gregory White, "The Community Cyber Security Maturity Model," in *Cyber-Physical Security. Protecting Critical Infrastructure*, ed. Robert M. Clark and Simon Hakim (Cham, Switzerland: Springer, 2017), 161-183, https://doi.org/10.1007/978-3-319-32824-9_8.

- *Уровень 4 – Интегрированный*: кибербезопасность интегрирована во всем сообществе, включает всех граждан и все организации, сообщество работает с государством и другими сообществами в пределах штата;
- *Уровень 5 – Авангардный*: сообщество сохраняет полную бдительность в отношении кибербезопасности.

Эти уровни улучшения состояния сосредоточены на четырех областях, называемых измерениями, которые показаны в таблице 2.

Таблица 2. Измерения модели зрелости кибербезопасности сообщества (CCSMM).

Измерения	Описание
Осведомленность	Большинство людей понимают, что киберугрозы существуют. Однако не так много людей понимают масштабы угрозы, текущие тенденции атак, то, как киберинцидент может повлиять на сообщество, какие уязвимости следует устранить, каковы могут быть каскадные эффекты, если сообщество подвергнется кибератаке.
Обмен информацией	Занимается тем, что делать с информацией о кибер-инцидентах и куда следует сообщать такую информацию. Кроме того, как один сектор может обмениваться информацией с другим, позволяя второму сектору потенциально предотвратить возникновение аналогичного инцидента.
Политика	Рассматривает необходимость интеграции киберэлементов в разные политики или руководящие принципы и включает все руководящие регламенты, законы, правила и документы, которые регулируют повседневную деятельность сообщества. Политики должны оцениваться, чтобы гарантировать, что принципы кибербезопасности отражены во всем, что мы делаем, и должны устанавливать ожидания и ограничения
Планы	Сообщества разработали планы по устранению множества различных опасностей, и это измерение гарантирует, что элементы кибербезопасности включены в эти планы, позволяя сообществам знать, что делать с киберинцидентами, которые могут повлиять на функционирование сообществ.

Отличительной чертой этой модели является то, что она трехмерна, с добавлением «географии» в качестве третьей координаты с тремя значениями: организация, сообщество и государство. Эта трехмерная модель кибербезопасности сообщества может служить для определения дорожной карты для отдельных лиц, организаций, сообществ, штатов и нации, а также в качестве:

- *«аршина»* для измерения текущего состояния программы кибербезопасности и отношения сообщества;
- *дорожной карты*, чтобы помочь сообществу понять шаги, необходимые для повышения уровня безопасности;
- *общей точке отсчета*, позволяющей людям из разных штатов и сообществ сравнивать и относиться к отдельным программам.

Она заявлена как совместимая с другими известными рамками, такими как Рамка по кибербезопасности NIST, CMMC Министерства обороны, и для поддержки Рамки по кибербезопасности персонала Национальной инициативы по обучению кибербезопасности (NICE).

Модель зрелости потенциала кибербезопасности для государств (CMM-GCSCC [16])

CMM-GCSCC [17] – это методическая рамка, разработанная для анализа зрелости потенциала страны в области кибербезопасности. Она была разработана Глобальным центром потенциала кибербезопасности (GCSCC) в ходе глобального совместного учения, начатого в 2014 году. Для каждого из пяти измерений (показанных в таблице 3) модель предоставляет факторы (всего 24 для данной версии), которые определяют критерии для демонстрации соответствующей способности кибербезопасности. Большинство факторов исследуются с нескольких точек зрения и состоят из серии показателей в рамках пяти стадий зрелости для каждого измерения, которые называются следующим образом: *инициированный; формирующийся; учрежденный; стратегический; динамический*.

CMM-GCSCC – один из самых популярных инструментов оценки, применимых к странам и регионам, используемый международными организациями, такими как МТКС, Организация американских государств (ОАГ), Всемирный банк, Центр кибербезопасности Океании, Центр потенциала кибербезопасности для Южной Африки, Корпорация RAND и т.д. Он был развернут в более чем 80 странах с более чем 110 оценками и двумя региональными исследованиями ОАГ. Многие профили стран доступны для общественности, и достигнутые уровни можно увидеть вместе с рекомендованными улучшениями.[18] Публикация новой версии запланирована на вторую половину 2020 года. Следует отметить, что «потенциал» не эквивалентен «способности», и модель менее формальна, чем оценки зрелости, хотя параметры и факторы могут совпадать.

---

[16] Обозначенная здесь как “CMM-GCSCC” (в оригинале используется “CMM”), чтобы отличать от классической Модели зрелости способностей SEI, CMU.

[17] “Cybersecurity Capacity Maturity Model for Nations (CMM),” Revised Edition, по состоянию на 18 октября 2020, https://gcscc.ox.ac.uk/the-cmm.

[18] “GCSCC: CMM Reviews Around the World,” Global Cyber Security Capacity Centre, по состоянию на 10 октября 2020, https://gcscc.ox.ac.uk/cmm-reviews.

Таблица 3. Модель зрелости потенциала кибербезопасности для стран (CMM – GCSCC).

Измерения	Факторы
Политика и стратегия кибербезопасности	Национальная стратегия кибербезопасности; Реагирование на инциденты; защита критической инфраструктуры (КИ); Кризисный менеджмент; Киберзащита; Резервирование коммуникаций
Киберкультура и общество	Мышление в плане кибербезопасности; Доверие и уверенность в Интернете; Понимание пользователем принципов защиты личной информации в Интернете; Механизмы докладов; СМИ и социальные сети
Образование, обучение и умения в области кибербезопасности	Повышение осведомленности; Рамка для образования; Рамка для профессионального обучения
Правовая и нормативная база	Правовые рамки; Система уголовного правосудия; Рамки для официального и неформального сотрудничества в борьбе с киберпреступностью
Стандарты, организации и технологии	Соблюдение стандартов; Устойчивость интернет-инфраструктуры; Качество программного обеспечения; Технический контроль безопасности; Криптографические средства контроля; Торговая площадка для кибербезопасности; Ответственное раскрытие информации

Оценка кибербезопасности финансовых учреждений – инструмент CAT FFIEC

В 2015 году Федеральный совет для оценки финансовых учреждений США (FFIEC) представил инструмент оценки кибербезопасности (CAT) на основе модели зрелости для банковских учреждений, позволяющий оценивать риски и готовность к кибербезопасности путем измерения уровней риска и соответствующих средств контроля. Используются пять уровней зрелости: *базовый, развивающийся, средний, продвинутый и инновационный*, на основе пяти областей, характеризующих поведение, практики и процессы учреждения, которые поддерживают готовность к кибербезопасности. Пять доменов содержат в общей сложности 15 «факторов оценки» с 497 «декларативными утверждениями», используемыми для оценки уровня зрелости, достигнутого для каждого домена. Пятью доменами являются:

- Управление киберрисками и надзор;
- Анализ угроз и сотрудничество;
- Средства контроля кибербезопасности;
- Управление внешними зависимостями;
- Управление киберинцидентами и устойчивость.

Для каждой области оценка определяет уровень зрелости по следующей шкале:

- *Исходный уровень*: менеджмент рассматривает и оценивает руководящие принципы;
- *Развивающийся*: устанавливаются дополнительные процедуры и политики. Кибербезопасность расширяется за счет включения информационных активов и систем;
- *Промежуточный*: имеют место подробные процессы, контроль остается последовательным, управление рисками интегрировано в бизнес-стратегии;
- *Продвинутый*: методы и аналитика кибербезопасности включены во все виды деятельности; постоянное совершенствование процессов управления рисками;
- *Инновационный*: есть движущие силы инноваций в людях, процессах и технологиях (новые инструменты, новые средства управления, новые группы обмена информацией).

CAT FFIEC предназначен для выполнения периодически, но также после значительных технологических или функциональных изменений. Это самооценка, которую может подтвердить аудитор. После споров по поводу «добровольной оценки» инструмент был усовершенствован, чтобы лучше соответствовать рамке по кибербезопасности NIST (пересмотр ведется с 2019 года). Аудиторы также все чаще требуют, чтобы компании проводили оценку, чтобы продемонстрировать соответствие CAT FFIEC.

Обзор киберустойчивости (CRR), проводимый МНБ

Пакет самооценки был разработан Министерством национальной безопасности (МНБ) в партнерстве с отделом CERT SEI Университета Карнеги-Мелона как производный от CERT-RMM, адаптированный к потребностям собственников и операторов критически важной инфраструктуры.[19]

Как и в случае с CERT-RMM, CRR учитывает, что организация развертывает свои активы (люди, информация, технологии, объекты) для поддержки конкретных операционных задач или критически важных услуг. Затем выполняется оценка способностей для выполнения, планирования, управления, измерения и определения практик и поведения операционной устойчивости в следующих десяти областях: управление активами; Управление средствами контроля; Конфигурация и менеджмент изменений; Менеджмент уязвимостей; Менеджмент происшествий; Менеджмент непрерывности обслуживания; Менеджмент рисков; Менеджмент внешних зависимостей; Обучение и осведомленность; Ситуационная осведомленность. Домены являются производными от CERT-RMM и аналогичны десяти доменам

[19] "Cyber Resilience Review (CRR)," Cybersecurity & Infrastructure Security Agency, по состоянию на 10 октября 2020, https://us-cert.cisa.gov/resources/assessments.

C2M2. Оценка основана на методе CERT-RMM и может проводиться двумя способами: самооценка или в ходе сессии с посредником.

Оценка модели зрелости кибербезопасности (CMMC) Министерством обороны США

CMMC – это новое требование к оценке модели зрелости кибербезопасности для всех участников оборонно-промышленной базы (ОПБ), которые являются поставщиками Министерства обороны. Все компании ОПБ должны будут пройти сертификацию третьей стороной, чтобы соответствовать одному из пяти уровней зрелости, необходимых для подачи предложений по государственным контрактам.[20] Мы включаем эту модель в обзор, поскольку она содержит наиболее подробные актуальные требования и критерии оценки не только устойчивости организации, но и всей экосистемы (например, национальной безопасности и обороны). Модель определяет 17 областей потенциала с 43 способностями и 171 практикой на пяти уровнях зрелости для измерения технических способностей: *выполняемые, задокументированные, управляемые, проверенные, оптимизационные* (несколько отличающиеся от уровней в CMMI и CERT-RMM). Логика уровней CMMC отличается, поскольку она обеспечивает средства улучшения согласования процессов зрелости и практик кибербезопасности с чувствительностью информации, которую необходимо защитить, и с диапазоном угроз. Соответственно уровни определяются как:

Уровень 1: Защита информации о федеральном контракте (ФКИ);

Уровень 2: Служит переходным этапом в процессе защиты КНИ;

Уровень 3: Защита контролируемой несекретной информации (КНИ);

Уровни 4–5: Защита КУИ и снижение риска продвинутых постоянных угроз.

Домены соответствуют областям, связанным с безопасностью, в Федеральных стандартах обработки информации (FIPS) и соответствующим требованиям безопасности из рамки NIST. Это 17 доменов: Контроль доступа; Управление активами; Аудит и отчетность; Осведомленность и обучение; Управление конфигурацией; Идентификация и аутентификация; Реагирование на инциденты; Обслуживание; Защита СМИ; Безопасность персонала; Физическая защита; Восстановление; Управление рисками; Оценка безопасности; Ситуационная осведомленность; Защита систем и коммуникаций; Системная и информационная целостность.

[20] Cybersecurity Maturity Model Certification (CMMC), www.acq.osd.mil/cmmc/.

Показатели киберустойчивости MITRE

Мы кратко рассмотрим еще один систематический и с точки зрения архитектуры взгляд на методологию MITRE для оценки киберустойчивости, которая основана на подходе системы-из-систем (СиС) [21] и позволяет определять и оценивать метрики киберустойчивости на разных уровнях и в разных масштабах вплоть до национальных и транснациональных предприятий:

- На системном уровне, включая направленные системы-из-систем (СиС);
- Миссии, в том числе признанные СиС внутри организации;
- Организации, в которых могут применяться CERT-RMM или CRR МНБ;
- Секторы (например, секторы или подсекторы важнейшей инфраструктуры), регионы и миссии, поддерживаемые множеством организаций через совместную СиС;
- Государства и транснациональные предприятия, поддерживаемые виртуальной СиС.

Предлагаемые метрики могут облегчить разработку технических показателей для оценки рисков и надежности (таким образом, возможных каскадных эффектов, возрастающего воздействия) систем и последующего определения приоритетов программ улучшения.

Индикаторы кибербезопасности и зрелость

В связи с растущим интересом и стремлением стран ускорить программы улучшений и продвигать свои достижения на международном уровне, еще одним инструментом оценки и ранжирования статуса стран являются международные/глобальные индексы. Существует множество индексов, установленных уже десятилетиями в таких областях, как развитие информационного общества, цифровая готовность, подключение к Интернету, компьютерная грамотность и т.д. МТКС опубликовал в 2017 году «Индекс индексов кибербезопасности» [22] с наиболее популярными международными индексами кибербезопасности. Прокомментируем три из них с упором на оценку стран.

---

[21] Deborah Bodeau, John Brtis, Richard Graubart, and Jonathan Salwen, “Resiliency Techniques for System of Systems: Extending and Applying the Cyber Resiliency Engineering Framework to the Space Domain,” MTR 130515 (Bedford, MA: MITRE, September 2013), www.mitre.org/sites/default/files/publications/13-3513-Resiliency Techniques_0.pdf.

[22] “Index of Indices,” International Telecommunication Union, 2017, по состоянию на 18 октября 2020, https://www.itu.int/en/itu-d/cybersecurity/documents/2017_Index_of_Indices.pdf.

Глобальный индекс кибербезопасности (GCI), МТКС[23]: структура оценки, основанная на Глобальной программе кибербезопасности (GCA) МТКС. Индекс GCI измеряет соответствие стран требованиям кибербезопасности на глобальном уровне. Оценка измеряет уровень развития или вовлеченности страны с помощью онлайн-опроса, структурированного по пяти основным направлениям – правовые меры, технические меры, организационные меры, наращивание потенциала и сотрудничество – с использованием 25 индикаторов и дополнительных субиндикаторов, а затем подсчет общего балла. Начиная с первого опроса в 2013 году, GCI продвигает инициативы в области кибербезопасности путем сравнения. Третий выпуск GCI (в 2018 году), охватывающий более 193 стран и выпускающий три региональных отчета, показывает значительные улучшения в области кибербезопасности во всем мире, поскольку все больше стран имеют стратегии кибербезопасности, национальные планы, группы реагирования и конкретное законодательство. Однако значительный разрыв между регионами все же наблюдается.

Индекс национальной кибербезопасности (NCSI)[24]: глобальный индекс, измеряющий готовность стран предотвращать киберугрозы и осуществлять менеджмент крупномасштабных киберинцидентов, киберпреступности и киберкризисов. Эстонская академия электронного управления развивает его в сотрудничестве с Министерством иностранных дел Эстонии. Индекс подчеркивает общественные аспекты национальной кибербезопасности, обеспечиваемой центральным правительством. Индекс состоит из 12 основных индикаторов с подиндикаторами, разделенными на три группы: общая кибербезопасность, базовая кибербезопасность, менеджмент инцидентов и кризисный менеджмент. Индикаторы были привязаны к вопросам информационного общества и кибербезопасности, таким как электронная идентификация, цифровая подпись и наличие безопасной среды для электронных услуг. NCSI предоставляет общедоступные доказательные материалы и инструмент для наращивания национального потенциала в области кибербезопасности. Рейтинг страны сравнивается с GCI (МТКС), Индексом развития ИКТ и Индексом сетевой готовности.

Индекс киберготовности 2.0 (CRI 2.0)[25]: оценивает кибер-зрелость национального государства, а также его общую готовность к решению киберпроблем, определяет значение понятия «кибер-готовность» и предлагает практические планы, которым следует следовать. В индексе используется набор из семи показателей: национальная стратегия, реагирование на инциденты, электронная преступность и правоохранительные органы, обмен информацией, инвестиции в НИОКР, дипломатия и торговля, оборона

[23] "Global Cybersecurity Index," International Telecommunication Union, www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx.

[24] National Cybersecurity Index, Estonia, https://ncsi.ega.ee/.

[25] Cyber Readiness Index (CRI), Potomac Institute for Policy Studies, https://potomacinstitute.org/academic-centers/cyber-readiness-index.

и реагирование на кризисы. Были изучены сто двадцать пять стран, и методология основана на тех же принципах, что и Глобальная программа кибербезопасности МТКС. Каждой стране присваивается оценка, в то время как оценка военных способностей выходит за рамки охваченных GCI МТКС. Однако CRI 2.0 не предлагает никакого ранжирования, несмотря на свой механизм подсчета очков.

Хотя эти и другие известные индексы (Индекс кибербезопасности Касперского, Киберзрелость в Азиатско-Тихоокеанском регионе и т.д.) довольно популярны и ими легко популяризировать страны, их использование в качестве индикаторов оценки кибербезопасности сомнительно. Области и индикаторы похожи на таковые в моделях зрелости, но им не хватает строгости и детализации уровней зрелости и оценок. Нет уровней, и планы улучшений не могут быть расставлены по приоритетам и структурированы с четкими этапами и целями. Более высокий рейтинг в индексе может быть индикатором успеха, но его достижение вряд ли можно поставить в качестве цели. Баллы на основе вопросов во многом зависят от участия и мотивации местных органов предоставлять доказательства.

Акцент на зрелости в национальных стратегиях кибербезопасности

Акцент на зрелость кибербезопасности уже интегрирован, и оценки зрелости рекомендуются в большинстве обновленных руководств и рекомендаций по разработке национальных стратегий кибербезопасности. В Руководстве по передовому опыту для Национальной стратегии кибербезопасности (NCSS) ENISA (обновленном в 2016 году)[26] есть две ссылки на зрелость и оценки в течение жизненного цикла разработки и реализации стратегии. Чтобы установить базовые меры безопасности, следует рассмотреть несколько комплексных аспектов: разные уровни зрелости разных заинтересованных сторон, различия с точки зрения операционных возможностей каждой организации и разные стандарты, существующие в каждом критическом секторе. Среди рекомендуемых действий – «Создание инструментов самооценки зрелости и поощрение заинтересованных сторон к их использованию». Согласно Рекомендации 9: *«Расширение способностей государственного и частного секторов»*, после определения базовых требований необходимо оценить существующие возможности для выявления пробелов и отклонений. Для разработки планов улучшений и оценки результатов правительствам рекомендуется «активно поддерживать наращивание потенциала путем публикации национальных стандартов, *разработки моделей зрелости способностей для обеспечения кибербезопасности*, содействия и поощрения обмена знаниями…».

[26] "NCSS Good Practice Guide," ENISA, https://www.enisa.europa.eu/publications/ncss-good-practice-guide.

Тем не менее, беглый обзор национальных стратегий кибербезопасности (перечисленных на веб-сайте ENISA) показывает, что слово «зрелость» почти не упоминается, а «уровни зрелости» или модели зрелости не упоминаются. Это наблюдение может быть неполным, поскольку проблема может быть решена в планах и дорожных картах. Некоторые из упоминаний киберзрелости и моделей зрелости это:

- Стратегия Великобритании, принятая в 2016 году, гласит, что уровень поддержки правительством Великобритании каждого сектора определяется «с учетом его кибер-зрелости». Введена система кибер-оценки (CAF) NCSC для руководства организаций, обеспечивающих жизненно важные услуги;[27]
- В третьей Стратегии кибербезопасности Эстонии (2019) «проверенный уровень зрелости» рассматривается как одна из основных сильных сторон Эстонии. Определены различные области способностей и индикаторы типа зрелости, с подробным описанием «начального» и «целевого» уровней, четких целей и областей деятельности (что действительно делает его хорошим примером действенной стратегии), но никакие дальнейшие разработки по поводу возможного внедрения «моделей киберзрелости» или оценок киберзрелости не рассматриваются;
- Стратегия кибербезопасности Литвы (2018 г.) определяет в качестве своей первой цели «*усиление кибербезопасности в стране и развитие способностей для киберзащиты*»;
- Стратегия Финляндии (обновленная в 2019 г.) рекомендует, чтобы «каждая административная служба провела свою оценку рисков и анализ зрелости ...», что получило дальнейшее развитие в Программе реализации, которую Секретариат Комитета безопасности будет «*выполнять исследовательский проект по созданию обновленной модели зрелости и инструментов для мониторинга состояния кибербезопасности Финляндии и достижения целей ... Модель зрелости и инструменты будут использоваться для предоставления регулярных отчетов о состоянии*».

Пример использования: устойчивость и зрелость в болгарской национальной стратегии кибербезопасности

При разработке Национальной стратегии кибербезопасности в Болгарии, нацеленной на «Киберустойчивость Болгарии в 2020 году», был выбран подход, основанный на зрелости, поощряемый в основном опытом внедрения CERT-RMM.[28] Киберустойчивость была определена как целевое состоя-

[27] UK NCSC Cyber Assessment Framework (CAF), www.ncsc.gov.uk/collection/caf/cyber-assessment-framework.

[28] "Cyber Resilient Bulgaria 2020," National Cybersecurity Strategy (in Bulgarian), 2016, http://www.cyberbg.eu.

ние при реализации стратегии. Согласно стратегии, «достижение киберустойчивости на национальном уровне требует скоординированных действий в отношении безопасности и надежности всех компонентов и активов киберпространства: информации, технологий, людей и объектов, проектирования и развертывания коммуникационных каналов и услуг, их взаимозависимость и взаимодействие».

Стратегия имеет «действенную архитектуру» и определяет девять доменов (областей) с несколькими целями для каждой области и наборы мер (практик) с индикаторами способностей. Для описания «зрелости» используется трехуровневое определение безопасности в киберпространстве, основанное на двух хорошо известных аспектах [29]:

- реализация фундаментальной «триады» информационной безопасности – конфиденциальности, целостности и доступности (КЦД);
- степень наших знаний о рисках и угрозах – адаптация классификации «*известных неизвестных*», исходящей из сферы финансов и структурированной в теории «Черного лебедя» Нассима Талеба, но также используемой в других областях, в том числе для национальной безопасности и киберпространства.

Эти два аспекта помогли структурировать цели и меры на трех уровнях и представить их как обобщенный «ярлык», чтобы выразить своего рода уровни зрелости не только организаций, но также государства, экосистем, сообщества и нации. Эти «вложенные» уровни кратко описаны следующим образом:

- *Уровень 1 – Информационная/ ИТ-безопасность («известные известные»):* защита информационных активов и инфраструктуры от известных «угроз КЦД»;
- *Уровень 2 – Кибербезопасность («известные неизвестные»)*: борьба с комбинированными угрозами, различными продвинутыми постоянными угрозами (ППУ), атаками на репутацию людей и организаций, кампаниями по дезинформации и другими непредсказуемыми последствиями массовой миграции деятельности в киберпространство, масштабные информационные утечки (в национальном, региональном и глобальном масштабе), требующие расширенного и систематического применения концепции КЦД ко всем активам цифровой экосистемы – людям, объектам, технологиям и информации (неформальное описание кибербезопасности);

[29] George Sharkov, "From Cybersecurity to Collaborative Resiliency," in *Proceedings of the 2016 ACM Workshop on Automated Decision Making for Active Cyber Defense (SafeConfig '16)*, 2016, ACM, New York, USA, 3–9, https://doi.org/10.1145/2994475.2994484.

- *Уровень 3 – Киберустойчивость («неизвестные неизвестные»)*: подготовка к неизвестному: неожиданные, непредвиденные угрозы в киберпространстве, динамически меняющиеся риски и сложные воздействия с непредсказуемыми последствиями, необходимая для гибкости и устойчивости систем, процессов и организаций, а также введение соответствующих требований при разработке и развертывании систем и процессов – важнейшие характеристики состояния киберустойчивости.

Кроме того, этапы реализации стратегии определяются как достижение «уровней зрелости» и *переход от кибербезопасности к киберустойчивости* для всей страны, а именно:

Этап 1 – Инициирование («Институты кибербезопасности»): Общее согласие по приоритетам Национальной стратегии кибербезопасности и Дорожной карты. Принятие скоординированного подхода и создание общей структуры национальной системы кибербезопасности. Определение основных структур и основного потенциала, процессов и принципов развития в координации с ключевыми заинтересованными сторонами. Не отставая от НАТО и ЕС обеспечить базовую кибербезопасность. Сосредоточение на необходимом базовом уровне *информационной безопасности* и использование его для достижения кибербезопасности на уровне отдельных организаций. Разработка определения «кибер-кризиса» в Национальной сети координации кибербезопасности. Проведение отраслевых и межотраслевых учений с участием таких организаций, как государственные органы, предприятия и научные круги.

Этап 2 – Развитие («От потенциала к способностям»): сосредоточение внимания на организациях, устойчивых к киберпространству, и в кибербезопасном обществе, разработка скоординированных мер реагирования на кибер-кризисы на национальном уровне. Продолжение профилактических мероприятий, внедрение надежного механизма взаимодействия и сотрудничества в случае инцидентов и кризисов. Контроль общей «кибер-картины» (ситуационная осведомленность). Создание базовых способностей для оперативного и стратегического анализа и оценки, оперативного и технического сотрудничества с НАТО, ЕС и другими международными сетями.

Этап 3 – Зрелость («Киберустойчивое общество»): эффективное сотрудничество на оперативном и стратегическом уровнях в национальном и международном масштабе. На основе участия и готовности всех заинтересованных сторон развивать передовые совместные способности в государственном, частном и исследовательском секторах. Определение нишей и занятие лидирующих позиций и специализация в регионе, ЕС и НАТО.

Впоследствии в национальном законе о кибербезопасности (2018 г.) использовался подход «уровней способностей» для определения требований к основным услугам и критически важным инфраструктурам. Целевые уровни способностей определяются следующим образом: «Базовый» (соответствует кибергигиене из Директивы NIS), «Кибербезопасность» (или «вы-

полнено», как определено Государственным агентством национальной безопасности) и «Устойчивый» (определяется Министерством обороны в соответствии с планами по гражданской устойчивости и обязательствами по коллективной обороне НАТО и ЕС).

Как видно, гибридные угрозы (например, дезинформация) были рассмотрены уже на *«Уровне 2 – Кибербезопасность»*, но более систематический охват «гибридного влияния», особенно в контексте повышенного особого интереса к Восточной Европе, продолжается для текущего обновления Национальной стратегии устойчивости и Дорожной карты, включающее новое кибер / гибридное влияние (также известное как «*кибрид*») на обе области – умы людей и критически важную инфраструктуру.[30]

Киберзрелость и стратегии ЕС и НАТО

Подход на основе уровней зрелости был рекомендован для включения кибербезопасности в «Общую политику безопасности и обороны ЕС» (ОПБО). В исследовании, проведенном ENISA и Группой оценки возможностей науки и технологий Европейского парламента, рассматриваются три аспекта более безопасного киберпространства в контексте ОПБО.[31] В области наращивания потенциала указано, что для содействия наращиванию потенциала необходимо иметь возможность его измерить. В исследовании рекомендуется использовать модели потенциала кибербезопасности, которые позволяют развивать и контролировать киберпотенциал и его зрелость. Упоминается модель зрелости способностей кибербезопасности (CMM GCSCC).

В другом исследовании финансовых услуг ЕС обсуждается «… степень устойчивости цифровых операций и зрелости кибербезопасности», которую необходимо учитывать.[32]

Новая рамка оценки зрелости, Рамка оценки зрелости кибербезопасности (CMAF), была недавно предложена и внедрена в качестве пилотного проекта в Греции, посвященного оценке соответствия требованиям Директивы NIS. Предусмотрены два основных применения CMAF: для самооценки со стороны операторов основных услуг и поставщиков цифровых услуг (определенных в соответствии с Директивой NIS, принятой государствами-

[30] Todor Tagarev, “Understanding Hybrid Influence: Emerging Analysis Frameworks,” in *Digital Transformation, Cyber Security and Resilience of Modern Societies*, ed. Todor Tagarev, Krassimir Atanassov, Vyacheslav Kharchenko, and Janusz Kasprzyk (Cham, Switzerland: Springer, 2021).

[31] EU Parliament, “Cybersecurity in the EU Common Security and Defence Policy (CSDP): Challenges and Risks for the EU,” 2017, по состоянию на 15 сентября 2020, https://www.europarl.europa.eu/stoa/en/document/EPRS_STU(2017)603175.

[32] European Commission, “Digital Operational Resilience Framework for Financial Services: Making the EU Financial Sector More Secure,” Consultation Document, 2019, accessed September 15, 2020, https://ec.europa.eu/info/sites/info/files/business_economy_euro/banking_and_finance/documents/2019-financial-services-digital-resilience-consultation-document_en.pdf.

членами) или в качестве инструмента аудита компетентных национальных органов по кибербезопасности.

ENISA также предоставила инструмент самооценки зрелости CSIRT,[33] чтобы помочь в развитии потенциала и возможностей национальных и отраслевых CERT.

В дополнение к очень требовательным моделям зрелости, введенным для оборонных закупок и цепочки поставок военной продукции (например, CMMC Министерства обороны США, представленной выше), НАТО использует подход уровней зрелости для планирования и оценки развития способностей для киберзащиты в странах в соответствии с текущим процессом Обязательства по кибероборонe.[34]

Заключение

Для оценки кибербезопасности и киберустойчивости отдельного сектора, сообщества, страны или региона необходим единый подход к определению целей и показателей измерения. Модели зрелости способностей предоставляют такой механизм, поскольку они реализуют схожую архитектуру и, независимо от возможных различий в масштабах и определениях доменов, они производят сопоставимую оценку достижений и облегчают агрегирование целевых состояний. Как показано, большинство популярных моделей могут быть сопоставлены естественным образом, что позволяет организациям выбирать наиболее подходящие для их профиля и бизнес-целей. На национальном уровне оценки и планы также могут быть разработаны эффективно, поскольку уровни зрелости и способностей имеют одинаковое значение. Однако это ставит под сомнение «зрелость» моделей зрелости. Поскольку «кибербезопасность» охватывает в основном сторону «защиты», необходимо ввести устойчивость, чтобы завершить цикл защиты и поддержания. Кроме того, следует ввести новые области, такие как гибридные угрозы, обеспечиваемые киберспособностями (называемые «кибридными»), поскольку ни одна из изученных моделей еще не охватывает эти аспекты, и «*умы людей – это не тот сектор, который мы знаем, как защищать*». То же самое и с новыми революционными технологиями, такими как ИИ, Quantum, 5G – «инновационных» способностей на более высоких уровнях развития недостаточно, и, безусловно, потребуются новые области и индикаторы. Модели зрелости помогают согласовать амбиции и программы на более высоком уровне (например, в государствах-членах ЕС, штатах США или регионах). Также рекомендуется привлекать и вовлекать МСП в «дорожную карту к зрелости».

---

[33] ENISA, “CSIRT Maturity – Self-assessment Tool, accessed September 15, 2020, https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-capabilities/csirt-maturity/csirt-maturity-self-assessment-survey.

[34] Jamie Shea, “Cyberspace as a Domain of Operations,” *MCU Journal* 9, no. 2 (Fall 2018): 133-150, https://doi.org/10.21140/mcuj.2018090208.

Отказ от ответственности

Выраженные здесь взгляды являются исключительно взглядами автора и не отражают точку зрения Консорциума оборонных академий и институтов изучения безопасности ПрМ, участвующих организаций или редакторов Консорциума.

Об авторе

Георги Шарков - советник министра обороны и национальный координатор по кибербезопасности в период 2014-2017 гг. Он руководил разработкой Национальной стратегии кибербезопасности Болгарии, принятой в 2016 году. Он имеет докторскую степень в области искусственного интеллекта и специализируется в прикладной информатике, термографии, генетике, интеллектуальных финансовых системах и системах безопасности. С 2003 года он является генеральным директором Европейского института программного обеспечения – Центр Восточной Европы, руководителем лаборатории кибербезопасности (CyResLab), а с 2014 года возглавляет лабораторию кибербезопасности в Софийском технологическом парке.
E-mail: gesha@esicenter.bg

Connections: The Quarterly Journal
ISSN 1812-1101, e-ISSN 1812-2973

Андраш Худик, *Connections QJ* 19, № 4 (2020): 29-44
https://doi.org/10.11610/Connections.rus.19.4.02

Рецензированная статья

Лучшие практики в применении концепции устойчивости: создание способностей для гибридной войны и кибербезопасности в Силах обороны Венгрии

Андраш Худик

Резюме: В своей Глобальной стратегии внешней политики и безопасности ЕС применяет устойчивость как всеобъемлющую концепцию внутренней и внешней безопасности. Параллельно с этим, на саммите 2016 года в Варшаве лидеры Североатлантического союза решили повысить устойчивость НАТО к полному спектру угроз. Каждый член НАТО должен быть устойчивым к серьезным потрясениям, вызванными стихийными бедствиями, отказом критически важной инфраструктуры, средствами гибридной войны или вооруженным нападением. Гибридная война, включая кибератаки, считается серьезной проблемой безопасности.

Стратегия национальной безопасности Венгрии, принятая в 2020 году, подтверждает, что основной международной рамкой политики Венгрии в области безопасности и обороны является членство в НАТО и ЕС, и подчеркивает необходимость повышения устойчивости страны к гибридным атакам. В этой статье представлен анализ применения концепции устойчивости в оборонном секторе Венгрии. Он знакомит нас с развитием устойчивости сил обороны Венгрии к гибридным угрозам, включая их кибер-компонент, а также дает лицам, принимающим решения, варианты для выбора в отношении военных и информационных инструментов национальной мощи. Автор определяет потенциальные гибридные угрозы против Венгрии, возможный сценарий кибератак и направления усилий для достижения максимально возможного уровня устойчивости к таким угрозам. Он принимает во внимание политическую и военную среду, а также более широкие национальные проблемы с учетом гибридных угроз и основных характеристик и дилемм кибервойны, таким образом стремясь способствовать применению концепции устойчивости в Венгрии.

Ключевые слова: устойчивость, политика безопасности, вооруженные силы, разведка, гибридная война, киберзащита, ЕС, НАТО, Венгрия.

Введение: Применение концепции устойчивости в Венгрии

Целью применения концепции устойчивости является усиление способности систем, организаций, политик и отдельных лиц оптимально реагировать на внешние воздействия. Многие эксперты сходятся во мнении, что «недавний энтузиазм по поводу концепции устойчивости во многих публикациях по политикам устойчивости является следствием ее соответствия неолиберальному дискурсу. Это не означает, что идея устойчивости сводится к неолиберальной политике и неолиберальному управлению, но она точно соответствует тому, что они пытаются сказать и сделать».[1]

Идеология неолиберализма в первую очередь видит гарантию экономического роста, благосостояния, свободы и общего блага в «либерализации» рынков. Неолиберальное государство радикально отходит от перераспределения, характерного для государства всеобщего благосостояния, принимает меры, благоприятствующие бизнесу и рынку, для защиты доходов частного капитала и превращает граждан в предпринимателей и потребителей.

Крах неолиберальной гегемонии после 2008 года привел к новой волне популизма. Популистские партии и движения включают в себя как левых, так и правых деятелей. Одна из их немногих общих черт заключается в том, что все они критикуют правящую элиту и ее идеологию заявляя, что элиты угнетают людей.

Согласно левой риторике, социальная и экономическая политика популистского правительства Орбана в Венгрии заключается в укреплении национального капиталистического класса, продаже дешевой рабочей силы иностранным промышленным инвесторам, при этом дисциплинируя этих рабочих и осуществляя централизованный контроль над бедными, в основном живущими в сельских районах. Целью его культурной политики является продвижение официальной венгерской идеологии эпохи до 1938 года: консервативная, христианская, националистическая идеология, основанная на исторической лжи, с несправедливой социальной системой, атмосферой ненависти и скрытым намерением вернуть территории, утраченные после Первой мировой войны. Орбан воспринимает неолиберальный Европейский Союз, тайные мошеннические действия международных капиталистов, олицетворяемые Джорджем Соросом, и мигрантов как врагов, чтобы объявить своих политических оппонентов врагами нации и взять на себя роль ее спасителя.

В то время как правительство атакует некоторые ценности ЕС перед политической аудиторией и вызывает громкое противостояние, с точки зре-

[1] Jonathan Joseph, “Resilience as Embedded Neoliberalism: A Governmentality Approach,” *International Policies, Practices and Discourses* 1, no. 1 (2013): 38-52, https://doi.org/10.1080/21693293.2013.765741.

ния экономических процессов, оно является подчиненным союзником европейских капиталистов.[2] Из-за конструктивистских элементов политики Виктора Орбана по установлению режима,[3] демократия, верховенство закона и плюрализм в Венгрии стали ограниченными и привели к созданию страны с нелиберальной демократией. В Венгрии те, кто находится у власти, полагают, что левые и либералы не являются частью нации, и все, что является левым или либеральным, будь то личность, любое произведение искусства, или просто точка зрения или подход, должно считаться чуждым и должно быть отвергнутым, потому что оно противоречит официальному национальному христианскому консервативному курсу.

Возможно, этот политический климат также способствует тому факту, что в Венгрии только оборонная наука, связанная с НАТО, инициирует разработку концепций безопасности и правоохранительной деятельности на основе устойчивости. Однако более правдоподобное объяснение состоит в том, что, в отличие от общепринятой всеобъемлющей политики безопасности и подхода к кризисному управлению, в отношение устойчивости мы должны сосредоточиться на решениях на национальном уровне. Многие венгерские эксперты считают это свидетельством целесообразности усилий по разработке комплексного подхода на национальном уровне, которые были начаты в нашей стране в 2010 году.

Большинство венгерских экспертов по политике безопасности считают, что в 2014 году во время украинского кризиса и НАТО, и ЕС нашли адекватный ответ на гибридные угрозы в повышении устойчивости стран и в поддержке военных усилий с помощью гражданских инструментов (гражданской готовности). Сама суть этого решения заключается в скоординированном применении военных и гражданских компонентов кризисного менеджмента, что также является основным принципом комплексного подхода.

Таким образом, можно считать, что предпосылки, фундаментальные принципы и инструментарий, применяемые для обеспечения устойчивости и гражданской готовности, практически совпадают с самим комплексным подходом; они являются всего лишь его переосмыслением в другом контексте. Поэтому, устойчивость и гражданская готовность не повлекли за собой иной образ мышления или набор требований. Тем не менее, их нельзя рассматривать как идентичные каким-либо уже существующим комплексам задач в соответствии с каким-либо законодательством.

---

[2] Тамаш Героч и Чаба Елинек, «Система венгерского национального сотрудничества в контексте Европейского Союза – об интеграции Венгрии в ЕС, исторический и социологический подход», *Analízis* (2018): 12-33 цитата на стр. 23, www.regscience.hu:8080/xmlui/bitstream/handle/11155/1768/jelinek_nemzeti_2018.pdf, – на венгерском.

[3] Gábor Illés, András Körösényi, and Rudolf Metz, "Broadening the Limits of Reconstructive Leadership – Constructivist Elements of Viktor Orbán's Regime-building Politics," *The British Journal of Politics and International Relations* 20, no. 3 (2018): 790-808, https://doi.org/10.1177/1369148118775043.

Следовательно, необходимо законодательно назначить национального координатора как для обеспечения устойчивости, так и для обеспечения гражданской готовности, а также для определения объема задач национального уровня, органов и организаций, ответственных за их выполнение, сотрудничающих организаций и процессуальных правил сотрудничества. Учитывая, что эта задача требует тесного и всестороннего сотрудничества всего правительства, эффективное выполнение этих обязанностей должно входить в компетенцию и возможности системы администрации обороны.[4]

Создание в Силах обороны Венгрии способностей для противодействия гибридной и кибервойне

Венгерские силы обороны

Венгерские силы обороны (ВСО) – это национальные силы обороны Венгрии. С 2007 года в Венгерских вооруженных силах действует единая командная структура. Министерство обороны осуществляет политический и гражданский контроль над армией. Подчиненное министерству Командование объединенных сил координирует и командует подразделениями ВСО.

В вооруженных силах несут действительную службу 28 000 человек. В 2019 году военные расходы составили 1,904 миллиарда долларов США, или около 1,2% ВВП страны, что значительно ниже целевого показателя НАТО в 2%. В 2016 году правительство приняло решение, согласно которому обязалось увеличить расходы на оборону до 2% ВВП, а численность действующего персонала – до 37 650 к 2026 году. Военная служба является добровольной, хотя в военное время может осуществляться и призыв.

Согласно Конституции Венгрии, тремя столпами безопасности нации являются способности ВСО, система Альянса и граждане.

В феврале 2017 года Министерство обороны обнародовало программу развития Зриньи 2026, которая направлена на повышение способностей действующих вооруженных сил, численности резервных сил, военной коммуникационной и информационной систем, а также для киберзащиты. Эти меры кажутся адекватными шагами для повышения устойчивости к гибридным угрозам.

Подход к повышению устойчивости к гибридным атакам

Гибридная война означает «использование военных и невоенных инструментов в интегрированной кампании, направленной на достижение внезап-

[4] Ласло Кесели, «Гибридная война и национальная устойчивость, или перезагрузка комплексного подхода», *Katonai Jogi és Hadijogi Szemle [Военное право и Обзор военного права]* 1 (2018): 29-62, цитата на с. 61-62, http://epa.uz.ua/02500/02511/00008/pdf/EPA02511_katonai_jogi_szemle_2018_1_029-062.pdf. – на венгерском.

ности, захват инициативы и получение психологических, а также физических преимуществ с использованием дипломатических средств; сложные и быстрые информационные, электронные и кибероперации; тайные, а иногда и открытые военные и разведывательные действия; и экономическое давление».[5] Другими словами, гибридные атаки сочетают в себе военные и невоенные, а также скрытые и открытые средства, включая дезинформацию, кибератаки, экономическое давление и развертывание нерегулярных вооруженных групп, а также использование регулярных сил. В настоящее время гибридная война считается серьезной проблемой безопасности; к этой более широкой категории угроз относятся кибератаки, которые воспринимаются как одна из основных угроз современному обществу каждой страны.

На фигуре 1 показан проект Сил обороны Венгрии в области повышения устойчивости к гибридным атакам, основанный на выводах Адриана Фехера.[6] Фехер следовал шагам методологии армейского строительства,[7] и поэтому описывает желаемую среду, определяет проблему и рекомендует оперативный подход. После модификации этим автором подход, используемый в проекте, состоит из шести целей, семи итогов и 15 предлагаемых результатов, которые должны повысить уровень устойчивости к гибридным угрозам и, таким образом, защитить страну. На фигуре показано сопоставление инструментов национального могущества с каждым из результатов.

Основная логика предлагаемого подхода заключается в том, что Венгрии нужна гибридная стратегия защиты для борьбы с потенциальными гибридными угрозами. Военный инструмент национальной мощи должен расширять свое значение и способствовать повышению информационной мощи, развитию потенциала информационного сдерживания для защиты суверенитета Венгрии посредством участия граждан. В то же время существует потребность в поддержке со стороны других агентств в создании потенциала информационного сдерживания для защиты населения от враждебной пропаганды и кибератак. Поскольку военный инструмент сильно зависит от других инструментов национального могущества, ВСО должны поддерживать и улучшать сотрудничество с другими заинтересованными сторонами, чтобы осуществлять «общегосударственный» подход. Область информации и связанные с ней информационные операции играют важную роль в гибридной войне. Исторически сложилось так, что военные операции в

---

[5] James K. Wither, “Making Sense of Hybrid Warfare,” *Connections: The Quarterly Journal* 15, no. 2 (2016): 73-87, цитата на стр. 76, https://doi.org/10.11610/Connections.15.2.06.

[6] Adrian Feher, “Hungary’s Alternative to Counter Hybrid Warfare,” Thesis (Fort Leavenworth, Kansas: U.S. Army Command and General Staff College, 2017), 128, 123, https://apps.dtic.mil/dtic/tr/fulltext/u2/1038681.pdf.

[7] Headquarters, Department of the Army, *Army Design Methodology*, ATP 5-0.1, July 1, 2015, https://armypubs.army.mil/epubs/DR_pubs/DR_a/pdf/web/atp5_0x1.pdf.

первую очередь сосредоточивались на способностях противника и только во вторую очередь – на ослаблении его решимости, тогда как информационные операции нацелены на ослабление его решимости и силы воли.

Целью информационных операций является достижение превосходства в лидерстве, информационного господства и информационного превосходства путем использования психологических операций и операций по обеспечению операционной безопасности, военному обману, физическому уничтожению, радиоэлектронной войне, общественной информации, компьютерным сетевым войнам и военно-гражданскому сотрудничеству с использованием военных информационных систем и разведывательной информации.[8] В доктрине информационных операций, применяемой в настоящее время Силами обороны Венгрии, детали концепции информационных операций еще не разработаны. Элементы информационных операций лишь частично отражают действия и способности, которые должны быть достигнуты в информационной среде. Эксперты утверждают, что главная задача, стоящая перед Силами обороны Венгрии, заключается в достижении способности решать сложные информационные вопросы: быстро получать, обрабатывать и интегрировать информацию в цикл принятия решений, а также контролировать нарративы о конфликтах в информационном пространстве.

Цель проекта: **Защита суверенитета и независимости Венгрии за счет повышения устойчивости к гибридным угрозам**		
Цели	Итоги и инструменты	Результаты
Обладать потенциалом военного сдерживания, чтобы остановить врага и поддержать интервенцию сил НАТО в Венгрии.	Повышение способностей добровольных резервных конвенциональных сил **(В&И)** и создание добровольческих неконвенциональных резервных силы **(В&И)**	1, 2, 3, 4, **5**, 7, 9, 10, 12, 13, 14, 15
Обеспечение конституционного порядка и оказание поддержки	Создание способностей для добровольной гражданской готовности (**В&И**)	1, 2, 3, 4, 6, 7, 9, 10, 12, 13, 14, 15

[8] Жолт Хейг, «Методология определения критических информационных инфраструктур, информационная война», ENO Advisory Ltd., 1 августа 2009 г., с. 88, https://nki.gov.hu/wp-content/uploads/2009/10/a_kritikus_informacios_infrastrukturak_meghatarozasanak_modszertana.pdf; Жольт Хейг и Иштван Вархеги, «Интерпретация киберпространства и кибервойны», *Военная наука* (2008): 5-10, на венгерском языке, http://mhtt.eu/hadtudomany/2008/2008_elektronikus/2008_e_2.pdf.

центральному правительству	Достичь приверженности граждан делу защиты нации **(И)**	1, 2, 3, 4, **5**, 7, 8, 9, 10, 12, 15
Помощь союзникам по НАТО в условиях коллективной обороны	Увеличение экспедиционного потенциала действующих сил (**В**)	1, 2, 3, **5,** 6, 7, 8, 9, 10, 11, 12, 13, 14, 15
Развитие информационных способностей для сдерживания	Защита граждан от средств враждебного влияния и национальных сил от кибератак **(И)**	1, 2, 3, **5**, 6, 7, 9, 10, 13, 15
Предотвращение неожиданности	Создание интегрированных средств разведки, наблюдения и рекогносцировки - обеспечение оперативной безопасности **(И)**	2, 3, **5,** 6, 9, 15
Следование «общегосударственному» подходу к обороне	Обеспечить межведомственное взаимодействие **(ДИВЭ)**	1, 2, 3, 4, **5**, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15
Результаты: (1) Повышение патриотизма через социальные и традиционные СМИ; (2) Устранение ложного чувства безопасности; (3) Выявление и опровержение ложных новостей; (4) нанятие волонтеров; (5) **Увеличение способностей для кибервойны**; (6) Улучшение контрразведки для выявления и обнаружения предупреждающих сигналов; (7) Проведение совместных и комбинированных учений (упражнений); (8) Устранение / интеграция экстремистских групп и создание движения сопротивления; (9) Выявление уязвимостей и пробелов в способностях; (10) Установление децентрализованного командования и управления с безопасной связью; (11) Обеспечение быстрого реагирования через правовую систему; (12) Создание систему готовности и мобилизации; (13) Обеспечить обучение и экипировать силы; (14) Создание предварительно размещенных запасов; (15) Обеспечение координации лиц, принимающих решения;		

Фигура 1: Проект по повышению устойчивости к гибридным атакам.
Сокращения: ДИВЭ - инструменты дипломатии, информации, военного дела и экономики; В (военный инструмент), И (информационный инструмент), В&И (военный и информационный инструмент).

В то же время необходимо развивать оперативные возможности ВСО в киберпространстве и обеспечивать их интеграцию как в военное планирование, так и в выполнение операций. С этой целью Силы обороны Венгрии должны принять новый образ мышления, в первую очередь сосредотачиваясь не только на проведении боевых действий, но и на желаемых результатах таких военных операций, включая влияние таких результатов. В военной

доктрине необходимо более широкое толкование системы информационных инструментов. Недостаточно рассматривать их как выполняющих простую вспомогательную функцию.

Киберзащита в Венгрии

Основные аспекты и дилеммы кибервойны

Как правило, в кибервойне государства начинают свои операции в разведывательных целях с подрывными или деструктивными намерениями и делают это напрямую или с привлечением третьих сторон, таких как хакеры. Атаки могут быть нацелены на критически важные публичные инфраструктуры, в частности на ИТ, информационные и коммуникационные системы, используемые в оборонном секторе. Кроме того, все более распространенными становятся враждебные действия с использованием социальных сетей и Интернет-платформ для воздействия на гражданское общество. В более широком смысле кибервойна охватывает все атаки, осуществляемые в киберпространстве, с полезными результатами для нападающего в военном или политическом плане.[9] Опыт показывает, что кибератака ложится серьезным бременем на страну только в том случае, если она скоординирована (связывает военное управление со стратегической целью, которой подчиняется каждое оперативное действие), происходит волнами (типы и цели атак разнообразны, непредсказуемы и они осуществляются последовательно), является многосекторальной (затрагивает несколько отраслей, в то время как координация обороны обычно охватывает лишь небольшой круг секторов), поддерживается информацией, полученной разведкой (информация, необходимая для атак, поступает не только из открытых источников, но и в результате сбора и анализа разведданных), и в первую очередь осуществляется для нанесения ущерба противнику. Цель состоит в том, чтобы заставить страну и ее граждан почувствовать атаку, т.е. такие атаки должны быть очень очевидными и включать эмоциональные воздействия – характеристики, которые отличают их от кибершпионажа.[10] Кибератаки обычно не используются государствами в деструктивных целях в мирные периоды, поскольку пребывание в «серой зоне» между миром и

[9] Тибор Рожа, «Теория, практика и тенденции информационных операций», *Оборонное обозрение 5* (2019): 82-84; Габор Берк, «Киберпространство, его опасности и текущее состояние киберзащиты в Венгрии», *Обзор национальной безопасности 3* (2018): 5-21, http://epa.oszk.hu/02500/02538/00024/pdf/EPA02538_nemzetbiztonsagi_szemle_2018_03_005-021.pdf; Жолт Чутак, «Новая война новых времен – когнитивная безопасность в эпоху информации и кибервойн», *Оборонное обозрение 5* (2018): 33-45, http://real.mtak.hu/84099/1/hsz_2018_5_beliv_033_045.pdf. – все источники на венгерском языке.

[10] Csaba Krasznay, “Protecting Citizens in a Cyber Conflict,” *Military Engineer* 7, no. 4 (December 2012), 142-151, цитата на стр. 144, http://hadmernok.hu/2012_4_krasznay.pdf.

войной наилучшим образом служит их интересам. Это не значит, что они не смогут выйти за пределы этой зоны в случае необходимости.

Основная дилемма кибервойны – отсутствие международного регулирования киберпространства. Хотя большинство государств-членов ООН признают расширение сферы действия международных соглашений в отношении киберпространства, их применимость по-прежнему проблематична.[11] Это связано с тем, что не существует международно признанного определения того, что мы называем кибератакой или кибероружием. Кроме того, при кибератаке обычно не происходит четкого объявления войны, злоумышленники остаются скрытыми в киберпространстве, а ожидаемые последствия также остаются неоцененными. Поэтому серьезное внимание уделяется применению соответствующих конвенций к операциям в киберпространстве.[12]

Инициатива «Парижский призыв к доверию и безопасности в киберпространстве» [13] была создана, чтобы гарантировать безопасность киберпространства на международном уровне. Венгрия присоединилась к инициативе, но крупнейшие владельцы кибер-арсенала (США, Израиль, Иран, Китай, Великобритания или Россия) не сочли это необходимым.

Киберзащита НАТО

Противодействие кибератакам является одним из основных приоритетов для НАТО. Однако в отношении обычно используемых терминов кибервойна или кибератака следует отметить, что в официальной терминологии НАТО нет согласованного определения кибервойны или кибератаки, а примеры определений можно найти только на уровне государств-членов.

В основном это связано с отсутствием границ в киберпространстве и постоянным расширением диапазона типов атак, которые оно допускает, а также с интересами Альянса. НАТО не считает определение понятия кибератаки необходимым, потому что оно индивидуально оценивает одновременные, но разные типы атак, чтобы принять решение о характере реакции на уровне альянса.

С 2007 года НАТО уделяет особое внимание киберзащите и кибервойне. В 2012 году киберзащита была включена в планирование обороны Североатлантического союза, а на саммите в Уэльсе в 2014 году были приняты ру-

---

[11] “Trends in International Law for Cyberspace,” NATO Cooperative Cyber Defense Centre of Excellence, May 2019, https://ccdcoe.org/uploads/2019/05/Trends-Intlaw_a4_final.pdf.

[12] David P. Fidler, “The UN Secretary-General’s Call for Regulating Cyberwar Raises More Questions than Answers,” Council of Foreign Relations, March 15, 2018, www.cfr.org/blog/un-secretary-generals-call-regulating-cyberwar-raises-more-questions-answers.

[13] Ministry for Europe and Foreign Affairs, “Cyber Security: Paris Call of 12 November 2018 for Trust and Security in the Cyber Space,” *France Diplomacy*, www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/france-and-cyber-security/article/cybersecurity-paris-call-of-12-november-2018-for-trust-and-security-in.

ководящие принципы НАТО по киберзащите. В Уэльсе Североатлантический союз заявил, что признает действительность международного права в киберпространстве, и включил киберзащиту в число задач коллективной обороны НАТО.[14]

В 2016 году в коммюнике Варшавского саммита союзники расширили сферу боевых действий, традиционно охватывающих море, воздух и сушу, включив в нее киберпространство,[15] и заявили, что кибератака против государства-члена может рассматриваться Североатлантическим союзом как атака на НАТО в целом и, при необходимости, в ответ могут быть приняты коллективные меры.

В Варшаве было принято Обязательство по киберзащите, в соответствии с которым государства-члены предприняли существенное и быстрое развитие защиты своих национальных сетей и инфраструктур в соответствии со статьей 3 Вашингтонского договора, развитие всеобъемлющего потенциала киберзащиты и усиление сотрудничества в выявлении и понимании угроз при улучшении образования и обучения в области кибербезопасности. Важным шагом в развитии потенциала киберзащиты НАТО является создание, начиная с 2018 года, Оперативного киберцентра (CyOC) для координации кибероперациий Североатлантического союза в рамках Главного штаба союзных сил в Европе (SHAPE).

В своих киберспособностях НАТО различает пассивные и активные оборонные способности: первые состоят в основном из превентивных способностей, способностей для менеджмента инцидентов, для восстановления данных и систем в пределах своей собственной сети. Активные – это способности наступательного характера для сдерживания и устранения угроз, выходящих за рамки собственных сетей.[16]

Кибербезопасность в Венгерских силах обороны

В Венгрии защита от киберугроз и определение киберпространства как театра военных действий появилось в стратегических документах еще в 2012 году. В 2018 году киберпространство, как автономный театр военных действий, было включено в венгерское законодательство (раздел 80 Закона CXIII 2011 г.). Направления и условия развития венгерских военных киберспособностей изложены в Национальной военной стратегии (2012 г.), Национальной стратегии кибербезопасности (2013 г.), Концепции кибербезопас-

[14] "Wales Summit Declaration," *NATO e-Library*, September 5, 2014, articles 72 and 73, https://www.nato.int/cps/en/natohq/official_texts_112964.htm.

[15] "Warsaw Summit Communiqué," *NATO e-Library*, March 29, 2017, articles 70 and 71, https://www.nato.int/cps/en/natohq/official_texts_133169.htm.

[16] Susan Davis, "NATO in the Cyber Age: Strengthening Security & Defence, Stabilising Deterrence," NATO Parliamentary Assembly, April 18, 2019, pp. 4-6, www.nato-pa.int/download-file?filename=sites/default/files/2019-04/087_STC_19_E%20-%20NATO.pdf.

ности Венгерских сил обороны (2013 г.), вышеупомянутых Варшавских обязательствах, Программе развития Зриньи до 2026 года. В Венгрии защита от киберугроз и определение киберпространства как театра военных действий появилось в стратегических документах еще в 2012 году. В 2018 году киберпространство как автономный театр военных действий было включено в венгерское законодательство (раздел 80 Закона CXIII 2011 г.). Направления и условия развития венгерского военного киберпотенциала изложены в Национальной военной стратегии (2012 г.), Национальной стратегии кибербезопасности (2013 г.), Концепции кибербезопасности Венгерских сил обороны (2013 г.), вышеупомянутых Варшавских обязательствах, Программе развития Зриньи до 2026 года.

Национальная военная стратегия определила «создание способностей для сетевой войны» как одну из основных целей, которую должны достичь Силы обороны Венгрии. С одной стороны, компьютерно-сетевая война направлена на то, чтобы повлиять на работу сетевых ИТ-систем противной стороны, ухудшить их работоспособность и сделать невозможной работу, а с другой стороны, она направлена на поддержание функционирования наших собственных аналогичных систем.[17] График создания этих кибервозможностей был определен в Концепции кибербезопасности Венгерских сил обороны. В этом документе первоначальный уровень возможностей кибербезопасности должен быть достигнут до 2014 года, базовый уровень способностей для обеспечения кибербезопасности – в период с 2014 по 2016 год, а полные способности для кибербезопасности – после 2016 года. Концепция направлена, *среди прочего*, на защиту жизненно важных компонентов информационной системы, снижение их уязвимости и как можно более быстрое устранение потенциального ущерба.

Разработки в области кибербезопасности, инициированные Силами обороны Венгрии, составляют неотъемлемую часть программы оборонной политики. В рамках этой программы был создан Центр ВСО менеджмента электронных инцидентов. Кроме того, в Силах обороны Венгрии могут потребоваться дальнейшие организационные и функциональные изменения для создания единой системы кибербезопасности. С этой целью также следует уточнить тип организаций по кибербезопасности для отдельных командных уровней. Основная задача в области кибербезопасности – сократить время реакции и повысить эффективность разведки.

На сегодняшний день большинство задач по кибербезопасности Венгерских сил обороны выполняет Военная служба национальной безопасности

[17] По словам Хейга и Вархеги, «компьютерно-сетевая война включает в себя следующие действия: картирование структуры компьютерных сетей; изучение иерархических и операционных функций на основе характеристик их трафика; регистрация содержимого потока данных в сети; вводящая в заблуждение, подрывная деятельность в сетях; изменение и уничтожение содержания программ и данных целевых объектов, а также вопросы защиты от аналогичных действий противостоящей стороны».

(ВСНБ). В последние годы в исполнение Инструкции Минобороны № 85/2014 ВСНБ инвестировала в развитие разведывательных способностей и способностей, позволяющих осуществлять менеджмент киберинцидентов.

На парламентских слушаниях в 2019 году начальник Генерального штаба указал, что в ближайшем будущем предусматривается развитие киберспособностей (которых в то время не было). В 2020 году правительство определило области в рамках киберспособностей и операций Венгерских сил обороны, которые необходимо применять или развивать, а парламент добавил к Закону о национальной обороне особые правила, касающиеся военных операций в киберпространстве.[18]

Хотя подробности не являются полностью общедоступными, оборонный бюджет на 2020 год показывает, что киберразвитие вооруженных сил является основным приоритетом.

Сценарий гибридной атаки против Венгрии

Само собой разумеется, что за последние десять лет на национальном уровне был достигнут значительный прогресс в области киберзащиты и безопасности. Однако мы остаемся относительно беззащитными и уязвимыми для хорошо структурированной и скоординированной серии кибератак. По словам Фехера, эти атаки могут привести к

> наиболее опасному курсу действий врага, когда агрессор проводит гибридные операции полного спектра, и он может найти достаточно сторонников для борьбы с центральной властью, таким образом удерживая конфликт ниже порога статьи 5. При скрытой поддержке Сил специальных операций и конвенциональных сил противник может достичь фундаментальной внезапности, парализовать систему командования и управления, успешно бороться с венгерскими силами безопасности и установить функциональную альтернативную политическую власть на оккупированных территориях. В этой ситуации Венгрия вынуждена бороться без официальной помощи НАТО на оккупированных или неоккупированных территориях.[19]

Основываясь на этом предположении и тезисе д-ра Ласло Ковача и д-ра Чаба Краснаи о сценарии кибератаки против Венгрии, я хотел бы представить процесс эскалации, который вполне возможен сегодня (фиг. 2).

Результаты

10 декабря 2019 года Европейский совет принял заключения, устанавливающие приоритеты и руководящие принципы сотрудничества ЕС в противо-

[18] Prime Minister's Office, *T/8029th Bill proposal* (12 November 2019), 5, 21-22, https://www.parlament.hu/irom41/08029/08029.pdf.

[19] Feher, "Hungary's Alternative to Counter Hybrid Warfare."

действии гибридным угрозам и для повышения устойчивости к этим угрозам. В заключениях содержится призыв к применению комплексного подхода к противодействию гибридным угрозам, работающего во всех соответствующих секторах политики более стратегическим, скоординированным и согласованным образом.

В случае Венгрии контроль над ДИВЭ, поддерживающее и активно участвующее население, адекватная военная мощь, эффективная разведка и контрразведка, а также повышение киберустойчивости, по-видимому, являются соответствующими приоритетами, где устойчивость определяется как «способность подготовиться к изменяющимся условиям и адаптироваться к ним, противостоять сбоям и быстро восстанавливаться…, [и] включает способность противостоять преднамеренным атакам, авариям или естественным угрозам или инцидентам и восстанавливаться после них».[20]

Киберустойчивость – это способность субъекта противостоять, реагировать и восстанавливаться после киберинцидентов, обеспечивая непрерывность его работы.[21] Стратегические кибератаки могут быть нацелены на критически важную инфраструктуру и коммунальные предприятия страны, в то время как оперативные кибератаки направлены против вооруженных сил противника.

В то же время кибератаки – это тип информационных операций в рамках информационной войны, направленные на «коррумпирование, опровержение, деградацию и использование информации и информационных систем и процессов противника, одновременно защищая конфиденциальность, целостность и доступность своей собственной информации».[22]

Потенциал в информационной сфере жизненно важен для государства, чтобы подготовить граждан к негативному влиянию врага, сохранить или восстановить взаимодействие между государством и народом и положить конец ложному чувству безопасности граждан.

Согласно интерпретации НАТО, устойчивость на национальном уровне – это сочетание готовности гражданского населения и военного потенциала.[23] Это означает, что мы должны решать следующие задачи: повышение осведомленности общества в области информационной безопасности;

---

[20] “Resilience,” Glossary, NIST Information Technology Laboratory, Computer Security Resource Center (source: NIST SP 800-53 Rev. 4), https://csrc.nist.gov/glossary/term/resilience.

[21] Kjell Hausken, “Cyber Resilience in Firms, Organizations and Societies,” *Internet of Things* (2020), 100204, https://doi.org/10.1016/j.iot.2020.100204.

[22] Anil Chopra, “Cyber Warfare a Key Element of Multi Domain Wars – Time to Push India,” *Air Power Asia*, June 3, 2020, https://airpowerasia.com/2020/06/03/cyber-warfare-a-key-element-of-multi-domain-wars-time-to-push-india/

[23] Gustav Pétursson, “NATO’s Policy on Civil Resilience: Added Value for Small States?” SCANSE Research Project, Policy brief no. 5 (26 June 2018): 2, http://ams.hi.is/wp-content/uploads/2018/06/NATO%C2%B4s-Policy-on-Civil-Resilience-Added-Value-for-Small-States.pdf.

I.	Кибератака (первая фаза возможной гибридной атаки – кибератака)
I.1. Психологические операции	1. Запугивание: новости о предполагаемой слабости венгерской киберзащиты появляются в блоге, поддерживаемом иностранной секретной службой. 2. Распространение: новости, появившиеся в блоге, распространяются в социальных сетях, достигая десятки тысяч пользователей. 3. Обмен. Благодаря обмену через псевдопрофили, созданные иностранными разведывательными службами, новости появляются в большем потоке новостей и распространяются дальше. 4. Освещение: из-за большого количества публикаций бульварная пресса также начинает освещать эту тему, и вскоре она становится темой и в уважаемых СМИ.
I.2. Эффектные атаки	1. Проводятся атаки с перегрузкой против определенных правительственных веб-сайтов, в результате чего некоторые услуги становятся недоступными в течение нескольких часов. 2. Взламываются веб-сайты некоторых муниципальных ведомств и служб поддержки, и на их главных страницах появляются сообщения с угрозами Венгрии. 3. В Интернете появляются базы данных, содержащие персональные данные десятков тысяч граждан Венгрии.
I.3. Влияние на политику	1. В случае утечки типа Wikileaks электронные письма государственных органов публикуются под заголовком HunLeaks; международная пресса начинает их анализировать. 2. «Венгерский Сноуден» передает секретные документы расследующему журналисту. Их анализирует международная команда журналистов. 3. Расследование, заказанное в результате предыдущих атак, обнаруживает сложное вредоносное ПО в ИТ-системе поставщика общественных услуг. Целью вредоносного ПО является получение данных. Согласно отчету о расследовании, вредоносная программа работает не менее двух лет.
I.4. Инфраструктурные атаки	1. Атаки на телекоммуникации. Большинство телекоммуникационных услуг становятся недоступными. Государственные коммуникации также затруднены. Координация защиты замедляется и блокируется. 2. Атаки на финансовую систему: Интернет-банкинг приостановлен; международные финансовые операции также приостановлены.

	3. Нападения на электроснабжение и транспорт: происходят отключения электроэнергии на районном уровне; транспорт парализован.
II. Агрессор осуществляет полный спектр гибрид-ных операций	Агрессор проводит комбинацию специальных и конвенциональных военных операций, использует агентов разведки, политических провокаторов, влияние средств массовой информации, экономическое запугивание, доверенных и подставных лиц, военизированные формирования, террористов и криминальных элементов. Агрессор может добиться фундаментальной неожиданности, парализовать систему командования и управления, успешно бороться с венгерскими силами обороны и безопасности и установить функционирующую альтернативную политическую власть на оккупированных территориях. В этой ситуации Венгрия вынуждена бороться без официальной помощи НАТО на оккупированных или неоккупированных территориях.

	Развитие устойчивости на национальном уровне	Развитие устойчивости на уровне ВСО
I. Гибридная атака	Назначение национального координатора по вопросам устойчивости и гражданской готовности, определение национальных задач, органов и организаций ответственные за их выполнение и участвующие в их выполнении, а также процедуры сотрудничества. Администрация обороны кажется подходящей системой для обеспечения полного сотрудничества между государственными органами.	Реализация предложенного проекта (фигура 1), чтобы достичь желаемой цели (конечное состояние), защита страны за счет повышения устойчивости к гибридным атакам. На фигуре указаны инструменты национальной мощи для достижения каждого результата.
II. Кибератака	Повышение осведомленности об информационной безопасности в обществе, усиление организаций киберзащиты, создание альтернативных, аварийных инфраструктур, усиление набора инстру-	Основная задача ВСО – решать информационные проблемы комплексным образом: как быстро получать и обрабатывать информацию и интегрировать ее в цикл принятия решений, так и контролировать

	ментов для скоординированной централизованной киберзащиты, укрепление партнерских отношений между административной, деловой и научной сферами.	нарратив о конфликте в информационном пространстве. Необходимо создать оперативные способности в киберпространстве и их интеграцию в военное планирование и исполнение.

Фигура 2: Возможная гибридная атака на Венгрию и обеспечение устойчивости.

укрепление организаций киберзащиты, создание альтернативных, аварийных инфраструктур (элементов); усиление инструментария для скоординированной централизованной защиты; укрепление партнерства между административной, деловой и научной сферами; повышение устойчивости ВСО к гибридным атакам, включая кибератаки, путем выполнения предложений в этой статье.

Чтобы обеспечить устойчивость к киберугрозам, ВСО должны уметь решать информационные проблемы комплексным образом: как для быстрого получения и обработки информации, так и для интеграции ее в цикл принятия решений, а также для управления нарративами о конфликте в информационном пространстве.

Отказ от ответственности

Выраженные здесь взгляды являются исключительно взглядами автора и не отражают точку зрения Консорциума оборонных академий и институтов изучения безопасности ПрМ, участвующих организаций или редакторов Консорциума.

Об авторе

Андраш **Хугик**, доктор военных наук, полковник полиции в отставке, главный советник венгерской полиции. Он инженер, экономист, политолог. Он бывший советник ГУАМ, ОБСЕ, МППЕС и Совместного механизма расследований ООН и ОЗХО. Прежде чем присоединиться к этим международным организациям, он служил в военной разведке, службе внутренней безопасности венгерских правоохранительных органов и в контртеррористическом центре Венгрии. E-mail: seniorhugyik@gmail.com.

Connections: The Quarterly Journal
ISSN 1812-1101, e-ISSN 1812-2973

Ш. Дзебисашвили, С. Калашиани, И. Габриадзе, Р. Берадзе, & М. Эджибия, *Connections QJ* 19, № 4 (2020): 45-67
https://doi.org/10.11610/Connections.19.4.03

Рецензированная статья

Российский экономический след и его влияние на демократические институты в Грузии

Шалва Дзебисашвили,[1] Сузана Калашиани,[2] Ираклий Габриадзе,[1] Резо Берадзе и Мириан Эджибия

[1] *Университет Грузии, https://www.ug.edu.ge/en*

[2] *Международная школа экономики при Тбилисском государственном университете, https://iset.tsu.ge/*

Резюме: В данной статье заново рассматривается пресловутая концепция «Энергетической Империи», сформулированная Анатолием Чубайсом, и делается попытка выявить инструменты и способы экономического влияния России в Грузии, которые приводят к формированию так называемого российского экономического следа в Грузии, который, в свою очередь, эффективно используется Кремлем в качестве мощного инструмента для злонамеренного политического влияния и давления. Проблема во многом связана со способностью молодых и хрупких демократий создавать устойчивые политические системы и институты, сдерживать давление и поддерживать необратимый процесс демократических преобразований. Анализ основных секторов национальной экономики Грузии показывает критическую зависимость основных секторов от компаний, управляемых Россией, а также растущий совокупный вес влияния России на всю национальную экономику. Предварительные результаты отраслевого анализа дополняются регрессионной моделью, применяемой для проверки корреляции между динамикой демократического институционального развития и выбранной экономической переменной, то есть экспортом в Россию.

Ключевые слова: влияние России, экономический след, Грузия, политические институты, экономическая инфильтрация, захват государства.

Введение

В стремлении превратиться в глобальный центр силы и обеспечить господство на постсоветском пространстве, Россия применяет концепцию «ближнего зарубежья» или исключительной сферы влияния, которая нашла широкое признание в политической и экономической элите России задолго до установления режима Путина, когда в самом начале своего правления он играл с идеей дружеских отношений с Западом.[1]

Концепция «энергетической империи», первоначально разработанная Анатолием Чубайсом, со временем превратилась в хорошо функционирующую модель, в которой торговля газом и нефтью приобрела не только экономическое, но и политическое значение и позволила Москве оказывать влияние в странах-получателях, извлекать выгоду из этого и проникать в другие секторы их национальной экономики.[2] Многочисленные исследования, проведенные в Европе, доказали, что усиление политического влияния было напрямую связано с явлением первоначального «позитивного экономического сотрудничества», превращавшегося в источник негативной и злонамеренной силы.[3] Грузия, страна, переживающая бурные демократические преобразования, все еще далека от стабильных и устойчивых демократических институтов, способных продолжать политическое развитие и обеспечивать функциональную стабильность, несмотря на разрушительное внешнее вмешательство. Поэтому очень важно изучить и выявить экономические основы политического влияния России и его общие модели, которые, как было продемонстрировано во многих случаях, предполагают доминирование в ключевых секторах национальной экономики, через которое становится возможным проникнуть, «заразить» и ослабить политические институты, что в конечном итоге позволяет Кремлю оказывать значительное влияние (осуществлять захват государства) на процесс принятия по-

---

[1] Сергей Караганов, «Россия вынуждена защищать свои интересы железной рукой», *Россия в глобальной политике*, 3 июня 2014 г., http://globalaffairs.ru/pubcol/Rossiya-vynuzhdena-zaschischat-svoi-interesy-zheleznoi-rukoi-16460; Эдуард Понарин и Борис Соколов, «Глобальная политика глазами российской элиты», *Россия в глобальной политике*, 11 ноября 2014 г., https://globalaffairs.ru/articles/globalnaya-politika-glazami-rossijskoj-elity/; Иван Крастев, «Чего и почему хочет Россия?» *Россия в глобальной политике*, 3 августа 2014 г., https://globalaffairs.ru/articles/chto-hochet-rossiya-i-pochemu/; Дмитрий Тренин, «Россия в СНГ: сфера интересов, а не сфера влияния», Московский Центр Карнеги, 9 февраля 2010 г., https://carnegie.ru/proetcontra/?fa=40690.

[2] Fiona Hill, *Oil, Gas and Russia's Revival* (London: The Foreign Policy Center, September 2004), 23, https://www.brookings.edu/wp-content/uploads/2016/06/20040930.pdf; Анатолий Чубайс, «Миссия России в XXI веке», *Независимая газета*, 1 октября 2003 г., https://www.ng.ru/ideas/2003-10-01/1_mission.html.

[3] Heather A. Conley, James Mina, Ruslan Stefanov, and Martin Vladimirov, *The Kremlin Playbook: Understanding Russian Influence in Central and Eastern Europe* (Washington, DC: Center for Strategic and International Studies, 2016), v.

литических решений на национальном уровне (делая его более пророссийским). В конце концов, намеченные политические институты и сама система становятся похожими на российские, характеризующимися олигархическим правлением и упадком демократической культуры. Не следует забывать, что Грузия, страна, которая энергично стремилась к членству в ЕС и НАТО, постоянно сталкивается с необходимостью повышения своей институциональной устойчивости, при этом ЕС уделяет особое внимание диверсификации экономики и энергетическим секторам, а НАТО подчеркивает, что странам-партнерам необходимо повышать устойчивость институтов, способных противостоять внешнему давлению и принуждению.[4]

Это исследование направлено на достижение полного понимания сложности российского экономического следа в Грузии и его распределения среди основных секторов экономики. Будут определены ключевые экономические игроки (предприятия) в каждом секторе и будет рассмотрена их политическая и экономическая зависимость от России, что, будучи агрегированным по секторам, даст более широкую картину экономического влияния (следа) России в каждом секторе и национальном хозяйстве в целом. Кроме того, основные переменные экономического влияния России будут предметом корреляционного анализа с силой демократических институтов в попытке установить доказательства моделей взаимозависимости (большее влияние ведет к упадку демократических институтов).

Аналитическая модель и методология

Использование средств экономической экспансии в политических целях – устоявшаяся черта российской внешней политики. Поскольку между контролируемым государством и частным бизнесом, часто переплетающимися в России, мало различий, крупномасштабные прямые инвестиции за границу с высокой вероятностью скрывают за собой политические интересы государства. Помимо определения картины присутствия России в ряде секторов экономики через доли в оборотах, ВВП, экспорте и прямых инвестициях, мы более подробно рассмотрим природу и источники финансового капитала, структуру и форму собственности бизнеса в каждом соответствующем секторе. Из-за небольшого размера экономики Грузии в некоторых секторах наблюдается сильная тенденция к монополизации, что позволяет

[4] European Commission, “Eastern Partnership – 20 Deliverables for 2020: Bringing Tangible Results for Citizens,” 2–3, accessed July 15, 2020, https://ec.europa.eu/neighbourhood-enlargement/sites/near/files/eap_deliverables_factsheet_2017.pdf; “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,” *NATO Press Releases*, July 11, 2018, https://www.nato.int/cps/en/natohq/official_texts_156624.htm; “Warsaw Summit Communiqué, Issued by the Heads of State and Government Participating in the Meeting of the North Atlantic Council in Warsaw 8-9 July 2016,” *NATO Press Releases*, July 9, 2016, https://www.nato.int/cps/en/natohq/official_texts_133169.htm.

нескольким компаниям доминировать в целых секторах, диктовать «правила поведения» и, следовательно, прямо или косвенно оказывать влияние на политиков, связанных с деловой деятельностью в этих отраслях.

Таким образом, степень важности каждого сектора для национальной экономики будет оцениваться через показатели, основанные на его доле в национальном ВВП, занятости, прямых иностранных инвестициях (ПИИ) и экспорте. Кроме того, мы включаем в анализ такие экономические области, как энергетика, связь и транспорт, которые считаются критически важными из-за их стратегической значимости для Грузии, не в последнюю очередь с точки зрения безопасности. После определения агрегированного отраслевого индекса порог в 4 % указывает, заслуживает ли конкретный сектор дальнейшего исследования. Секторы с индексом выше 4 % составляют почти 80 % национальной экономики, тогда как восемь секторов с индексом ниже 4 % имеют лишь маргинальный эффект в 2,3 %. Поэтому только в секторах с рейтингом 4 % и выше крупные компании были включены в короткий список и разделены на две группы: Категория-1 и Категория-2. Компании с годовым доходом более 100 млн лари и стоимостью активов более 50 млн лари относились к первой категории, а компании с доходом от 20 до 100 млн лари и стоимостью активов от 10 до 50 млн лари ко второй. Затем компании из обеих категорий были помечены цветом: черный (сильное российское влияние), красный (частичный риск российского влияния) и зеленый (отсутствие российского влияния) в соответствии со степенью политического или финансового влияния России, оцениваемого на основе набора показателей, таких как российское гражданство (со)владельца, доступность и прозрачность деловой информации, источник финансового капитала, оффшорная регистрация и т.д. Доля «черных» и «красных» компаний в каждом секторе позволила оценить примерный масштаб российского следа, что впоследствии позволило сформировать всю картину экономического влияния России на макроэкономическом уровне, то есть на национальную экономику. Наконец, была введена регрессионная модель с возможностью отслеживать взаимозависимость экономических переменных российского влияния (таких как экспорт, прямые инвестиции и денежные переводы) с силой внутренних (в Грузии) демократических институтов, оцениваемых на основе показателей Freedom House и Всемирного банка.

Основные секторы экономики

Выявление основных секторов позволяет нам анализировать национальную экономику с макроэкономической точки зрения и определять истинный размер и акцент российского влияния на экономику Грузии.[5] Из списка

[5] "NACE Rev. 2 – Statistical Classification of Economic Activities," Eurostat, доступ на 5 февраля 2020, https://ec.europa.eu/eurostat/web/nace-rev2; "Statistical Information," National Service of Statistics, по состоянию на 8 сентября 2019, www.geostat.ge/ka.

14 секторов экономики первыми будут выбраны те, доля которых в национальном ВВП превышает 4 %, и добавив доли секторов в национальной занятости, ПИИ и экспорте, будет создан агрегированный отраслевой индекс, позволяющий получить гораздо больше детальное (зависящее от релевантности) ранжирование наиболее критических секторов.

При расчете агрегированного индекса применяется тот же порог в 4 % для рассматриваемых секторов, и он основан на данных за 2003–2018 годы. Результаты не являются неожиданными, так как производство, транспорт, торговля и строительство занимают лидирующие позиции во всех отношениях. Соответственно, следующий этап исследования направлен на измерение российского присутствия в ведущих секторах национальной экономики и вклада России в основные экономические показатели, такие как прямые иностранные инвестиции, экспорт и количество посетителей как основных движущих сил и индикаторов роста (или снижения) российского экономического влияния.

Российский след в экономике Грузии

В этом разделе более подробно рассматриваются несколько макроэкономических показателей, с помощью которых становится очевидной динамика и направление российской экономической деятельности в Грузии. К ним относятся размер и структура (секторальные получатели) прямых российских инвестиций. Кроме того, будут проанализированы характер и динамика грузинского экспорта в Россию, а также количество российских посетителей в Грузии, чтобы оценить степень уязвимости Грузии перед потрясениями, исходящими из России (например, политически мотивированное эмбарго).

Прямые иностранные инвестиции

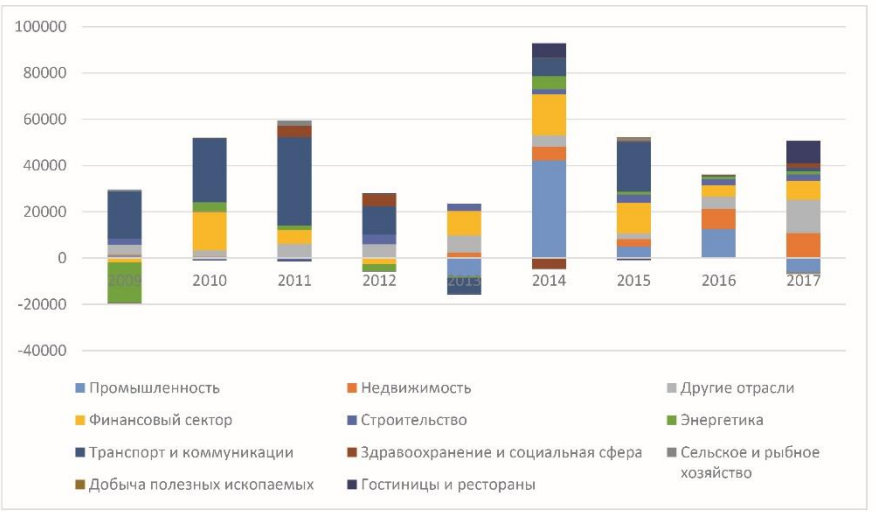
Похоже, российские ПИИ следуют общей модели поведения (изменчивости) всех ПИИ, хотя с 2014 г. они демонстрируют общую тенденцию роста (фиг. 1). Следует отметить, что инвестиции, исходящие от офшорных компаний, составляют значительную долю от общего объема прямых иностранных инвестиций, и, следовательно, невозможно определить первоначальный источник. С большой долей вероятности, российские инвесторы активно используют офшорную деятельность для перемещения финансовых капиталов в Грузию, тем самым доводя реальный размер российских инвестиций до гораздо более высокой отметки.

Распределение по отраслям российских инвестиций показано на фиг. 2, где видно, что наибольшему влиянию подверглись финансы (27 %), производство (17 %), транспорт и связь (8 %) и недвижимость / строительство (8 %).

Таблица 1: Доля сектора и агрегированный индекс.

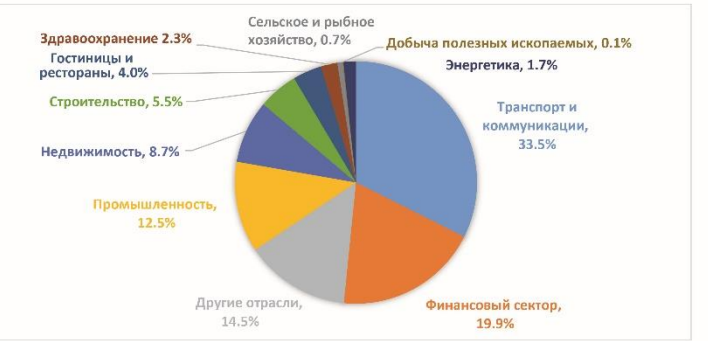
Доля сектора в ВВП	**%**	**Доля сектора в экспорте**	**%**	**Доля сектора в ППИ**	**%**	**Агрегированный индекс**	**%**
Оптовая и розничная торговля	19.4	**Промышленное производство**	43.8	Транспорт	23.2	**Промышленное производство**	19.3
Сельское, лесное и рыбное хозяйство	11.8	Оптовая и розничная торговля	28.7	Электроснабжение, газ, пар и кондиционирование	13.0	Добыча полезных ископаемых и разработка карьеров	3.0
Промышленное производство	11.6	Транспорт	12.7	**Промышленное производство**	11.6	Торговля	17.2
Транспорт	9.4	Добыча полезных ископаемых и разработка карьеров	6.1	Финансовая и страховая деятельность	11.2	Сельское, лесное и рыбное хозяйство	14.2
Строительство	9.1			Строительство	9.6	Транспорт и коммуникации	13.7
Здравоохранение и социальная работа	6.7			Операции с недвижимостью	9.2	Строительство	6.2
Операции с недвижимостью	6.3			Гостиницы и рестораны	6.9	Электроснабжение, газ, пар и кондиционирование	4.9
Образование	5.5					Финансовая и страховая деятельность	4.1
Другие услуги	5.0						

Фигура 1: Доля России в общем объеме прямых иностранных инвестиций в Грузию.



Фигура 2: Распределение российских ПИИ в Грузии по секторам (в 1000 долларов США).

Еще раз подчеркнем, что из-за широко распространенной практики инвестирования через офшорные компании доля отраслевого распределения реальных российских инвестиций может иметь совсем иную картину. Что касается среднего отраслевого распределения российских ПИИ в период с 2009 по 2017 год, на фиг. 3 показана аналогичная тенденция, когда самый большой кусок пирога занимают транспорт и связь (ТС), финансовый сектор, производство и недвижимость.



Фигура 3: Средняя доля в ПИИ (2009-2017).

Экспорт в Россию

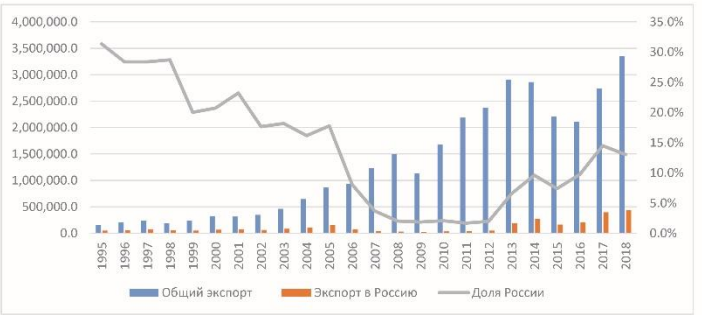
Как ясно видно из динамики экспорта в Россию (фиг. 4), Грузия снова приближается к точке, когда объемы экспорта достигли своего рекордного уровня (15 %), как и в 2006 году, когда Россия, руководствуясь политическими мотивами, запретила грузинские товары и ввела полное эмбарго. Нельзя исключать возможность подобных решительных действий с соответствующими тяжелыми последствиями для экономики Грузии.

Существует несколько секторов, которые доминируют в грузинском экспорте в Россию, а обрабатывающая промышленность (рост 48 %) и сельское хозяйство продемонстрировали исключительные темпы роста, заняв львиную долю в общем экспорте, как показывает статистика распределения экспортных секторов на фиг. 5.

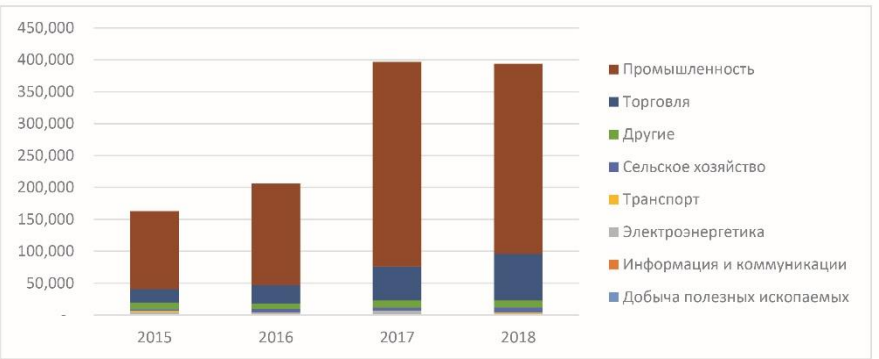
Гости из России – туризм

Растущая зависимость экономики Грузии, и в частности туризма, от российских гостей хорошо видна по устойчивому росту туристов с 8,1 % (доля от общего числа) в 2011 году до 19,5 % в 2018 году.

Учитывая высокую подверженность российского туризма политическим предпочтениям Кремля, то есть возможность туристического бойкота страны-мишени, Грузия определенно приближается к точке, после которой карательные меры России будут иметь серьезные негативные последствия для грузинской экономики. Ограничения на поездки, введенные после так называемой «ночи Гаврилова» в июне 2019 года, сильно ударили по туристическому сектору и еще раз подтвердили стандартную мудрость недоверия к России при открытии для экономического сотрудничества.



Фигура 4: Экспорт в Россию (тысячи долл. США).



Фигура 5: Экспорт в Россию по отраслям (2015-2018 гг., 1000 долл. США).

Фигура 6: Гости из-за границы (в т.ч. из России).

В заключение мы можем считать, что ключевые макроэкономические показатели грузинской экономики, такие как прямые иностранные инвестиции, экспорт и туризм, показывают неуклонно растущую экономическую зависимость от России. Официально отслеживаемые потоки финансового капитала из России направляются в основном в секторы транспорта и коммуникаций, финансов и обрабатывающей промышленности Грузии. Это довольно тревожно, поскольку сектор Т&К официально признан стратегически важным. Финансовый сектор до сих пор пользовался гораздо более высокой степенью «свободы действий» по сравнению с ужасными условиями российского финансового сектора, напрямую зависящими от политической доброй воли Кремля. Хотя доля грузинского экспорта в Россию в общих объемах экспорта достигла уровня 2006 года, абсолютное количество и объем товаров, экспортированных в Россию, намного превышают показатели 2006 года. Таким образом, риск повторного применения экономических санкций в политических целях становится еще больше, с гораздо большей вероятностью оказания политического давления и с большими опасениями негативных социально-экономических последствий для Грузии.

Анализ основных компаний, связанных с сектором

Очевидно, что ограниченный объем статьи не позволит охватить все действующие предприятия в Грузии и провести существенный, глубокий анализ, чтобы выявить финансовые источники, существующий контроль и сильно запутанные механизмы влияния в каждом секторе. Поэтому был выбран более ограниченный, но действенный подход путем выявления крупных компаний *Категории-1* и *Категории*-2 в каждом секторе экономики.[6]

Компании, принадлежащие к *категории 1*, должны были соответствовать следующим критериям: годовой доход более 100 млн лари и стоимость активов более 50 млн лари. В *категорию 2* входят все компании с доходом от 20 до 100 млн лари и стоимостью активов от 10 до 50 млн лари. Небольшие предприятия были исключены из анализа, несмотря на их значительное количество, поскольку основное внимание уделялось компаниям, занимающим доминирующее положение в соответствующих секторах экономики. Таким образом, исследование может дать объективно ограниченную картину российского «следа» в крупных компаниях наиболее важных секторов национальной экономики. Тем не менее, в значительной степени результаты можно обобщить и считать действительными для остальных компаний, то есть для всего сектора. Во-вторых, компании из обеих категорий подверглись цветовому кодированию и были окрашены в черный цвет (сильное российское влияние), красный (риск или частичное российское влияние) и зеленый (отсутствие российского влияния) на основе набора показателей степени российского политического или финансового

[6] "Useful Information," Service of Financial Accounting, Accountability, Monitoring and Audit," n.d., https://saras.gov.ge/.

влияния, включая российское гражданство (со)владельцев, доступность и прозрачность деловой информации, источник финансового капитала, оффшорную регистрацию и т.д. В конечном итоге цель этого раздела – рассчитать в процентных пунктах долю зависимых от России (черных и красных) компаний в основных секторах экономики, т.е. след России в национальной экономике.

Компании в 2017 году

Общее количество компаний в обеих категориях составляет 397 в Категории-1 и 312 в Категории-2 соответственно. Что касается товарооборота всей национальной экономики, то доля компаний обеих категорий в обороте составляет 37 %. Учитывая, что мы не включали в свой анализ более мелкие компании (категории 3 и 4), реальным оборотом компаний, «находящихся под влиянием России», следует считать не просто упомянутые 37 %, а гораздо более высокий процент. Из 397 компаний 110 (28 %) являются либо «черными», либо «красными». Это весьма тревожная цифра, указывающая на то, что почти треть крупных предприятий в Грузии, которые в той или иной степени находятся под влиянием России, дают 9,2 % от оборота национального бизнеса и в значительной степени доминируют в горнодобывающей (63,4 %), энергетической (36,6 %) и сельскохозяйственной (24,7 %) отраслях (см. Таблицу 2).

Таблица 2. «Черные» и «красные» компании в национальной экономике 2017.

Секторы: красные и черные	Число	Доход, 2017, тыс.	Оборот сектора 2017, тыс.	Доля
Оптовая и розничная торговля	40	3,402,388	32,816,300	10.4 %
Энергетика (електричество, газ, пар и вентиляция)	10	1,077,826	2,943,600	36.6 %
Промышленность	21	764,329	8,532,100	9.0 %
Добыча полезных ископаемых	2	425,717	671,400	63.4 %
Транспортировка и хранение	11	244,178	4,699,500	5.2 %
Информация и коммуникации	6	240,913	1,657,700	14.5 %
Строительство	7	219,768	7,051,200	3.1 %

Сельское, лесное и рыбное хозяйство	5	105,192	425,900	24.7 %
Деятельность в сфере недвижимости	8	101,187	1,090,900	9.3 %
Всего	**110**	**6,581,498**	**71,740,300**	**9.2 %**

51 из 397 (13 %) «черных» компаний категорий 1 и 2 дают 4,7 % от общего оборота бизнеса, в значительной степени доминируют в горнодобывающей промышленности (63,4 %) и энергетике (27,7 %), и имеют значительную долю присутствия в транспорте и строительстве (таблица 3).

Таблица 3. «Черные» компании в национальной экономике, 2017 г.

Секторы: черные	Число	Доход, 2017, тыс.	Оборот сектора 2017, тыс.	Доля
Оптовая и розничная торговля	16	1,331,814	32,816,300	4.1 %
Энергетика (електричество, газ, пар и вентиляция)	7	815,995	2,943,600	27.7 %
Промышленность	13	438,095	8,532,100	5.1 %
Добыча полезных ископаемых	2	425,717	671,400	63.4 %
Транспортировка и хранение	6	240,913	1,657,700	14.5 %
Информация и коммуникации	3	61,844	7,051,200	0.9 %
Строительство	2	58,196	425,900	13.7 %
Сельское, лесное и рыбное хозяйство	2	24,863	1,090,900	2.3 %
Деятельность в сфере недвижимости			4,699,500	0.0 %
Всего	**51**	**3,397,436**	**71,740,300**	**4.7 %**

Компании в 2018

В 2018 году к Категории-1 или Категории-2 относились 414 компаний, что составляет 4 % роста по сравнению с 2017 годом. На их долю приходилось 34,2 % от общего оборота бизнеса (снижение на 2,8 %). Черные и красные компании (всего 114) дают 8,6 % от оборота национального бизнеса, что сопоставимо с данными 2017 года, хотя и с небольшим снижением (таблица 4). Черные компании (всего 55) составляют 4,5 % от общего оборота бизнеса и доминируют в горнодобывающем, энергетическом, транспортном и строительном секторах (таблица 5).

За период с 2017 по 2018 год в общей сложности 415 компаний были тщательно проверены, из которых 55 были закодированы как черные (полностью российское доминирование) и 59 как красные (подверженные риску или частично подверженные влиянию), что составляет 27,5 % от всех компаний 1-й и 2-й категорий (таблица 6).

Количество красных или черных компаний выросло со 110 в 2017 году до 114 в 2018 году. Из-за отсутствия информации об обороте в 2018 году для 34 крупных компаний из этого списка мы предполагаем, что средний уровень оборота будет таким же, как в 2017 году, и таким образом, их доля в общем обороте остается на уровне 9 % (Таблица 7).

Таблица 4. «Черные» и «красные» компании в национальной экономике, 2018.

Секторы: красные и черные	Число	Доход, 2018, тыс.	Оборот сектора 2018, тыс.	Доля
Оптовая и розничная торговля	42	4,052,831	37,409,500	10.8 %
Энергетика (электричество, газ, пар и вентиляция)	10	1,087,385	3,294,600	33.0 %
Промышленность	22	858,090	9,212,300	9.3 %
Добыча полезных ископаемых	3	453,276	7,171,300	6.3 %
Транспортировка и хранение	7	318,786	5,054,000	6.3 %
Информация и коммуникации	11	222,291	749,300	29.7 %
Строительство	6	214,555	1,275,300	16.8 %
Сельское, лесное и рыбное хозяйство	8	132,136	446,900	29.6 %
Деятельность в сфере недвижимости	5	107,873	1,750,800	6.2 %
Всего	**114**	**7,447,225**	**86,625,200**	**8.6 %**

Таблица 5. «Черные» компании в национальной экономике, 2018.

Секторы: красные и черные	Число	Доход, тыс.	Оборот сектора, тыс.	Доля
Оптовая и розничная торговля	18	1,702,435	37,409,500	4.6 %
Энергетика (электричество, газ, пар и вентиляция)	7	879,467	3,294,600	26.7 %
Промышленность	14	491,109	9,212,300	5.3 %
Добыча полезных ископаемых	3	453,276	749,300	60.5 %
Транспортировка и хранение	6	214,555	1,750,800	12.3 %
Информация и коммуникации	3	79,879	7,171,300	1.1 %
Строительство	2	61,441	446,900	13.7 %
Сельское, лесное и рыбное хозяйство	2	51,169	1,275,300	4.0 %
Деятельность в сфере недвижимости			5,054,000	0.0 %
Всего	**55**	**3,933,331**	**86,625,200**	**4.5%**

Таблица 6. Проверенные компании и отмеченные цветом.

Сектор	Зеленые	Красные	Черные	Всего
Деятельность, связанная с недвижимостью	13	6	2	21
Транспорт и хранение	22	11		33
Сельское, лесное и рыбное хозяйство	3	3	2	8
Добыча полезных ископаемых	2		3	5
Оптовая и розничная торговля	125	24	18	167
Строительство	55	4	3	62
Информация и коммуникации	7		6	13
Энергетика (электричество, газ, пар и вентиляция)	14	3	7	24
Промышленность	60	8	14	82
Всего	**301**	**59**	**55**	**415**

Таблица 7. Изменение оборота красных и черных компаний по годам.

Секаторы: красные и черные	Число 2017	Число 2018	Изме-нение	Доля 2017	Доля 2018	Изме-нение
Оптовая и розничная торговля	40	42	2	10.4 %	10.8 %	0.5 %
Энергетика (электричество, газ, пар и вентиляция)	10	10	0	36.6 %	33.0 %	-3.6 %
Промышленность	21	22	1	9.0 %	9.3 %	0.4 %
Добыча полезных ископаемых	2	11	9	63.4 %	29.7 %	-33.7 %
Транспортировка и хранение	11	7	-4	5.2 %	6.3 %	1.1 %
Информация и коммуникации	6	5	-1	14.5 %	6.2 %	-8.4 %
Строительство	7	3	-4	3.1 %	6.3 %	3.2 %
Сельское, лесное и рыбное хозяйство	5	8	3	24.7 %	29.6 %	4.9 %
Деятельность в сфере недвижимости	8	6	-2	9.3 %	16.8 %	7.5 %
Всего	**110**	**114**	**4**	**9.2 %**	**8.6 %**	**-0.6 %**

Среди 100 крупнейших компаний-экспортеров в Россию 23 компании в 2017 году относились к категории 1 или 2. Из этих 23, девять компаний черного (7) или красного цвета (2), т. е. 39 %, и представляют исключительно производственный (розлив в бутылки) сектор экономики.

- Сама *обрабатывающая промышленность* относится к рискованному сектору из-за того, что 22 компании имеют черно-красную цветовую маркировку, что составляет почти 9 % от общего оборота в секторе;
- В секторе *оптовой торговли* в 2017 году находились 42 черные и красные компании с долей в соответствующем общем обороте 10,4 % (3,4 млрд лари);
- Хотя в *агропромышленном секторе* было выявлено всего пять черно-красных компаний (2017 г.), их доля в отраслевом обороте составила 24,7 %;

- *Энергетический сектор*, являющийся стратегическим сектором в Грузии, представлен десятью компаниями с черным или красным кодом, что составляет 36,6 % (1,1 млрд лари) от общего оборота сектора;
- В другом стратегически важном секторе – *информации и коммуникациях* – всего шесть черных или красных компаний. Однако их общая доля в отраслевом обороте составляет более 14 %. Интересно, что в сфере мобильной связи российский «Билайн» контролирует 23,9 % рынка, что является значительной долей с учетом короткого периода выхода на местный рынок.[7]

Компании, находящиеся под полным или частичным российским влиянием, прочно занимают 9 % грузинского бизнеса. На первый взгляд это число кажется довольно низким; тем не менее, поскольку мы включили в наш анализ лишь ограниченное число компаний (категории 1 и 2), а более мелкие компании с уверенностью могли бы выявить большое количество красных и черных компаний, реальное присутствие России может быть еще больше. Доминирование России демонстрирует значительную динамику роста, если принять во внимание ведущие секторы экономики, и уже приблизилось к тревожному порогу. В некоторых секторах доля российского следа намного больше, чем в среднем по стране, и часто представлена несколькими компаниями (например, две компании в энергетическом секторе, контролирующие 25 %, и две компании в сельском хозяйстве с 18 %). Более того, почти во всех доминирующих секторах компании, «находящиеся под влиянием России», пользуются исключительной ролью естественных монополий, тем самым диктуя ценовые условия и полностью контролируя «правила поведения» в этом секторе. Таким образом, можно согласиться с тем, что 9 % национального товарооборота, находящегося под контролем России, можно принять как граничную линию, за которой начинается зона тяжелой и опасной экономической зависимости.

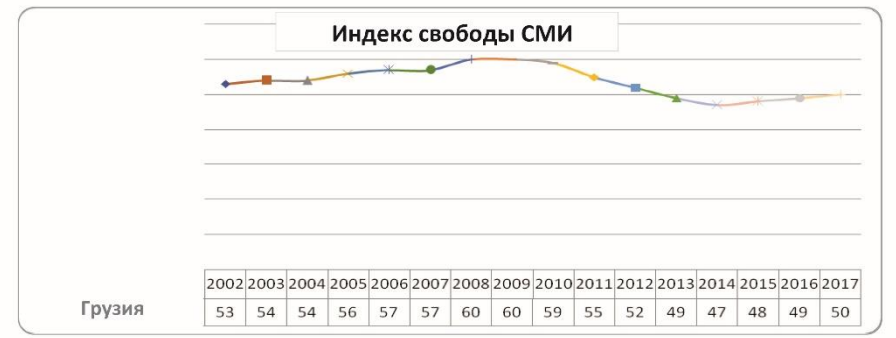
Анализ СМИ

Ввиду огромной важности свободных СМИ для общего развития демократической институциональной динамики, мы включаем краткий анализ медиа-сектора, его основных действующих субъектов и тенденций. Это позволяет нам понять глубину и серьезность политического влияния на сектор и установить связи с общей институциональной динамикой Грузии, часто движимой скрытыми и незаконными интересами определенных деловых или политических кругов.

По данным Freedom House, Грузия занимает лучшее место среди своих соседей в отношении свободы СМИ, с самым ниским рейтингом в 2008 году

[7] "Analytical Portal," National Commission of Communication, n.d., https://analytics.comcom.ge/.

и лучшим в 2014 году (см. фиг. 7).[8] Несмотря на это, с самым высоким показателем 47, Грузия по-прежнему отстает от стран Восточной Европы (индекс 30).



Фигура 7: Грузия в рейтинге индекса свободы СМИ.

В ходе анализа медиа-сектора нам удалось определить основных операторов теле- и радиовещания, их источники доходов, структуру собственности и динамику доли рынка в период с 2012 по 2018 год.[9] На основе предварительной оценки распределения доходов рынка для дальнейшего анализа были отобраны все субъекты СМИ, достигающие более 2 % доли рынка СМИ.[10] Из семи крупнейших телеканалов, компании *ТВ-Имеди*, которая напрямую связана с правящей партией и правительством, принадлежит 22,7 % медиарынка. Несмотря на то, что ей принадлежит менее 1 % рынка, еще одна телекомпания, *Media Union Objective*, была дополнительно выбрана из-за ее прямой и открытой деятельности, связанной с распространением российских нарративов и поддержкой пророссийских политических идей. Одним из ее основателей является генеральный секретарь пророссийской политической партии «Альянс патриотов» Ирма Инашвили. Доходы *Objective* росли в геометрической прогрессии с 2012 года (смена правительства в Грузии) по 2018 год со 134 000 лари до 1,9 млн лари, из которых 1,35 млн поступили от частных пожертвований. То же самое можно сказать и о радиовещании, где 11,6 % рынка принадлежит *Радио-Имеди*, а 0,4 % – *Радио-Объектив*. Что касается степени российского влияния, *ТВ-Имеди* было

[8] "Georgia," Freedom House, 2016, accessed July 29, 2020, https://freedomhouse.org/report/freedom-press/2016/georgia; "Georgia, Countries and Regions," Reporters without Borders, n.d., https://rsf.org/en/ranking.

[9] "Annual Reports," National Commission of Communication, n.d., https://comcom.ge/ge/the-commission/annual-report.

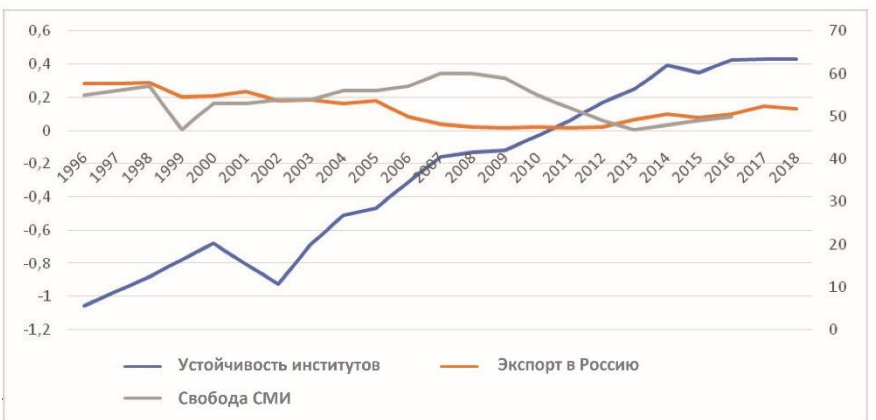
[10] "Broadcasting – Media Incomes by Enterprises," National Commission of Communication, May 28, 2020, https://analytics.comcom.ge/ka/statistics-share/?c=broadcasting&sid=757292&f=revenue&exp=tv&sid=757293.

классифицировано как «красное» из-за двойного (российского и британского) гражданства двух его владельцев, Ии Патарказшвили и Лианы Жмотовой. Другой игрок на медиарынке, MediaNetwork, получил ссуду от российского банка ВТБ в 2016 году, и поэтому также был обозначен как «красный».

Российский экономический след и демократические институты

В этом разделе представлена регрессионная модель, созданная для проверки зависимости демократического развития (институциональной силы) от российского экономического следа в Грузии. Мы будем использовать долю экспорта в Россию в общем экспорте в качестве ключевой объясняющей переменной, а силу демократических институтов и свободу СМИ в качестве зависимых переменных (фиг. 8). Для измерения свободы СМИ мы будем использовать критерий Freedom House,[11] а институциональную мощь – с помощью глобальных показателей качества управления Всемирного банка:[12]

- Гласность и подотчетность;
- Политическая стабильность;
- Эффективность управления;
- Качество нормативной базы;
- Верховенство закона;
- Борьба с коррупцией.



Фигура 8: Индекс свободы СМИ, институциональная устойчивость и экспорт в Россию.

[11] "Publication Archives," Freedom of the Press, Freedom House, n.d., https://freedomhouse.org/reports/publication-archives.

[12] World Bank, "Worldwide Governance Indicators," n.d., https://info.worldbank.org/governance/wgi/.

Как видно на фиг. 8, с 1996 года институциональное развитие в целом было положительным, за исключением видимого замедления в последние четыре года. Свобода средств массовой информации (прессы) также начала снижаться с 2015 года, а экспорт в Россию, близкий к нулю с 2006 по 2013 год, продемонстрировал быстрый рост на 13 % в 2018 году.

Выбранные институциональные переменные стандартизированы и варьируются от -2,5 до 2,5, причем более высокий результат указывает на лучшие институты. Чтобы измерить институциональную силу, мы рассчитали средний индекс всех шести факторов. Кроме того, шесть показателей были сгруппированы в три группы: первый и второй сформировали группу политических институтов; третий и четвертый определяли группу административных учреждений; а последние два касались юридических институтов. Что касается показателей свободы СМИ (прессы), мы использовали индекс Freedom House, который помещает страны в три уровня: уровень 1 для стран со свободными СМИ (с индексом от 0 до 30), уровень 2 для стран с частично свободными СМИ (от 31 до 60), и третий уровень стран без свободы СМИ (от 61 до 100).[13]

Применение регрессионной модели для проверки взаимосвязи между этими переменными дало следующие результаты. Регрессия в первом и втором столбцах включает в себя среднюю устойчивость институтов, как зависимую переменную и долю экспорта в Россию в общем экспорте, как управляющую переменную. Вторая регрессионная модель в строке 3 дополнительно включала ВВП с запаздыванием. Результаты регрессии указывают на отрицательную связь между экспортом в Россию и институциональным качеством. Регрессия в четвертой, пятой и шестой строках имеет в качестве зависимых переменных политические, административные и юридические институты. Как ясно видно, рост экспорта в России оказывает негативное влияние на административные и правовые институты и не влияет на политические институты. Что касается наличия свободы СМИ (прессы) в качестве зависимой переменной, шестой столбец не дает статистически значимой связи.

Следует отметить, что эта регрессионная модель имеет определенные ограничения, которые включают относительно небольшое количество наблюдений (23 для первых пяти зависимых переменных и 22 для шестой – свобода СМИ) и могут быть уравновешены большим периодом наблюдения и данными из других стран. Временные ряды и поперечные сечения позволят генерировать панельные данные, которые повысят качество и достоверность полученных результатов.

[13] “Publication Archives,” Freedom House.

Заключение

Способность государства поддерживать эффективные институты, которые могут противостоять внешнему (российскому) давлению, и минимизировать влияние Кремля в политическом, институциональном и экономическом плане, является важнейшим признаком стран-кандидатов на членство в ЕС или НАТО. Наличие свободной, диверсифицированной и стабильной экономической системы – это конечная цель экономического измерения стремления Грузии согласовать с ЕС свою практику в юридических, торговых, энергетических и социальных вопросах. Для достижения этой цели представленное здесь исследование было направлено на проверку достоверности обязательств Грузии, в частности путем изучения моделей российского влияния на демократические институты Грузии посредством углубленного анализа экономического следа России в стране. Он проводился в несколько этапов.

Таблица 8. Регрессионная модель.

Переменные	Экспорт	Отложенный ВВП	Константа	R-квадрат
(1) Институты	-0.0420*** (0.00826)		0.290** (0.131)	0.552
(2) Институты	-0.00529** (0.00249)	0.000460*** (2.19e-05)	-1.367*** (0.0839)	0.980
(3) политические	0.00304 (0.00412)	0.000299*** (3.63e-05)	-1.292*** (0.139)	0.856
(4) административные	-0.0124** (0.00483)	0.000503*** (4.25e-05)	-1.085*** (0.163)	0.949
(5) правовые	-0.00656* (0.00376)	0.000577*** (3.31e-05)	-1.725*** (0.127)	0.972
(6) свободная пресса	-0.236 (0.177)	-0.00449** (0.00184)	68.11*** (6.590)	0.288

В скобках стандартная ошибка
*** p < 0.01, ** p < 0.05, * p < 0.1

Первая цель заключалась в выявлении основных секторов экономики в стране и выявлении крупных компаний в каждом соответствующем секторе, полностью или частично подверженных влиянию России. Из восьми идентифицированных секторов (производство, торговля, сельское хозяйство, транспорт, связь, энергетика, строительство и финансы) российские финансовые вложения в основном направлялись в финансы, производство, строительство и связь. Однако следует напомнить, что статистика, показывающая ПИИ, охватывает лишь часть всех потоков российского капитала, инвестированного в Грузию, из-за возможности инвестиций через третьи

страны и офшорные компании. Как четко указано в Отчете о результатах за 2020 год, торговля с другими странами Восточного партнерства значительно сократилась из-за резких скачков продаж продукции российского производства в Грузии.[14]

Обрабатывающая промышленность на сегодняшний день является ведущей отраслью экспорта товаров в Россию. Серьезные вопросы возникают в связи с многочисленными проектами, запущенными в энергетическом секторе, поскольку они демонстрируют практически нулевую осуществимость и серьезные риски коррупции.[15] Как и в 2006 году, Грузия подошла к моменту, когда возможность российского эмбарго может серьезно ударить по национальной экономике, вызвав разрушительные последствия и создав условия для усиления политического давления со стороны Кремля. Точно так же экспоненциальный рост гостей из России резко увеличил долю российских туристов в общем числе туристов, и все больше подвергает туристическую отрасль российскому бремени. Почти треть (114 из 415) крупных грузинских компаний полностью или частично демонстрируют связи с Россией и дают в среднем 9,2 % национального делового оборота. В некоторых секторах серьезность доминирования компаний, связанных с Россией, вызывает тревогу (горнодобывающая промышленность – 63,4 %, энергетика – 36,6 %, сельское хозяйство – 24,7 %). Другие секторы, имеющие стратегическое значение, такие как информация и связь, показывают постоянно растущую степень влияния (14,5 %). Разработанная регрессионная модель, которая связывает три категории государственных институтов (политические, административные и правовые) с экспортом в Россию и национальным ВВП, выявила четкую статистическую зависимость между увеличением экспорта и снижением институциональной силы в Грузии, при этом никакого статистического воздействия на свободу СМИ установлено не было.

Общий вывод, сделанный из исследования, заключается в том, что Грузия уже достигла точки сильной экономической зависимости от России, которая чрезмерно непропорционально влияет на несколько ключевых отраслей национальной экономики и продолжает расширяться в некоторых секторах, имеющих стратегическое значение. Российский след, находящийся на уровне 9 % от оборота национального бизнеса, уже является красной линией, и статистические модели, отражающие взаимосвязь между ростом российского экономического влияния и снижением институционального качества, четко подтверждают упомянутый порог. Еще многое предстоит сделать, чтобы обратить вспять эту тенденцию и вернуть Грузию на четкий путь

[14] “Georgia’s Implementation of 20 Eastern Partnership Deliverables for 2020,” Assessment by Civil Society (Tbilisi: Georgian Institute of Politics, International Society for Fair Elections and Democracy, 2020), 49, http://gip.ge/georgias-implementation-of-20-eastern-partnership-deliverables-for-2020/.

[15] “Georgia’s Implementation of 20 Eastern Partnership Deliverables for 2020,” 78–89.

минимизации российского следа, приложив заслуживающие доверия усилия по повышению устойчивости как в экономическом, так и в политическом измерениях.

Отказ от ответственности

Выраженные здесь взгляды являются исключительно взглядами авторов и не отражают точку зрения Консорциума оборонных академий и институтов изучения безопасности ПрМ, участвующих организаций или редакторов Консорциума.

Об авторах

Шалва Дзебисашвили получил докторскую степень в Институте европейских исследований (IEE-ULB, Брюссель) в январе 2016 года. В 2008–2009 годах он успешно окончил магистратуру по исследованиям в области стратегической безопасности в Национальном университете обороны в Вашингтоне, округ Колумбия, и впоследствии занял должность старшего гражданского представителя Министерства обороны Грузии (советник по обороне) при представительстве Грузии в НАТО. С 2003 по 2012 год и с 2016 по 2019 год он занимал различные руководящие должности, связанные с оборонной политикой и планированием, в Министерстве обороны Грузии. Он доцент и руководитель программы международных отношений и политологии в Университете Джорджии, член различных грузинских неправительственных организаций и аналитических центров, таких как Гражданский совет по обороне и безопасности (ГСОБ) и Грузинский Центр стратегического анализа (ГЦСА). E-mail: kartweli@yahoo.de

Резо Берадзе имеет степень магистра экономики Международной школы экономики в Тбилиси, Грузия (МШЭТ) и степень магистра финансовой математики Университета Сассекса. Он опытный финансовый аналитик и аналитик данных с доказанным опытом работы в государственном и частном секторах. В настоящее время он работает аналитиком данных в Национальном банке Грузии, работая над внедрением XBRL (расширяемого языка бизнес-отчетности) для финансового сектора Грузии. С 2016 года Резо активно работает преподавателем в различных грузинских университетах, преподает предметы, связанные с данными. Его исследовательские интересы лежат в области экономики развития, финансовой экономики и анализа данных.

Ираклий Габриадзе – аспирант экономического факультета Тбилисского государственного университета. Его основные исследовательские интересы лежат в области экономики развития, экономического роста, стран с переходной экономикой, институтов и политической экономии. Недавно он стал главой отдела анализа, мониторинга и оценки в Enterprise Georgia. Также Ираклий является приглашенным лектором по макроэкономике и статистике в Университете Грузии.

Сузана Калашиани имеет 12-летний опыт работы в сфере журналистики, социальных исследований и медиа-коммуникаций в Грузии, работая координатором проекта «Российский экономический след в Грузии и влияние на грузинские институты». Ранее она участвовала в различных проектах, направленных на борьбу с антизападной пропагандой в Грузии и повышение осведомленности об отношениях между ЕС, НАТО и Грузией.

Мириан Эджибиа – выпускник Международной школы экономики в Тбилиси, Грузия (МШЭТ). Он приобрел обширный профессиональный опыт в области отчетности и финансового анализа, работая в Центре углубленной отчетности и экономического анализа. Он также приобрел большой опыт в области анализа данных и программ веб-приложений, и в настоящее время работает разработчиком полного цикла (ERP-системы) в BSC LLC.

Connections: The Quarterly Journal
ISSN 1812-1101, e-ISSN 1812-2973

Филипп Х. Флури, *Connections QJ* 19, № 4 (2020): 68-80
https://doi.org/10.11610/Connections.rus.19.4.04

Рецензированная статья

Миссии по стабилизации – уроки основанного на устойчивости миростроительстве

Филипп Х. Флури

Университет Вэньцзао, Тайвань, https://english.wenzao.tw/

Резюме: Международные миссии по стабилизации часто оказываются безуспешными, о чем свидетельствует тот факт, что в большом количестве стран, принимавших такие миссии, в течение последующих 20 лет вновь разгорелся конфликт. Автор предлагает обратиться к опыту основанного на устойчивости миростроительстве, чтобы получить более успешные примеры. Они остаются в значительной степени неизвестными или игнорируемыми и по-прежнему не пользуются должным вниманием, будь то из-за того, что «неправильная» группа НПО доминирует над программами миростроительства, «неправильные» департаменты и министерства считаются основными партнерами по миростроительству или просто проекты, основанные на устойчивости, недостаточно дорогостоящи, чтобы привлечь внимание. В статье обсуждаются рамка для обеспечения устойчивости и примеры из Гватемалы, Либерии, Тимора-Лешти и Афганистана, а также идентифицируются уроки в результате этих миссий.

Ключевые слова: либеральное миростроительство, стабилизация, стабилизационные миссии, SIGAR, Афганистан, Гватемала, Либерия, Тимор-Лешти, оценка устойчивости, рамки, устойчивость для мира.

Введение

Либеральное миростроительство было преобладающей концепцией миротворческих миссий после распада Советского Союза и исчезновения биполярной мировой системы. Со временем высокие затраты, связанные с либеральными миротворческими миссиями, ростом насильственного экстремизма и государственными спонсорами терроризма, привели к переосмыслению целей и средств интервенции в нестабильных или затронутых конфликтом государствах. Миссии по стабилизации стали новой парадигмой

интервенции, с сильным, если не исключительным, вниманием к безопасности. Однако серьезное внимание к безопасности не обходится без проблем. Чтобы проиллюстрировать это, в докладах Специального генерального инспектора по восстановлению Афганистана (SIGAR) было проанализировано и подробно рассмотрено, что именно пошло не так в усилиях по стабилизации в Афганистане под руководством США. Параллельно с появлением миссий по стабилизации, но редко в тесном взаимодействии с ними, миротворческое сообщество разработало ориентированный на устойчивость подход, определяя местный потенциал для развития и поддержания позитивного мира. В этой статье автор предлагает изучить роль устойчивости в миростроительстве и то, как миростроительство является необходимым дополнением к стабилизации, если целью международных миротворческих миссий должны быть жизнеспособные самодостаточные общества.

Как мы оказались здесь – от либерального миростроительства к стабилизации

Окончание холодной войны ознаменовало начало эры нарастания внутригосударственных конфликтов. Руководящей концепцией международного вмешательства под эгидой региональных организаций или Организации Объединенных Наций на протяжении почти двух десятилетий был «Либеральный мир».[1] Основные посылки либерального мира влекли за собой перестройку/построение государственных институтов на основе демократии, верховенства закона, прав человека и продвижения рыночной экономики как пути к миру и процветанию.

Эта концепция либерального мира в настоящее время практически исчезла, как на практике, так и как теоретическая концепция. Либеральное миротворчество оказалось сложнее и дороже, чем ожидалось. Оказалось также, что местные власти поддерживали его менее бескорыстно, чем предполагалось. Правительства принимающих стран, как правило, сопротивлялись вмешательству и настаивали на выполнении мандатов, соответствующих личным интересам власть имущих. Вследствие этих событий, травмирующего опыта нападений на США 11 сентября 2001 г. и глобального финансового кризиса 2008-2009 годов, западные демократии сместили акцент с продвижения либеральных норм и принципов мира на сочетание

[1] Карту текущих (2020 г.) многосторонних миротворческих операций см. на вебсайте SIPRI по адресу www.sipri.org/sites/default/files/2020-06/mpo20_fill.pdf. Под «миротворческой операцией» мы понимаем миссии, проводимые одной или несколькими международными организациями. По сути, такие миротворческие миссии не определены четко в международном праве. В «минимальном» определении, предложенном ZIF, www.zif-berlin.org/en/what-peace-operation, миротворческие операции: (1) развертываются международной организацией; (2) с согласия соответствующей принимающей страны; (3) для разрядки кризисных ситуаций, прекращения насильственных конфликтов и обеспечения мира в долгосрочной перспективе.

усилий по борьбе с терроризмом и стабилизации, которое было характерно для международных операций со времени интервенции в Афганистан.

Усилия по стабилизации, начиная с учреждения Миссии ООН по стабилизации на Гаити в 2004 году, включали глобальных партнеров западных заинтересованных сторон и региональные коалиции. Эту тенденцию можно было приветствовать как справедливое разделение бремени и как признак того, что региональные заинтересованные стороны берут на себя большую ответственность за региональную безопасность. Однако развертывание в Мали показало, что беспристрастность миссий ООН по стабилизации может оказаться спорной. Тогда они рискуют оказаться неработающими в поддержку всего пострадавшего населения.

Повестка дня по борьбе с терроризмом и предотвращению насильственного экстремизма и борьбы с ним (PVE / CVE) продвигались правительствами США и других западных стран, чтобы эти вопросы стали центральными в повестке дня таких организаций, как ООН и ОЭСР. Если президент США Джордж Буш объявил *Войну с терроризмом*, то она продолжалась и при администрации Обамы с более изощренным подходом: были ограничены боевые действия в Ираке и Афганистане и была одобрена новая ограниченная стратегия с упором на использование специальных сил и удары дронов (точечные убийства). Были привлечены местные вооруженные силы, их обучали и экипировали за счет бюджета, выделенного на операции. Таким образом, театр военных действий расширился за счет Мали, Нигерии, Сомалии и Йемена. Вместо на устранение коренных причин конфликтов, этот подход был направлен на разрешение таких конфликтов с помощью силы. На союзников и партнеров оказывалось давление, чтобы они приняли новую концепцию и взяли на себя часть бремени. Президентство Трампа практически не внесло никаких концептуальных изменений.

Включение региональных и *ad hoc* коалиций в миротворческие операции ООН также оказалось проблематичным. Можно ожидать, что местные органы власти будут иметь собственное мнение о своих соседях и региональных событиях, в том числе о том, кого они считают угрозой региональной стабильности. Эти взгляды обязательно должны быть учтены в мандатах, которые направлены на использование регионального сотрудничества.

С сокращением бюджетов и возвращением геополитики мы, вероятно, увидим больший упор на политическую стабилизацию через существующие формы правления. Стабилизация изображается как более эффективная и соответствующая текущей мировой ситуации и потребностям государств, переживающих конфликт. Однако с учетом того, что при стабилизации уделяется большее внимание безопасности в ущерб управлению и развитию, проявление недостатков такого подхода было лишь вопросом времени. Это уже происходит в Афганистане и Мали.

Тогда энтузиазм по поводу стабилизации, вероятно, будет ограничен во времени, поскольку он смещает акцент с коренных причин конфликтов и дефицита развития, в то же время обеспечивая слабое и коррумпированное

управление, маргинализацию, изоляцию и отсутствие социальной сплоченности. Соответственно, страдает репутация ООН как миротворческой силы. Как сказал Джон Карлсруд в своей проницательной статье: «Для ООН поворот к стабилизации и борьбе с терроризмом подрывает легитимность организации и ее работу в области посредничества и гуманитарных сфер, и в частности миротворческих операций ООН, и роль миротворческих операций ООН как центрального инструмента в наборе инструментов международного мира и безопасности».[2]

Уроки американского опыта стабилизации в Афганистане

В недавнем отчете об извлеченных уроках Специальный генеральный инспектор по восстановлению Афганистана (SIGAR) рассмотрел работу США по стабилизации в Афганистане.[3] В докладе подробно рассказывается о том, как с 2002 по 2017 год Агентство США по международному развитию, Государственный департамент и Министерство обороны пытались поддержать и легализовать правительство Афганистана в спорных районах.

Стабилизация не определяется одинаковым образом для всех заинтересованных сторон и была консолидирована как явная стратегия США только в 2009 году. Отчет SIGAR удивляет своей необычной откровенностью и тщательностью.[4] Международные силы содействия безопасности под руковод-

---

[2] John Karlsrud, “From Liberal Peacebuilding to Stabilization and Counterterrorism,” *International Peacekeeping* 26, no. 1 (2019), https://doi.org/10.1080/13533312.2018.1502040.

[3] Special Inspector General for Afghanistan Reconstruction, *Stabilization: Lessons from the U.S. Experience in Afghanistan* (SIGAR, 2018), https://www.sigar.mil/interactive-reports/stabilization/index.html.

[4] Согласно отчету SIGAR, «Правительство США сильно переоценило свою способность создавать и реформировать государственные институты в Афганистане в рамках своей стратегии стабилизации» (обратите внимание на формулировку: *способность правительства США создавать и реформировать государственные институты*, выделено автором). Таким образом, стратегия стабилизации и программы, использованные для ее достижения, «не были должным образом адаптированы к афганскому контексту». Большой стабилизационный бюджет, выделенный Соединенными Штатами Афганистану в поисках быстрых успехов, «часто обострял конфликты, способствовал коррупции и укреплял поддержку боевиков». Поскольку коалиция «в первую очередь уделяла приоритетное внимание наиболее опасным районам, она постоянно пыталась очистить их от повстанцев. В результате коалиция не смогла добиться достаточного прогресса, чтобы убедить афганцев в этих или других районах, что правительство может защитить их, если они открыто выступят против повстанцев». Кроме того, «усилия по мониторингу и оценке программ стабилизации в целом были небольшими», а успехи «в стабилизации афганских районов редко длились дольше, чем физическое присутствие коалиционных войск и гражданских лиц». В отчете делается вывод о том, что «стабилизация была наиболее успешной в районах, которые явно находились под физическим контролем правительственных сил

ством НАТО считали себя находящимися под огромным давлением и ответственными за быстрый прогресс. В результате афганские граждане остались с серьезными сомнениями относительно будущего их личной безопасности и надежности своего правительства. Интересно, что после того как афганских граждан действительно пригласили присоединиться к дискуссии,[5] некоторые предположения коалиции были подвергнуты сомнению: граждане сочли поведение афганских правительственных чиновников более опасным, чем отсутствие правительства; с самого начала, они не ожидали стабилизации за счет обширных социальных услуг, гарантированных и предоставляемых правительством (Талибан обеспечивал стабильность, «верховенство закона» и даже очень ограниченную систему социального обеспечения); они не ожидали, что стабилизация увенчается успехом, если не будут преодолены противоречивые интересы руководства Афганистана.

Как возможное следствие ограниченных результатов процесса стабилизации в Афганистане, можно было бы утверждать, что лучше забыть о миссиях такого типа. Доклад SIGAR не рекомендует столь радикальных решений. Он скорее предупреждает нас о том, что даже в лучших условиях стабилизация требует времени.

В свете частых ротаций, перезапусков и «волн наращивания» усилия по стабилизации в Афганистане до 2018 года выглядят не как одно непрерывное усилие и процесс в течение 17 лет, а скорее, как 17 однолетних мероприятий, каждое с начальным этапом и поэтапным окончанием, со стоимостью 17-летнего процесса. Кроме того, предусмотренный тип «стабилизации» мог быть достигнут только с помощью сил и подходов, выходящих за рамки задачи и выделенных ей ресурсов. Другими словами: для прочной стабилизации, как это ни парадоксально, требуется нечто большее, чем стабилизационная миссия, и она невозможна без сопутствующей стабилизации государства, гражданского общества и рынков.

безопасности, имели хотя бы небольшую долю местного управления до разработки программ, поддерживались силами коалиции и гражданскими лицами, которые признавали ценность тесного сотрудничества, и которых правительство постоянно привлекало к работе, по мере расширения программирования».

[5] Автор вспоминает личные интервью с избранными парламентариями всех политических партий в Кабуле в 2010 году. Опрошенные жаловались на то, что не имеют права голоса в усилиях по обороне и безопасности, а также в принятии решений в стране, которые, как утверждается, были полностью отданы на усмотрение президента и его международные советники. Они в равной степени остались в неведении о фактических цифрах бюджета, и тем самым сделало нелепыми все усилия по наращиванию потенциала депутатов и сотрудников парламента в области прозрачности бюджета и надзора за ним. See DCAF Afghanistan Working Group, *Afghanistan's Security Sector Reform Challenges* (Geneva: DCAF, 2011), https://www.dcaf.ch/sites/default/files/publications/documents/DCAF_RPS_Afghanistan.pdf.

Доклад SIGAR завершается рекомендациями правительству США. Их можно рассматривать как послание всем правительствам, заинтересованным в будущих стабилизационных миссиях:

- Даже в наилучших условиях стабилизация требует времени. Без терпения и политической воли для запланированной и длительной работы крупномасштабные миссии по стабилизации, скорее всего, потерпят неудачу. Ожидаемый срок должен составлять минимум 10 лет.
- Большая часть способностей и институтов правительства США, необходимых для крупномасштабной миссии по стабилизации, должна быть создана и поддерживаться между кризисными ситуациями, чтобы они были эффективными, когда они наиболее важны.
- Увеличение финансирования само по себе не может компенсировать неотъемлемые проблемы стабилизации и убеждение, что оно может усугубить эти проблемы.
- Физическая безопасность – основа стабилизации.
- Наличие местного самоуправления является предварительным условием для эффективных программ стабилизации.
- Стабилизация сообществ требует индивидуального подхода.
- Усилия по стабилизации должны строго контролироваться и оцениваться.
- Успешная разработка и реализация стратегии стабилизации требует обширных знаний о государстве и населении принимающей страны.

Виды услуг, которые правительство США стремилось помочь афганскому правительству обеспечить, были излишне амбициозными и не адаптировались к местной среде. В то время как улучшения в сфере здравоохранения, формального верховенства закона, образования и агрокультуры, вероятно, помогли многим афганцам, коалиция и правительство Афганистана стремились предоставить афганцам в спорных районах широкий спектр высококачественных услуг, что выходило далеко за рамки того, что предоставлял Талибан (и ожидало население). Им требовался уровень способностей и легитимности, намного превышающий то, что могло предложить афганское правительство, особенно в отведенное время. Коалиция стремилась построить мир *для* афганцев, а не *с* ними.

Миростроительство

Миротворческие организации могут все активнее участвовать в предотвращении насильственного экстремизма. В то время как *противодействие* насильственному экстремизму включает в себя жесткую позицию по вопросам безопасности, *предотвращение* насильственных конфликтов и насильственного экстремизма – нет. Более того, как было признано Генеральной

Ассамблеей ООН и Советом Безопасности в 2016 году, переход от менеджмента конфликтов и реагирования на них к их устойчивому, инклюзивному и коллективному предотвращению может значительно сократить расходы.[6]

Миростроительство определяется по-разному, в зависимости от приоритетов и опыта пишущих по вопросу и практиков. Термин «миростроительство» был придуман норвежским борцом за мир и ученым Йоханом Галтунгом в 1970-х годах, когда он утверждал, что «мир имеет структуру, отличную от поддержания мира и ад хок миротворчества, и что необходимо найти структуры, которые устраняют причины войн и предлагают альтернативы войне в ситуациях, когда может начаться война».[7]

Миростроительство на основе устойчивости, как это практикуется *Международной организацией миростроительства в Женеве*, направлено на выявление специфических для контекста и общества потенциалов, существующих на разных уровнях социальной организации. Потенциалы могут состоять из физической собственности, норм и ценностей, сетей. Они являются источниками средств правовой защиты, к которым можно получить доступ для выживания и/или трансформации конфликта в случае угрозы или бедствия по природным или антропогенным причинам. Вместо того, чтобы сосредотачиваться на слабостях и их устранении, подход устойчивости фокусируется на внутренних ресурсах и возможностях общества и их укреплении.

Если такие способности для обеспечения устойчивости существуют, как их можно выявлять, развивать и применять с пользой? *Рамки для оценки устойчивости* пытаются определить устойчивость как способности к абсорбции, адаптации и трансформации. Последнее, возможно, придется проанализировать и, по сути, осознать в процессе диалога с участием многих заинтересованных сторон. Такая конкретная работа над общими ценностями, интересами и ресурсами вполне может объединить участников, которые ранее отказывались сотрудничать друг с другом (опыт Гватемалы).[8]

---

[6] *«Пути к миру»* рекомендуют более согласованные усилия со стороны факторов, определяющих политику, интеграцию профилактических повесток в набор политик и усилий в области развития, инклюзивное и устойчивое развитие, такое как предотвращение конфликтов, развитие и сокращение масштабов нищеты, и отход от традиционных экономических и социальных политик. United Nations and World Bank, *Pathways for Peace: Inclusive Approaches to Preventing Violent Conflict* (Washington, DC: World Bank, 2018), p. iii, https://openknowledge.worldbank.org/handle/10986/28337.

[7] Johan Galtung “Three Approaches to Peace: Peacekeeping, Peacemaking, and Peacebuilding,” in *Peace, War and Defense: Essays in Peace Research*, vol. 2 (Copenhagen: Ejlers, 1976), 282-304.

[8] Автор имел честь быть приглашенным для оценки процесса в Гватемале. Для академической версии наших выводов см. Bernardo Arévalo de León, José Beltrán Dona, and Philipp H. Fluri, eds., *Hacia una Política de Seguridad para la Democracia en Guatemala: Investigación y Reforma del Sector de Seguridad* (Frankfurt: LIT Verlag, 2005).

Подход устойчивости, а не сосредоточение внимания исключительно на выживании в неустойчивой среде, мобилизует «инстинкты и способности к преобразованию».[9]

В то время как стихийные бедствия и гуманитарные кризисы – это ситуации, которые позволяют вернуться к *статус-кво до*, конфликты – нет. Они являются продуктом динамики внутри общества (или между обществами), и процессы, лежащие в основе конфликтов, продолжают развиваться – поэтому устойчивость для обеспечения мира должна быть способностью понимать и трансформировать их.

Устойчивость не ведет к миру автоматически. Устойчивость – это нейтральное понятие, которое может привести как к положительным, так и к отрицательным результатам. Поэтому важно тщательно проанализировать, какие возможности могут привести к установлению мира, а действие каких необходимо смягчать.

Как упоминалось выше, ответственность местных властей, которая повсеместно рассматривается как важная для заслуживающих доверия и устойчивых мирных процессов, может быть обеспечена с помощью подхода, основанного на устойчивости. То, что обычно считается отправной точкой интервенции при миростроительстве, – оценка конфликта, которая выявляет причины и движущие силы конфликта, – может не быть идеальным инструментом для обеспечения такой ответственности на местах. Дополнительная оценка устойчивости, направленная на общую оценку существующих возможностей, может обеспечить путь к прочному миру за счет вовлечения заинтересованных сторон в диалог о том, что объединяет и удерживает вместе людей.

Опыт, полученный Interpeace с помощью подхода обеспечения устойчивости, позволил выработать ряд рекомендаций. Подход, основанный на устойчивости, может обогатить стратегии миростроительства. Было также показано, что он вносит существенный вклад в национальный диалог по миростроительству. Поэтому специалисты-практики могут дополнить свой анализ конфликтов оценкой устойчивости на самых ранних этапах своей работы, направленной на выявление потенциалов, существующих на всех уровнях общества. Следует определить не только потенциалы, обеспечивающие устойчивость, в перспективе ведущие к положительным результатам, но и все качества способствующие устойчивости, включая потенциально отрицательные.

---

[9] В Тиморе-Лешти Национальная рабочая группа по гражданскому образованию разработала *Руководство по гражданскому образованию* (на основе ранее выявленных способностей для обеспечения устойчивости). Кроме того, группа предложила создать Национальный координационный совет по гражданскому образованию. Группа совместно пришла к выводу, что прочный мир требует *правильных условий* для качественного руководства на всех уровнях. Под такими правильными условиями понимались механизмы привлечения к ответственности лидеров и расширение прав и возможностей населения.

Возможности, способствующие устойчивости, могут по-разному выражаться на разных уровнях и в разных секторах общества. В случае разногласий в восприятии таких возможностей участники миростроительства должны стремиться устранять различия путем диалога с участием многих заинтересованных сторон. Отсутствие системной интеграции таких возможностей может привести к усилению «негативной устойчивости».

Проявления отрицательной устойчивости необходимо встречать с помощью стратегий, которые оказывают влияние и побуждают использовать их для достижения положительных результатов. Они не должны вести к демонтажу групп, из которых проистекает такая негативная устойчивость. Оценка устойчивости – как показала программа РОУ – не только часть пути к миростроительству, но и сама по себе усиливающее действие по миростроительству, мобилизующее национальные заинтересованные стороны для совместных действий.

Принимая во внимание огромные затраты на преимущественно внешние усилия по стабилизации, подход устойчивости является рентабельным, и поэтому должен рассматриваться всеми заинтересованными сторонами.

Оценка устойчивости – рамки для оценки устойчивости (РОУ)

Результаты двухлетней программы по определению и оценке устойчивости в интересах мира, начатой в 2014 году, были задокументированы в различных публикациях, в том числе в *Руководстве по оценке устойчивости во имя мира* и в серии публикаций о ее пилотном применении на местах в Гватемале, Либерии и Тимор-Лешти.[10] Согласно этой точке зрения, успешное разрешение конфликтов предполагает не только анализ первопричин, но также исследование и, в идеале, укрепление внутренних способностей и ресурсов для разрешения и преодоления таких конфликтов. Таким образом, подход РОУ выходит за рамки традиционной ориентации на выявление слабостей и поиск решений. Местным заинтересованным сторонам было предложено поделиться мнениями о том, как они понимают устойчивость в диалоге с национальными практикующими специалистами, международными учеными, экспертами-практиками и специалистами в области политики. При выполнении программы Interpeace сотрудничала с Гарвардской гуманитарной инициативой (HHI). Страны были выбраны на основе их постконфликтного контекста и уровня уязвимости, а также их различного географического контекста. Либерия и Тимор-Лешти во время реализации программы стремились решить проблему государственного строительства в контексте миростроительства. В Гватемале один из самых высоких показателей убийств в мире.

[10] Все доступны на https://www.interpeace.org/programme/far-1/. Смотри еще “Using Resilience to Build Peace,” Practice Brief: Resilience and Peacebuilding, Interpeace, 2016, p. 1ff.

Даже в самых сложных ситуациях, будь они вызваны конфликтом или стихийными бедствиями, можно найти людей и сообщества, которые стремятся разрешить ситуацию и противодействовать ей. Интервенции по миростроительству часто игнорируют и пренебрегают такими усилиями в ущерб тому, что могло быть согласованными усилиями по миростроительству, основанными на местных сообществах и их ресурсах, которые можно было бы использовать для преобразовательных процессов, выходящих за рамки простой реакции на хрупкость.

Конфликты часто сопровождаются историей социальной асимметрии и исключения. Подход устойчивости использует «автоиммунные» ресурсы, с помощью которых общество трансформирует обстоятельства и условия, которые приводят к возникновению конфликтов. Такие ресурсы, способствующие устойчивости, можно найти на разных уровнях общества, и они могут быть взаимосвязаны или взаимосвязываемыми как по горизонтали (с другими сообществами и отдельными людьми), так и по вертикали (с учреждениями более высокого уровня, включая государственные учреждения). Эта взаимосвязь может серьезно повлиять на усилия по миростроительству, особенно если ее не выявить и не мобилизовать. «Устойчивость» сама по себе нейтральна к ценностям – она касается в основном инстинктов самосохранения данного субъекта в более широком контексте. Она может проявиться негативно, если групповая солидарность идет за счет успеха миростроительства для общества в целом. Поэтому важно, чтобы усилия по миростроительству всесторонне затрагивали такие группы в их идентичности. Это особенно актуально для (коренных) этнических групп с высоким уровнем самоорганизации, который обеспечивает не только чувство идентичности, но и «социальный капитал», поскольку эти группы тем самым получают доступ к общественным благам, которых они в противном случае были бы лишены (например, образование и здравоохранение). В Гватемале эти прочные узы явно приносят пользу имеющим отношение сообществам, но не обязательно ведут к большей сплоченности общества, а также к доверию и желанию сотрудничать с институтами государства:

> В результате группы коренного населения становятся еще более изолированными от государства. Это пример того, как неспособность соединить ресурсы устойчивости на разных уровнях – здесь между уровнем сообщества и уровнем государства – может способствовать динамике конфликта. Таким образом, есть веские основания для выявления неформальных лидеров или посреднических институтов, которые могут преодолеть пропасть между коренным населением и государством, чтобы можно было использовать сильную социальную сплоченность внутри коренных общин для достижения большего мира в стране на социальном уровне.[11]

[11] “Using Resilience to Build Peace.”

В таком случае необходимо задать вопрос: как можно улучшить сотрудничество между группами? И какая политика должна быть введена в действие, чтобы усилить механизмы сотрудничества, типичные для данного общества? *Устойчивость не обязательно и автоматически ведет к миру.*

Точно также заинтересованные стороны в Тиморе-Лешти определили культуру, религию, лидерство, право и безопасность как двойственные и иногда используемые в целях исключения. Следовательно, анализ устойчивости должен привести к тщательному различению факторов, потенциально способствующих миру, от других, действие которых необходимо смягчить. Существенное отличие подхода, основанного на устойчивости, от подхода, ориентированного на хрупкость, становится очевидным в этом контексте: в то время как подход, ориентированный на уязвимость, скорее остановит и устранит негативные факторы, подход, основанный на устойчивости, будет стремиться основываться на существующих возможностях при смягчении негативных факторов.

В то время как традиционное миростроительство должно начинаться с анализа причин и движущих сил конфликта, подход, основанный на устойчивости, дополняет такой анализ одним из ресурсов устойчивости – и при этом за счет привлечения местных заинтересованных сторон – помещает дискурс в центр местной ответственности, оставляя его в то время ориентированным на поиск решения с самого начала. Поэтому рекомендуется дополнять анализ конфликта в начале программного цикла картированием ресурсов устойчивости на всех уровнях общества, включая те, которые имеют амбивалентный или негативный оттенок. Негативной устойчивости можно избежать, если обращать внимание на то, как ресурсы устойчивости проявляются и используются на разных уровнях общества. Затем программы должны быть разработаны таким образом, чтобы позволить смягчить и положительно использовать такие ресурсы.

Программа РОУ продемонстрировала, что устойчивость, конечно, это полезное дополнение к подходу к миростроительству с потенциалом способствовать практике миростроительства таким образом, чтобы помочь предотвратить возникновение и повторное возникновение конфликтов и способствовать устойчивому миру. Устойчивость значительно усиливает повестку дня по предотвращению конфликтов и имеет добавленную стоимость для международного сообщества. В то время как оценка устойчивости ориентирована на то, чтобы повлиять на действия и политику, направленные на достижение устойчивого мира на всех уровнях в долгосрочной перспективе, программа РОУ продемонстрировала, что оценка устойчивости сама по себе также расширяет возможности миростроительства, поскольку она мобилизует заинтересованные стороны внутри страны предпринимать коллективные действия на благо мира. Она имеет большой потенциал как с точки зрения предотвращения, так и с точки зрения экономической эффективности, и поэтому доноры должны учитывать ее во всех ини-

циативах по миростроительству, государственному строительству, гуманитарной помощи и развитию. Помимо присущего ему потенциала миростроительства, подход, связанный с устойчивостью, дает возможность для более тесного сотрудничества между практиками, донорами и политиками, работающими в различных областях международного развития.

Выводы

Программы миростроительства и международные миротворческие миссии традиционно проходят в относительной изоляции друг от друга. Способ создания миротворческих миссий оставляет мало гибкости для корректировки мандата после согласования мандата и его включения в бюджет. Против «механистической» реализации мандата по стабилизации, которая опирается на жесткую позицию обеспечения безопасности, которой подчиняются все другие действия, если их вообще замечают, автор выступает в пользу миротворческих миссий, сформированных на основе миростроительства, базирующегося на устойчивости. Общества, вероятно, могут быть консолидированы и снова станут жизнеспособными в рамках процесса сотрудничества, руководство которого осуществляется местными властями, на основе потенциала восстановления сил, уже существующего внутри (части) данного общества. Таким образом, организации и страны, участвующие в миротворческих миссиях, будут избавлены от позора покидать страны, когда цели миссии все еще не достигнуты.

Предполагается, что миротворческое сообщество обладает лингвистической компетенцией и лидерскими качествами, чтобы находить общий язык, а также обсуждать и определять общие ценности, нормы и процедуры в сложных ситуациях. Для того чтобы это произошло, миротворческое сообщество, а также поддерживающие его ведомства и организации должны предусмотреть возможность выхода из кокона изоляции, в котором они работали, проактивно начав практиковать в отношении сообщества безопасности то, что они сами делают лучше всего на месте: протягивать руку, находить этот общий язык и определять политические рамки для устойчивого сотрудничества.

Отказ от ответственности

Выраженные здесь взгляды являются исключительно взглядами автора и не отражают точку зрения Консорциума оборонных академий и институтов изучения безопасности ПрМ, участвующих организаций или редакторов Консорциума.

Об авторе

Филипп Х. **Флури**, доктор по двум специальностям, является соучредителем и бывшим заместителем директора Женевского центра демократического контроля над вооруженными силами (DCAF) и локальным исполнительным директором Женевского центра политики безопасности. После многих лет работы политическим советником и преподавателем на всех континентах, он в настоящее время работает приглашенным профессором в Университете Вэньцзао, Тайвань. *E-mail*: drphilippfluri@gmail.com.

Connections: The Quarterly Journal
ISSN 1812-1101, e-ISSN 1812-2973

В. Ваени Нзиоки, *Connections QJ* 19, №. 4 (2020): 81-101
https://doi.org/10.11610/Connections.rus.19.4.05

Рецензированная статья

Технологии как фактор устойчивости в миротворческих операциях

Вероника Ваени Нзиоки

Министерство иностранных дел Кении, http://www.mfa.go.ke/

Резюме: Миротворческие операции претерпели значительные изменения с момента их концептуализации. Они перешли от наблюдения за прекращением огня в межгосударственных конфликтах к поддержке выполнения всеобъемлющих мирных соглашений. Некоторые миротворческие операции в настоящее время направлены на стабилизацию обстановки и во все большей степени на защиту гражданского населения. Другие проводятся в районах, подверженных насильственному экстремизму, терроризму, транснациональной организованной преступности и жестоким внутригосударственным конфликтам, в основном с участием негосударственных вооруженных групп. Эти изменения, вкупе с трансформациями глобального порядка, требуют адаптации и устойчивости миротворческих операций, чтобы обеспечить их «соответствие цели» отвечать нынешним и будущим потребностям в области безопасности. Центральное место в этой адаптации и устойчивости имеют «инструменты», «технологии» и «оборудование», которые используют миротворцы. В этой статье рассматривается устойчивость миротворческих операций с технологической и инновационной точки зрения, исследуется, как технологии могут повышать / повышают устойчивость миротворческих операций, и как миротворческие операции принимают и используют новые технологии для реализации своих меняющихся мандатов и адаптации к меняющейся динамике конфликтов. Участники миротворческих операций и их национальные технологические возможности (или их отсутствие) укрепляют или подрывают коллективную устойчивость более широкой архитектуры миротворческих операций. В статье утверждается, что гибкость, дальновидность и предвидение в сочетании со своевременной адаптацией к технологическому развитию и инновационным системам операций являются важными компонентами

устойчивости миротворческих операций в условиях меняющейся динамики безопасности.

Ключевые слова: инновации, технологии, предвидение, адаптация, устойчивость, миротворческие операции.

Введение

> *Миротворческая деятельность ООН может превратиться в обучающую инициативу, которая постоянно ищет и применяет новые технологии и инновации, тем самым позволяя лучше подготовиться к будущему*.[1]

Международный мир и безопасность остаются в центре внимания Организации Объединенных Наций (ООН) с момента ее основания, когда страны взяли на себя обязательство «избавить грядущие поколения от бедствий войны».[2] Устав ООН (Глава VII) предусматривает, что Совет Безопасности «решает, какие меры должны быть приняты в соответствии со статьями 41 и 42 для поддержания или восстановления международного мира и безопасности», включая региональные договоренности (Глава VIII).[3] В связи с этим ООН часто ссылается на операции по установлению мира[4] (особенно миротворческие), как на один из «инструментов» противодействия угрозам международному миру и безопасности.[5]

Со времени своей первой миротворческой миссии, ООН провела более 70 миротворческих операций по всему миру.[6] В настоящее время у ООН 13 миссий по поддержанию мира в Африке (7), Азии (1), Европе (2) и на Ближнем Востоке (3)[7] (см. фиг. 1).

---

1 United Nations, *Performance Peacekeeping*, Final Report of the Expert Panel on Technology and Innovation in UN Peacekeeping, 2014, по состоянию на 18 августа 2020, 19, https://peacekeeping.un.org/sites/default/files/performance-peacekeeping_expert-panel-on-technology-and-innovation_report_2015.pdf.

2 United Nations, *Charter of the United Nations and Statute of the International Court of Justice* (New York: United Nations Publications, 2015), 2.

3 United Nations, Charter of the United Nations, 27, 35.

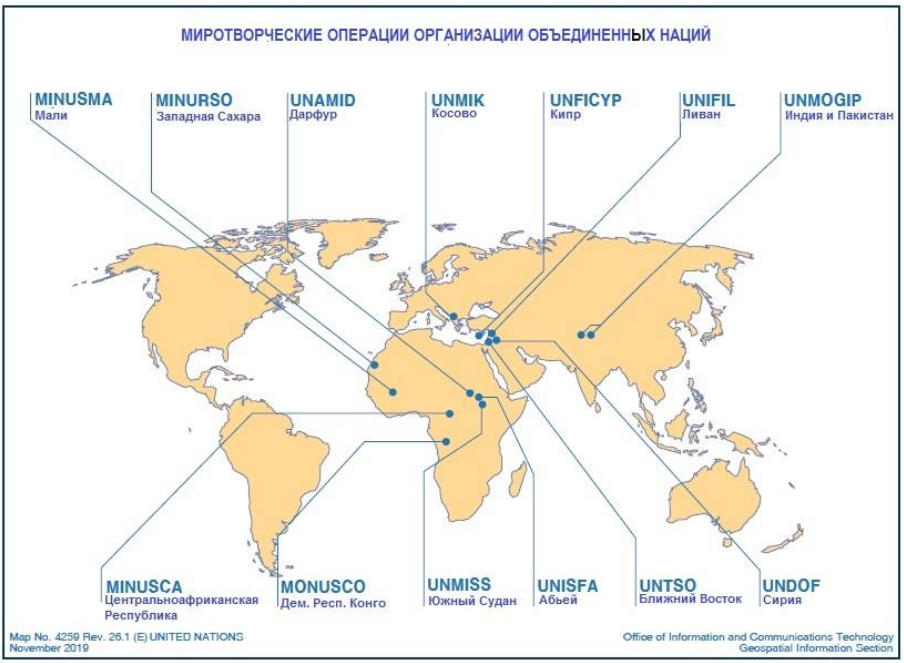
4 Термин «операции по установлению мира» в контексте данной статьи относится к миссиям по поддержанию мира и принуждению к миру. Миротворческие операции влекут за собой более широкий спектр деятельности, начиная от предотвращения конфликтов, поддержания мира, принуждения к миру, миротворчества и миростроительства. См. United Nations Peacekeeping, *Principles and Guidelines (Capstone Doctrine)* (New York: United Nations, 2008), 17-20, по состоянию на 18 августа 2020, https://peacekeeping.un.org/sites/default/files/peacekeeping/en/capstone_eng.pdf.

5 United Nations, *Capstone Doctrine*, 7.

6 United Nations, *Capstone Doctrine*.

7 United Nations Peacekeeping, “Where We Operate,” по состоянию на 1 августа 2020, https://peacekeeping.un.org/en/where-we-operate.

Миротворческими операциями активно руководили также региональные и субрегиональные организации, а также коалиции государств, особенно Организация Североатлантического договора (НАТО), Африканский союз (АС), Организация по безопасности и сотрудничеству в Европе (ОБСЕ), и Экономическое сообщество западноафриканских государств (ЭКОВАК). Наряду с многочисленными участниками миротворческих операций растут сложности как в динамике безопасности, так и в динамике конфликта (например, более широкое использование самодельных взрывных устройств (СВУ) негосударственными вооруженными группами), появляются новые угрозы (такие как продолжающаяся пандемия COVID-19), а также сдвиги в политической динамике и вкладе в миротворческие операции. Эти и другие подрывные изменения требуют от миротворческих операций устойчивости, гибкости и адаптивности, чтобы эффективно выполнять свои мандаты, сохраняя при этом свою легитимность и авторитет.



Фигура 1: Миссии Организации Объединенных Наций по поддержанию мира по состоянию на 31 марта 2020 г.[8]

[8] United Nations Peacekeeping, “Peacekeeping Operations Factsheet,” по состоянию на 18 октября 2020, https://peacekeeping.un.org/sites/default/files/pk_factsheet_3_20_english.pdf.

В мире также наблюдается экспоненциальный рост технологий и других форм инноваций, включая цифровые технологии, передовую робототехнику, искусственный интеллект, блокчейн, большие данные, Интернет вещей (IoT) и 3D-технологии. В дополнение к развитию новых технологий, также растут темпы их распространения, принятия и применения. В отношении интернет-приложений, например, Международный союз телекоммуникации (ITU) оценивает, что по состоянию на 2019 год 4,1 миллиарда человек (53,6 % мирового населения) использовали Интернет, что является значительным увеличением по сравнению с 16,8 % мирового населения в 2005 году.[9] Что касается цифровых технологий, то к 2018 году количество абонементов на мобильные телефоны на 100 человек населения мира составило 106; в Африке к югу от Сахары их было 82; Европейский Союз – 123; Ближний Восток и Северная Африка – 106; Восточная Азия и Тихий океан – 122; а в нестабильных и затронутых конфликтами государствах – 77.[10]

Технологии предвещают значительные выгоды для секторов безопасности и обороны. Использование новых технологий по-прежнему имеет решающее значение для повышения устойчивости миротворческих операций за счет лучшего удовлетворения потребностей борьбы с возникающими вызовами в области безопасности (таких, как увеличение количества СВУ и самодельных взрывных устройств на транспортных средствах, СВУТС), в основном нацеленных на миротворцев и гражданских лиц. Новые технологии также могут играть важную роль как для защиты гражданского населения (ЗГН), так и для защиты сил, обеспечивая лучшее наблюдение, мониторинг и раннее предупреждение. Новые технологии также становятся критически важными инструментами и мультипликаторами силы в обширных областях миссий, где все более востребованы способности для генерации разведданных, для анализа и мониторинга.

Группа экспертов по технологиям и инновациям в миротворческой деятельности ООН в своем отчете «Оперативная деятельность по поддержанию мира» признала, что «миротворческая деятельность ООН по-прежнему отстает от кривой развития» в освоении и применении технологий, отметив при этом, что миротворческая деятельность ООН «может и должна совершить скачок – по крайней мере – в сегодняшний день и подготовиться к вызовам будущего».[11] Признавая сложность кризисов, для управления которыми задействованы миротворцы, в Докладе отмечается значение техно-

[9] International Telecommunication Union (ITU), “Measuring Digital Development: Facts and Figures 2019,” по состоянию на 1 августа 2020, https://www.itu.int/en/ITU-D/Statistics/Documents/facts/FactsFigures2019.pdf.

[10] World Bank, “Mobile Cellular Subscriptions (per 100 people),” International Telecommunication Union, World Telecommunication/ICT Development Report and Database, по состоянию на 2 августа 2020, https://data.worldbank.org/indicator/IT.CEL.SETS.P2.

[11] United Nations, *Performance Peacekeeping*, 16.

логий в миротворческой деятельности и подчеркивается, что «нельзя ожидать успеха в сегодняшних сложных условиях без способности вводить новшества и эффективно использовать технологии, как и нельзя лишать возможных преимуществ тех, кто работает на благо мира».[12]

Поскольку проблемы безопасности в районах, где действуют миссии, продолжают усложняться, внедрение новых технологий будет иметь ключевое значение для повышения устойчивости миротворческих операций. Для операций по установлению мира устойчивость также предполагает стратегическое предвидение и картирование трансформирующегося характера конфликта, а также обеспечение гибкости реагирования и адаптации к этим изменениям. Независимая группа специалистов высокого уровня по миротворческим операциям (HIPPO) в своем отчете за 2015 год отмечает необходимость адаптации миротворческих операций «к новым обстоятельствам» и необходимость «обеспечить их повышенную эффективность и надлежащее использование в будущем».[13] Значительная часть этой адаптации заключается в повышении технологических возможностей миротворческих операций, чтобы они соответствовали нынешним и будущим потребностям. Для того чтобы миротворческие операции пользовались легитимностью и авторитетом, они должны быть адаптируемыми и устойчивыми, чтобы удовлетворять меняющиеся потребности в безопасности населения, которому они призваны служить и которое они предназначены защищать.

Хотя новые технологии не являются панацеей для решения всех проблем, с которыми сталкиваются миротворческие операции, они играют важную роль, позволяя миротворческим операциям заново формировать себя и выполнять свои мандаты более информированным и эффективным образом в условиях новых вызовов.

Эволюция миротворческих операций

> *Ясно, что в 21-м веке мы не можем продолжать работать инструментами 20-го века.*
>
> – Эрве Ладсу [14]

---

[12] United Nations, *Performance Peacekeeping*, 3.

[13] United Nations General Assembly, *Identical letters dated 17 June 2015 from the Secretary-General addressed to the President of the General Assembly and the President of the Security Council: Comprehensive review of the whole question of peacekeeping operations in all their aspects, Comprehensive review of special political missions, Strengthening of the United Nations system* (HIPPO Report), 17 June 2015, A/70/95–S/2015/446, 9, по состоянию на 23 августа 2020, https://www.un.org/en/ga/search/view_doc.asp?symbol=S/2015/446.

[14] Эрве Ладсус – бывший заместитель Генерального секретаря Организации Объединенных Наций по операциям по поддержанию мира. Смотри "UN Peacekeeping Chief Wants More Drones," *Al Jazeera*, May 30, 2014, по состоянию на 18 октября 2020, https://www.aljazeera.com/news/africa/2014/05/un-peacekeeping-chief-wants-more-drones-201453045212978750.html.

Технологии, как фактор устойчивости миротворческих операций, должны рассматриваться в контексте эволюции миротворческих операций и их существенной трансформации, а также их будущих траекторий. Ряд операций по установлению мира имеют сложные и надежные мандаты и реализуются в сложных условиях. Развитие миротворческих операций также определялось характером угроз глобальной безопасности, особенно меняющимся характером вооруженного конфликта.

Миротворческие операции являются развитием «миссий наблюдателей», основной обязанностью которых было наблюдение за действиями и развертыванием вооруженных сил конфликтующих государств, привязанных к соглашениям о прекращении огня при посредничестве ООН. В первые сорок лет своего существования миротворческая деятельность ООН главным образом реализовывалась в наблюдении и контроле за прекращением огня в межгосударственных конфликтах.[15]

«Разделяющие силы», «второе поколение» миротворческих операций, состояли из небольших подразделений военнослужащих, выполняющих в основном функции наблюдения, мониторинга и надзора, «размещенных между конфликтующими вооруженными силами».[16] Время от времени этим силам приходится заниматься физическим разделением комбатантов, чтобы создать условия для наблюдения за взрывоопасными районами, и участвовать в усилиях по обеспечению соблюдения режима прекращения огня, в то же время гарантируя, что стороны не получат новых предлогов для возобновления огня.[17]

Многомерные миротворческие операции составляют «третье поколение» операций по поддержанию мира. Их роль возросла в эпоху после окончания холодной войны, когда конфликт трансформировался в преимущественно внутренние (внутригосударственные) конфликты, расширяясь «как по численности, так и по интенсивности», и таким образом, предполагал более активное участие миротворческих операций ООН во внутренней динамике государств в стремлении к устойчивому миру и построению функционирующего государства.[18] С 1989 года было проведено более 30 многомерных миротворческих операций.[19] Сегодня многомерные миротворческие операции составляют большинство миротворческих операций. Они охватывают более широкий спектр функций, включая «разоружение, демобилизацию и реинтеграцию бывших комбатантов», гуманитарную помощь, утверждение и защиту прав человека, восстановление верховенства закона,

---

15 Mateja Peter, “Peacekeeping: Resilience of an Idea,” in *United Nations Peace Operations in a Changing Global Order,* ed. Cedric de Coning and Mateja Peter (Cham: Palgrave Macmillan, 2019), 25-44, цитата на стр. 29.

16 Dorn, *Keeping Watch,* 11.

17 Dorn, *Keeping Watch,* 11.

18 Dorn, *Keeping Watch,* 12-13.

19 Dorn, *Keeping Watch,* 13.

содействие политическим процессам, защиту гражданских лиц,[20] разведку, анализ, расследования и судебно-медицинскую экспертизу.

«Переходные администрации» – «четвертое поколение» миротворческих операций, созданное в конце 1990-х годов – повлекло за собой выход Организации Объединенных Наций за рамки надзора за мирными соглашениями и осуществление управления над целыми территориями в течение переходных периодов.[21] Миротворческие операции переходного периода имеют комплексный характер и включают широкий спектр мероприятий, в том числе образование, военные, юридические и даже санитарные функции, с совместным участием гражданских, полицейских и военных субъектов.[22]

В период после 1988 г. произошел сдвиг в миротворческих операциях как в количественном, так и в качественном отношении: 58 из 71 миротворческой операции ООН были учреждены в этот период.[23] В качественном отношении мандаты, возложенные на операции по поддержанию мира, стали более сложными, многомерными и влекли за собой решение некоторых внутренних вопросов государств, в которых они проводились, в основном осуществляя мониторинг аспектов, которые не являются военными по своему характеру.[24]

В 2000-х годах мандат на защиту гражданского населения (ЗГН) стал центральным в миротворческой деятельности ООН, обозначив дополнительный сдвиг от мандатов государственного строительства и миростроительства к «гуманитарным миротворческим операциям в чрезвычайных условиях».[25] Преобразования в миротворческих операциях также были определены субъектами, предоставляющими персонал для миротворческих операций, с увеличенным вкладом военных и полицейских из стран Африки и Азии.

Несмотря на эволюцию миротворческих операций, наблюдение и необходимость в мониторинге, мобильности и защищенной связи сохраняются. При разворачивании миротворческих операций в нестабильных районах все большее значение приобретают такие функции, как сбор информации, анализ, разведка для миротворчества и нахождение целей во враждебных условиях.

---

[20] United Nations Peacekeeping, “What is Peacekeeping,” по состоянию на 29 августа 2020, https://peacekeeping.un.org/en/what-is-peacekeeping.

[21] Dorn, *Keeping Watch,* 13.

[22] Dorn, *Keeping Watch,* 17.

[23] Peter, “Peacekeeping: Resilience of an Idea,” 31.

[24] Peter, “Peacekeeping: Resilience of an Idea,” 31-32.

[25] Peter, “Peacekeeping: Resilience of an Idea,” 36.

Технологии как фактор устойчивости миротворческих операций

> *По мере того как мировая технологическая революция продолжается, Организация Объединенных Наций может извлечь огромную пользу из множества технологий, которые помогут ее миротворческим операциям. Упускать такие возможности означает упускать шансы на мир ...*
>
> – Уолтер Дорн [26]

Устойчивость миротворческих операций, позволяющая миссиям оптимально реагировать на меняющиеся потребности в области безопасности, имеет важное значение для поддержания доверия к более широкой многосторонней системе. Поддержание мира «является деятельностью, с которой ООН наиболее явно связана»,[27] поэтому адаптивность и устойчивость миротворческих операций связаны с авторитетом всей системы Организации Объединенных Наций. Для повышения устойчивости миротворческих операций жизненно важен ряд факторов, начиная от инновационных систем операций, партнерства и заканчивая внедрением новых технологий.

Миротворческие операции претерпели ряд трансформаций, и технологии могут повысить / уже повышают устойчивость миротворческих операций в условиях этих преобразований. В будущем новые изменения в миротворческих операциях потребуют дальнейшей адаптации для повышения устойчивости. В этом разделе основное внимание уделяется тому, как технологии могут повысить / повышают устойчивость миротворческих операций в условиях:

i. динамической среды безопасности и меняющихся моделей конфликтов (с упором на растущую угрозу СВУ)
ii. возрастающее значение мандата по защите гражданского населения (ЗГН).

Динамические среды безопасности и меняющиеся моделей конфликтов (с упором на растущую угрозу СВУ)

Период с 1990-х годов характеризовался активизацией развертывания миротворческих операций, что в значительной степени отражает рост конфликтов, большинство из которых являются внутригосударственными, затяжными и асимметричными по своему характеру. Существует также частое, интенсивное и неизбирательное использование СВУ, и это будет определяющей угрозой для миротворческих операций, поскольку СВУ все чаще

[26] A. Walter Dorn, *Smart Peacekeeping: Toward Tech-Enabled UN Operations* (New York: International Peace Institute, 2016), 1.

[27] Peter, “Peacekeeping: Resilience of an Idea,” 25.

становятся «предпочтительным оружием» негосударственных вооруженных групп,[28] в том числе в районах проведения миротворческих операций. Так обстоит дело с Многомерной комплексной миссией Организации Объединенных Наций по стабилизации в Мали (MINUSMA) и Миссией Африканского союза в Сомали (AMISOM).

Воюющие стороны, в большинстве своем не имеющие доступа к обычным вооружениям, используют асимметричную тактику и оружие, такое как СВУ, для получения тактического и оперативного преимущества над миротворцами, что часто приводит к большим жертвам как среди миротворцев, так и среди гражданского населения.[29] Хотя самодельные взрывные устройства не являются проблемой для всех миссиях, они, тем не менее, приводят к значительному количеству жертв среди миротворцев.[30] Они также создают серьезные проблемы для безопасности и мобильности миротворцев и ограничивают масштабы операций миссий.[31]

В Сомали, как и в случае с Мали, атаки с использованием СВУ/СВУТС все чаще дополняются минометными обстрелами, засадами, рейдами и атаками повстанцев и террористов на базы и конвои миротворцев.[32] В Сомали террористическая группа «Аль-Шабаб» также совершает атаки с использованием самодельных взрывных устройств под транспортными средствами (СВУПТС), устраивая засады и нападения на основных маршрутах снабжения (ОМС) наряду с множеством других асимметричных тактик, в частности, террористов-смертников и убийств.[33]

Есть прогнозы, что будущие миссии могут быть развернуты в средах, сталкивающихся с аналогичными угрозами, особенно в Сирии, Йемене и Ливии.[34] Хотя миссии не совсем схожи, элементом устойчивости миротворческих операций могло бы стать извлечение уроков из опыта многонациональных сил в Ираке и Афганистане по применению технологий для противодействия СВУ.

---

[28] United Nations Office for Disarmament Affairs, “Improvised Explosive Devices (IEDs) Publication,” по состоянию на 12 сентября 2020, www.un.org/disarmament/convarms/ieds2/. См. еще Report of the UN Secretary General on Countering the Threat Posed by Improvised Explosive Devices (2018), 3.

[29] Lisa Sharland, “Counter-IED Technology in UN Peacekeeping: Expanding Capability and Mitigating Risks,” *International Peacekeeping* 22, no. 5 (2015): 587-602.

[30] Sharland, “Counter-IED Technology in UN Peacekeeping.”

[31] United Nations, *Performance Peacekeeping*, 46.

[32] Cedric De Coning, Chiyuki Aoi, and John Karlsrud, eds., *UN Peacekeeping Doctrine in a New Era: Adapting to Stabilization, Protection and New Threats* (Oxon: Routledge, 2017), 1.

[33] См. African Union, “Peace and Security Council 865th meeting: Progress Report of the Chairperson of the Commission on the Situation in Somalia/AMISOM,” по состоянию на 12 сентября 2020, 2 https://au.int/sites/default/files/documents/37727-doc-psc-progress-report-865-meeting-amisom-somalia-7-august-2019-eng.pdf.

[34] De Coning, Aoi, and Karlsrud, eds., *UN Peacekeeping Doctrine in a New Era,* 1.

В противодействии СВУ могут применяться как высокотехнологичные, так и низкотехнологичные решения. Для целей наблюдения могут использоваться относительно более дешевые привязные воздушные шары, а также дирижабли.[35] Автомобили с противоминной защитой и бронированные машины скорой помощи,[36] а также вертолеты повышают защиту сил и повышают их мобильность во время миссий в враждебной среде, а также могут использоваться для медицинской эвакуации. Это ключ к обеспечению того, что силы не будут нести потерь.

Группа экспертов по технологиям и инновациям в миротворческой деятельности ООН рекомендует, чтобы в районах, где используются СВУ, колонны были оснащены «небольшими тактическими БПЛА», которые можно было бы использовать для «мобильной разведки», а также использовать платформы для «разведки, наблюдения и рекогносцировки» (РНР) для обследования узких мест и других опасных мест на маршрутах.[37] Средства электронного противодействия (глушители СВУ) могут быть связаны с ресурсами разведки для дальнейшего снижения угрозы СВУ.[38] Приложения для смартфонов для обнаружения СВУ и других форм взрывоопасных пережитков войны (ВПВ) могут применяться в миссиях по борьбе с СВУ.[39] Радиолокаторы наземного зондирования (РНЗ) могут использоваться для обнаружения мин под землей, в то время как некоторые портативные устройства могут использоваться для обнаружения взрывоопасных составов.[40]

В выявленных горячих точках, в опасных точках или узких участках для улучшения наблюдения могут быть установлены «привязанные платформы наблюдения».[41] Привязанные аэростаты могут быть интегрированы с такими устройствами, как акустические детекторы, радары, электрооптические/ инфракрасные датчики и видеокамеры с высоким разрешением, чтобы расширить их возможности наблюдения.[42] Они также могут быть связаны с наземной станцией управления для передачи данных, хранения мультимедиа и управления системой.[43] Это полезно для передачи информации миротворцам, находящимся в различных районах миссии, или миротворцам, находящимся в движении. Автомобили с противоминной защитой

[35] Sharland, “Counter-IED Technology in UN Peacekeeping,” 594.

[36] Sharland, “Counter-IED Technology in UN Peacekeeping,” 595.

[37] United Nations, *Performance Peacekeeping*, 46.

[38] United Nations, *Performance Peacekeeping*, 47.

[39] United Nations, *Performance Peacekeeping*, 47.

[40] United Nations, *Performance Peacekeeping*, 46.

[41] United Nations, *Performance Peacekeeping*, 46.

[42] Space and Naval Warfare Systems Center Atlantic, “Tethered Aerostat Systems Application Note: System Assessment and Validation for Emergency Responders (SAVER),” September 2013, 1.

[43] Space and Naval Warfare Systems Center Atlantic, “Tethered Aerostat Systems,” 1.

необходимы для защиты передвигающихся военных и для предоставления платформ для эвакуации во время чрезвычайных ситуаций.[44]

В противодействии устройствам, которые потенциально могут вызвать срабатывание СВУ, может применяться технология как для электрического, так и для механического разрушения.[45] В то время как технологии повысят устойчивость миротворческих операций в усилиях по борьбе с СВУ, работа с местными сообществами и наращивание всеобъемлющих глобальных усилий по разрушению как сетей, так и их вспомогательных механизмов являются важными элементами более широких усилий по борьбе с СВУ в миротворческих операциях.[46] Использование технологий в трехсторонних оперативных подходах к противодействию СВУ является ключевым моментом, особенно в «подготовке сил, уничтожении устройств и атаке на сеть».[47]

Развитие сотрудничества между миссиями и партнерства по применению технологий противодействия СВУ является ключевым, особенно для миссий, сталкивающихся с аналогичными проблемами, таких как MINUSMA и AMISOM, и поэтому учитывается опыт Международных сил содействия безопасности НАТО (ISAF) в Афганистане и Ираке. Обмен опытом, постоянное наставничество и обучение повысят устойчивость миротворческих операций к возникающим угрозам. Это также будет ключом к отслеживанию моделей и пониманию меняющейся технологической динамики угрозы СВУ.

Решение проблем, связанных с различными технологическими способностями и обучением военнослужащих, полицейских и гражданских лиц, участвующих в миротворческих операциях, по-прежнему имеет жизненно важное значение для повышения технологической устойчивости архитектуры миротворческих операций в противодействии СВУ.

В то время как технологии и инновации важны для смягчения угроз, создаваемых СВУ, для обеспечения устойчивости стратегий противодействия СВУ, миротворческие операции и национальные армии, из которых формируются контингенты, должны понимать и справляться с развивающимися технологическими аспектами применения СВУ воюющими сторонами. Продолжающаяся легкость распространения информации о производстве и сборке СВУ в Интернете по-прежнему вызывает озабоченность. Генеральный секретарь ООН отмечает тревожное развитие использования беспилотных летательных аппаратов (БПЛА) для «сбрасывания» СВУ с воздуха.[48] Исламское Государство Ирака и Леванта (ИГИЛ), в частности, использовало «выстреливаемые гранаты» как «воздушные самодельные взрывные

---

[44] United Nations, *Performance Peacekeeping*, 46.

[45] United Nations, *Performance Peacekeeping*, 3.

[46] Sharland, “Counter-IED Technology in UN Peacekeeping.”

[47] Sharland, “Counter-IED Technology in UN Peacekeeping,” 593.

[48] United Nations General Assembly, “Countering the Threat Posed by Improvised Explosive Devices: Report of the Secretary General,” A/73/156, 12 July 2018, p. 5, по состоянию на 12 сентября 2020, https://digitallibrary.un.org/record/1637474?ln=en.

устройства».[49] Распад группировки и ее распространение в другие регионы вызывает озабоченность, особенно в отношении распространения технологических ноу-хау для производства и использования СВУ.

В связи с возрастающей потребностью в улучшении возможностей наблюдения и мониторинга для воздушной разведки полезны БПЛА, оснащенные камерами, и с 2013 года ООН применяет БПЛА в миссиях в Демократической Республике Конго.[50] БПЛА также были развернуты в Мали, где голландский контингент использовал БПЛА и вертолеты Apache, оборудованные контейнерами с камерами для воздушной разведки.[51]

Аэростаты, оснащенные камерами, полезны для наблюдения и мониторинга, и теперь ООН использует их в Мали на удаленных аэродромах, где воюющие стороны ранее совершали атаки, а также устанавливали СВУ. [52] Аэростаты также могут быть оснащены акустическими датчиками и помогают войскам определять направление стрельбы и направлять бортовые камеры в этом направлении, тем самым обеспечивая раннее предупреждение, лучшую ситуационную осведомленность и усиление защиты сил.[53]

Негосударственные вооруженные группы, действующие в некоторых районах развертывания миссий, все чаще используют покров тьмы для нападений как на гражданских лиц, так и на миротворцев,[54] а также для других гнусных целей, включая контрабанду людей и незаконного оружия,[55] установку мин и других видов взрывных устройств. Технологии позволяют миротворцам «преодолеть ночной барьер».[56] Усилители изображения улучшают видимость в ночное время, а тепловые инфракрасные (ИК) датчики позволяют видеть в ночное время тепло как от человеческих тел, так и от транспортных средств.[57] Эти возможности, используемые с другими технологиями, такими как дроны с датчиками ночного видения, будут продолжать повышать устойчивость миротворческих операций к работе как днем, так и ночью, поскольку конфликт с участием негосударственных субъектов

---

[49] UN General Assembly, “Countering the Threat Posed by Improvised Explosive Devices,” 5.

[50] Dorn, *Smart Peacekeeping: Toward Tech-Enabled UN Operations,* 6-7.

[51] Dorn, *Smart Peacekeeping: Toward Tech-Enabled UN Operations,* 7.

[52] Dorn, *Smart Peacekeeping: Toward Tech-Enabled UN Operations,* 7.

[53] Dorn, *Smart Peacekeeping: Toward Tech-Enabled UN Operations*, 8.

[54] Например, в декабре 2017 года в результате того, что было названо «худшим нападением на миротворцев ООН в новейшей истории Организации», при ночном нападении погибли 12 миротворцев ООН, 40 получили ранения, а четверо получили тяжелые ранения. Смотри United Nations Secretary-General, “Secretary-General’s Remarks on the attack on peacekeepers in the Democratic Republic of Congo,” 8 December 2017, по состоянию на 16 сентября 2020, https://www.un.org/sg/en/content/sg/statement/2017-12-08/secretary-general%E2%80%99s-remarks-attack-peacekeepers-democratic-republic.

[55] Dorn, *Smart Peacekeeping: Toward Tech-Enabled UN Operations*, 9.

[56] Dorn, *Smart Peacekeeping: Toward Tech-Enabled UN Operations*, 9.

[57] Dorn, *Smart Peacekeeping: Toward Tech-Enabled UN Operations*, 9.

по-прежнему включает ночные тактические и оперативные элементы. Усовершенствованные очки ночного видения, а также БПЛА со встроенными ИК-датчиками являются ключевыми факторами, позволяющими миротворцам проводить более эффективные операции в ночное время.[58]

Новые Великие силы, такие как Китай и Индия, также играют все более важную роль в миротворческих операциях, предоставляя военных и финансируя миротворческие операции. С увеличением числа миротворческих операций это «новое созвездие» также обладает технологической динамикой, которая может повысить их технологическую устойчивость. Миссии могут охватывать более широкое технологическое сотрудничество юг-юг, а также трехстороннее технологическое сотрудничество, при котором более технологически сильная страна поддерживает страны, предоставляющие военных и полицию (СПВ, СПП) через организацию, возглавляющую миротворческую операцию.[59]

Приобретение технологий является решающим элементом, как и обучение миротворцев применению технологий/инноваций в таких сложных вопросах безопасности, как кибербезопасность. Существует потребность в непрерывном обучении (на национальном уровне) и на местах во время службы для повышения устойчивости миротворческих операций в условиях растущих угроз кибербезопасности. Также необходимо решить проблему ротации войск для обеспечения того, чтобы войска на местах обладали необходимыми технологическими способностями для выполнения конкретных задач.

Возрастающее значение мандата на защиту гражданского населения

> *Этот сложный мандат часто является критерием, по которому международное сообщество и те, кого мы стремимся защитить, судят о нас как о миротворцах*.[60]

Сегодня более 95 % миротворцев уполномочены защищать мирных жителей.[61] После окончания «холодной войны» насильственные конфликты все чаще носят внутригосударственный характер с участием негосударственных субъектов. Эти конфликты вызвали массовые гуманитарные кризисы, и гражданские лица все чаще становятся преднамеренными мишенями. Повышенное внимание к защите гражданских лиц направлено на то, чтобы не допустить повторения кризисов и неудач в защите гражданских лиц со стороны правительств и миротворческих операций в 1990-х годах в Руанде,

---

[58] Dorn, *Smart Peacekeeping: Toward Tech-Enabled UN Operations*, 9.

[59] Интервью автора с профессором Седриком Де Конингом, 13 марта 2020.

[60] United Nations Peacekeeping, “Protecting Civilians,” по состоянию на 23 августа 2020, https://peacekeeping.un.org/en/protecting-civilians.

[61] United Nations Peacekeeping, “Protecting Civilians.”

Боснии и Сомали. Само по себе стремление включить защиту гражданского населения в мандаты большинства миротворческих операций находится в резонансе с развивающейся динамикой современных конфликтов, когда граждане становятся мишенями или все чаще оказываются под перекрестным огнем, что указывает на устойчивость миротворческих операций.[62]

Генеральный секретарь ООН в своем докладе «Защита гражданского населения в вооруженном конфликте» отмечает, что в 2019 году «более 20 000 мирных жителей были убиты или ранены» в результате связанных с конфликтом нападений в 10 странах – «Афганистан, Центральноафриканская Республика, Ирак, Ливия, Нигерия, Сомали, Южный Судан, Сирийская Арабская Республика, Украина и Йемен».[63] Это число, безусловно, выше, если принять во внимание количество жертв среди гражданского населения и раненых среди гражданского населения в Камеруне, Чаде, Демократической Республике Конго, Мали, Мозамбике, Мьянме, Нигере, Судане (Дарфуре) и на оккупированной палестинской территории.[64]

Поскольку большинство операций по поддержанию мира имеют мандат на защиту гражданского населения, их успех в этой функции зависит, среди прочего, от наличия надлежащих ресурсов и оснащения. Беллами, Уильямс и Гриффинс отмечают, что «хорошо экипированные операции», проводимые при поддержке международного сообщества, обеспечивают большую вероятность спасения жизней по сравнению со «спорными, плохо оснащенными и непродуманными операциями».[65]

В ситуациях вооруженного конфликта своевременная и точная информация может спасти жизни.[66] Цифровые технологии могут использоваться в районах миссий, чтобы помочь гражданским лицам и миротворцам подключаться, обмениваться информацией и новостями, проводить обучение, а также принимать решения.[67] Это усиливает элемент «коллективного миротворчества», когда существует взаимодействие между миссией и местными жителями, а последние обмениваются информацией для раннего

---

[62] Идея миротворчества оказалась устойчивой в условиях меняющихся моделей конфликтов, влекущих за собой «различные виды деятельности», начиная с первой миротворческой миссии в 1948 году. Поддержание мира также адаптируется к меняющейся динамике сил в глобальном порядке. Подробнее об *устойчивости идеи миротворчества* см. Mateja Peter, "Peacekeeping: Resilience of an Idea," in *United Nations Peace Operations in a Changing Global Order,* ed. Cedric de Coning and Mateja Peter (Cham: Palgrave Macmillan, 2019), 25-44.

[63] United Nations Security Council, "Protection of Civilians in Armed Conflict. Report of the Secretary General," S/2020/366. May 6, 2020, стр. 3, по состоянию на 17 сентября 2020, https://www.unocha.org/sites/unocha/files/SG%20POC%20Report-May%202020.pdf.

[64] United Nations Security Council, "Protection of Civilians in Armed Conflict," 3.

[65] Alex J. Bellamy, Paul D. Williams, and Stuart Griffin, *Understanding Peacekeeping,* 2nd ed. (Cambridge: Polity Press. 2010), 2.

[66] UN Security Council, "Protection of Civilians in Armed Conflict," para 13, 10.

[67] UN Security Council, "Protection of Civilians in Armed Conflict," para 13, 10.

предупреждения, тем самым участвуя в повышении собственной безопасности, что также способствует «защите через связь».[68]

Миссия Организации Объединенных Наций по стабилизации в ДР Конго (MONUSCO) разработала «Сеть оповещения населения», которая использовала раздачу телефонов лидерам общины, которые затем делились бы информацией с миссией в случае надвигающейся опасности.[69] Раннее предупреждение и разведка будут по-прежнему иметь ключевое значение для обеспечения того, чтобы миротворцы действовали до фактических инцидентов и тем самым предотвращали нападения до их совершения. Технологии будут играть ключевую роль в предоставлении информации как о запланированных инцидентах, так и в обмене фотографиями, а также в использовании передовых устройств с поддержкой глобальной системы позиционирования (GPS), предоставляя информацию о местах, где можно связаться с гражданскими лицами.

Доступ к спутниковым снимкам можно получить на коммерческой основе, а операции по поддержанию мира могут иметь пользу от разведки почти в реальном времени, когда цены на снимки падают вместе с периодами задержки и временем доставки.[70] Спутниковые изображения полезны для наблюдения за большими удаленными районами, особенно там, где миссии призваны защищать гражданское население.

Миссии также могут использовать Интернет, сети SMS-оповещений, телевидение, радио и социальные сети для обмена информацией с гражданским населением [71] в рамках инициатив по защите. В дополнение к SMS, технологические сети оповещения (CAN) могут использовать мобильные телефоны, номера бесплатных горячих линий, высокочастотные (HF) радиоприемники и спутниковые телефоны.[72] Использование технологий для защиты должно сопровождаться защитой конфиденциальных личных данных, чтобы гарантировать соблюдение конфиденциальности уязвимых людей, находящихся под защитой.[73] Также необходимо следить за тем, чтобы воюющие стороны не использовали социальные сети для распространения дезинформации, подстрекательства к насилию и разжигания ненависти, которая усиливает раскол и усугубляет насилие.[74]

---

[68] Dorn, *Smart Peacekeeping: Toward Tech-Enabled UN Operations,* 12-13.

[69] Dorn, *Smart Peacekeeping: Toward Tech-Enabled UN Operations,* 13.

[70] Dorn, *Smart Peacekeeping: Toward Tech-Enabled UN Operations,* 5.

[71] Dorn, *Smart Peacekeeping: Toward Tech-Enabled UN Operations,* 13.

[72] United Nations Department of Peace Operations, “The Protection of Civilians in United Nations Peacekeeping Handbook,” 97

[73] United Nations, Performance Peacekeeping, 118; См. также John Karlsrud, *The UN at War: Peace Operations in a New Era* (Cham: Palgrave Macmillan, 2018), 75.

[74] United Nations Security Council, “Protection of Civilians in Armed Conflict,” Report of the Secretary General S/2020/366, May 6, 2020, para. 39, 10, по состоянию на 17 октября 2020, https://www.unocha.org/sites/unocha/files/SG%20POC%20Report-May%202020.pdf.

Устойчивость также гарантирует, что миссии будут продолжать прилагать усилия к мониторингу, обнаружению и оценке угроз в социальных сетях в рамках картирования конфликтов, учитывая, что негосударственные вооруженные группы и другие воюющие группы злонамеренно используют такие инструменты, как социальные сети, для соблазнения, манипуляции, вербовки и координации.[75]

С 2019 года Unite Aware (ранее называвшаяся «Программой ситуационной осведомленности») – платформа ИТ-приложений – применяется в миротворческих миссиях для ситуационной осведомленности.[76] Платформа состоит из приложений, таких как «Unite Aware Incidents», которое помогает защищать гражданских лиц путем отслеживания инцидентов ЗГН и их хранения в «центральной базе данных», «Unite Aware Maps», которое предлагает визуальные, геопространственные данные, как фиксированные, так и переменные, такие как планы патрулирования, а также местонахождение критически важной инфраструктуры и инцидентов, а также «Панели мониторинга Unite Aware», которое предлагает индивидуализированные представления данных о проблемах с ЗГН, таких как количество инцидентов изнасилования, убийств и других происшествий, которые могут быть дополнительно сгруппированы по конкретным местам, полу и возрасту.[77]

С трансформацией методов боевых действий и воюющих сторон, которые все чаще действуют в сообществах, как в городских, так и в сельских районах, предоставление гражданским лицам безопасных энергосберегающих коммуникационных технологий, особенно в районах без надежного электроснабжения, является ключом к активному участию в миссии по коммуникации о любых запланированных нападений и других отвратительных действий, планируемых на уровне сообществ. Это, в свою очередь, повысит безопасность как гражданского населения, так и вооруженных сил, а также повысит устойчивость миротворческих операций в условиях меняющейся динамики конфликта. Фотографии, сделанные гражданскими лицами, могут быть использованы в качестве доказательства в судебных процессах, касающихся возможных злодеяний и насилия в отношении гражданских лиц.

БПЛА, используемые в районах миссии, оснащенные такими устройствами, как тепловизионные камеры, имеют решающее значение для получения подробных изображений с высоким разрешением, которые полезны для определения местоположения объектов, анализа местности, измерения расстояний и территорий, а в случае инцидентов БПЛА можно использовать, чтобы получить точное местоположение.[78] Несмотря на обширную территорию, которую покрывает большинство миссий, БПЛА могут играть

[75] UN Security Council, “Protection of Civilians in Armed Conflict,” para. 39, 10.

[76] United Nations Department of Peace Operations, “The Protection of Civilian,” 104.

[77] United Nations Department of Peace Operations, “The Protection of Civilians,” 104.

[78] United Nations Department of Peace Operations, “The Protection of Civilians,” 104.

решающий мультиплицирующий эффект, позволяя миссии «видеть и собирать информацию» из труднодоступных или враждебных мест, что обеспечивает более широкое присутствие миссии, а также продвижение защиты как гражданских лиц, так и миротворческих сил.[79] Полученная информация обеспечивает ситуационную осведомленность, отслеживает передвижения воинственных вооруженных групп, а также перемещенного гражданского населения, и может использоваться позже при расследовании инцидентов, связанных с защитой гражданского населения (ЗГН).[80]

Технологии, несомненно, будут играть важную роль в защите гражданского населения. Однако, поскольку миротворческие операции используют технологические возможности как фактор устойчивости для усиления защиты гражданского населения, также важно планировать и учитывать гендерную динамику технологических разногласий, особенно в отношении доступа к технологиям и их применения. Это обеспечит гибкость миротворческих операций с использованием технологий для защиты всех, «никого не оставляя без внимания». В большинстве обществ, где происходят жестокие конфликты, женщины также несут культурную ответственность за воспитание детей и содержание приусадебных участков. Следовательно, защита детей во многом связана с защитой женщин. И если у женщин нет доступа к цифровым технологиям и Интернету, которые можно использовать для защиты, дети и пожилые люди (за которыми женщины также ухаживают) становятся подверженными воздействию и уязвимыми.

Частью мер предвидения и повышения устойчивости, направленных на обеспечение возможности использования Интернета для связи и усиления защиты, является решение проблемы разрыва в возможностях подключения к Интернету. Из нынешних 13 миротворческих операций под руководством ООН семь находятся в Африке, 3 на Ближнем Востоке и 2 в Европе.[81] Однако, подключение к Интернету по состоянию на 2019 год составляло 28,2 % в Африке, 51,6 % в арабских государствах, 48,4 % в Азиатско-Тихоокеанском регионе и 82,5 % в Европе (фиг. 2).[82]

В будущих миссиях может потребоваться найти механизмы для снижения стоимости и соответствующего подключения к Интернету для групп населения, подвергающихся риску, если они хотят подключиться к Интернету для защиты. Это аспект, который потребует более тесного сотрудничества и партнерства с частным сектором.

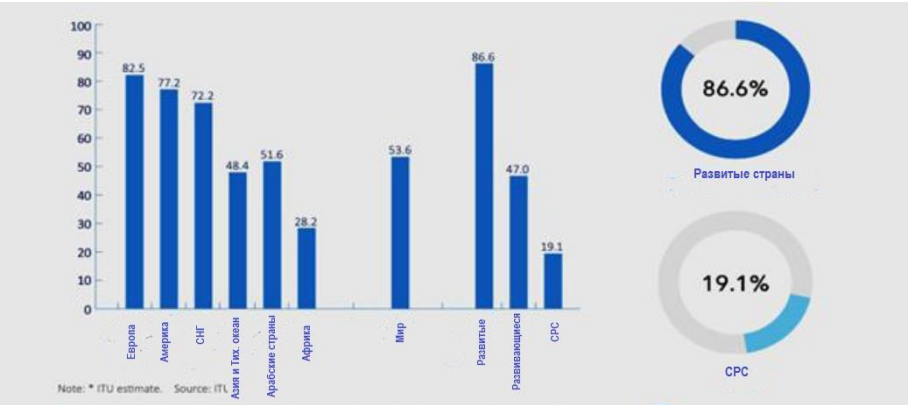
---

[79] United Nations Department of Peace Operations, “The Protection of Civilians,” 104.

[80] United Nations Department of Peace Operations, “The Protection of Civilians,” 104.

[81] United Nations Peacekeeping, “Where we operate.”

[82] International Telecommunication Union (ITU), “Measuring Digital Development: Facts and Figures 2019,” accessed August 1, 2020, https://www.itu.int/en/ITU-D/Statistics/Documents/facts/FactsFigures2019.pdf.



Фигура 2: Процент людей, использующих Интернет, по регионам и статусу развития, 2019.[83]

Часть технологической устойчивости повлечет за собой *защиту умов*, поскольку миротворческие операции сосредоточены на *защите тел*. *Битва за умы* мирных жителей все больше становится одним из пространств, в которых борются негосударственные вооруженные группировки, которые стремятся повлиять на мирных жителей с помощью Интернета и цифровых технологий. Защита умов только будет приобретать все большее значение среди огромного спектра защиты. Стратегическая коммуникация станет еще более важной; поэтому в некоторых миссиях, таких как Сомали, ООН уже участвует в стратегических коммуникационных кампаниях, чтобы противостоять радикализирующим посланиям и воздействиям террористической группировки «Аш-Шабаб».[84]

Защита гражданского населения при использовании цифровых технологий, особенно мобильных телефонов, должна учитывать внедрение и использование мобильных телефонов в районах развертывания миротворческих операций. Мобильные телефоны позволяют членам сообщества предупреждать миротворцев о любой опасности (текущей или надвигающейся), или даже сообщать о любых нерегулярных действиях, особенно когда воюющие стороны связаны с гражданским населением. Часть устойчивости включает в себя вопрос о том, как можно смягчить эту новую динамику угроз, а также о том, насколько доступными могут быть мобильные телефоны для защиты более широких слоев населения. В то время как в 2018 году количество абонентов мобильных телефонов «на 100 человек» составляло 106, цифры кажутся мрачными, когда речь идет о странах, затро-

[83] ITU, “Measuring Digital Development: Facts and Figures 2019.”

[84] Peter, “Peacekeeping: Resilience of an Idea,” 38.

нутых конфликтом, особенно тех, в которых проводятся активные миротворческие операции и где больше всего в них нуждаются, как показано в следующей таблице.[85]

Таблица 1. Страны, переживающие насильственный конфликт (все, кроме Йемена с активными миротворческими операциями), и количество абонентов мобильных телефонов на 100 человек, 2018.

Страна	Абонементы на мобильные телефоны на 100 человек
Афганистан	59
Центральноафриканская Республика	27
Демократическая Республика Конго	43
Мали	115
Сомали	51
Южный Судан	33
Судан	72
Йемен	54

Заключение

Внедрение технологий остается важным шагом в повышении устойчивости миротворческих операций. Картирование и стратегическое предвидение имеют решающее значение для миротворческих операций, чтобы предвидеть, планировать и готовиться к будущим угрозам. Это немалый подвиг для миротворческих операций, которые состоят из сил со всего мира с различной военной культурой, подготовкой и возможностями. Включение стратегического предвидения в миротворческие операции является важным элементом для определения инструментов, оборудования, инноваций и технологий, необходимых для повышения устойчивости миротворческих операций.

Сотрудничество и взаимодополняемость будут по-прежнему важны, учитывая различные возможности государств в рамках международной системы и их вклад в миротворческие операции. Технологическая устойчивость операций по поддержанию мира предполагает устойчивость ключевых участников миротворческих операций, в частности ТСС, РСС и все в большей степени стран, предоставляющих технологии (TechCC). [86] Для TechCC важно изучить возможности долгосрочного партнерства. Устойчивость вооруженных сил отдельных ТСС в значительной степени оказывает

[85] World Bank, “Mobile Cellular Subscriptions (per 100 people).”

[86] Dorn, *Smart Peacekeeping: Toward Tech-Enabled UN Operations,* 1.

влияние на устойчивость более широкой архитектуры миротворческих операций в отношении технологий и инноваций.

На миротворческие операции могут оказывать воздействие динамические изменения и тенденции, влияющие на глобальную безопасность, политическое и экономическое пространство. Трансформация конфликта порождает новые потребности и смещает фокус полномочий на нетрадиционные аспекты, такие как стабилизация в условиях таких угроз, как пандемия (как в настоящее время имеет место борьба с продолжающейся пандемией COVID-19), а также неблагоприятное изменение климата и связанные с ними инциденты, такие как наводнения, засухи и гуманитарные потребности, которые они порождают.

Хотя быстрое развитие технологий открывает новые возможности для миротворческих операций при выполнении их мандатов, при внедрении технологий необходимо учитывать потенциальные непредвиденные и нежелательные воздействия, связанные с новыми технологиями. К их числу относятся технологии двойного назначения и потенциальное применение технологий в насильственных целях, кибер-вторжения в важные данные миссии и враждебное использование новых технологий воюющими сторонами.

В условиях неоднозначных, неопределенных и сложных изменений,[87] сопровождающихся очень серьезными срывами, миротворческие операции должны быть гибкими, новаторскими и адаптивными для смягчения угроз при выполнении своих мандатов. Внедрение технологий и других инноваций дает возможность мирным операциям более эффективно держать курс среди этих изменений.

Принятие технологий также должно сочетаться с гибкостью и другими факторами устойчивости, среди которых стратегическое предвидение, прогнозирование и инновации для адаптации конкретных реакций к потребностям миссии по мере их появления; обновление руководств (например, руководства по принадлежащему контингентам имуществу) с учетом меняющихся потребностей операций по установления мира; непрерывное образование и развитие навыков для конечных пользователей новых технологий в областях миссии; партнерские отношения для усиления возможностей различных участников, предоставляющих персонал; и непрерывное изучение во время миссии и между миссиями технологических тенденций, потребностей миссии и пригодности технологий.

[87] Hassan Abul-Enein, “Resilience and Agility: Managing and Mitigating Evolving Threats in a Hyperconnected World,” *Strategic Security Analysis*, no. 13 (Geneva Centre for Security Policy, August 2020), 3, https://www.gcsp.ch/publications/resilience-and-agility-managing-and-mitigating-evolving-threats-hyperconnected-world.

Отказ от ответственности

Выраженные здесь взгляды являются исключительно взглядами автора и не отражают точку зрения Консорциума оборонных академий и институтов изучения безопасности ПрМ, участвующих организаций или редакторов Консорциума.

Об авторе

Вероника Ваени **Нзиоки** – сотрудник дипломатической службы Министерства иностранных дел Кении и исследователь по вопросам мира и безопасности. Ее исследовательские интересы сосредоточены на новых технологиях, инновациях, миротворческих операциях, вооруженных конфликтах и трансформации войны. Вероника ранее работала в Международной организации труда (Программа занятости) в офисе Центральной и Восточной Европы в Будапеште, Венгрия. Она также работала в Иезуитской службе по делам беженцев в Северной Уганде, а также в Университете Найроби в качестве координатора академических программ и исследователя политики. Вероника имеет степень магистра перспективных исследований в области международной и европейской безопасности, предлагаемую совместно Женевским университетом и Женевским центром политики безопасности (GCSP), Швейцария, степень магистра международных отношений Будапештского университета Корвинуса, Венгрия, а также степень магистра международных отношений. Степень бакалавра политологии и социологии (двойная специализация) Университета Найроби, Кения. Она изучала гендерные вопросы в университете Або Академи в Финляндии в рамках программы обмена Север-Юг-Юг. Вероника – выпускница GCSP в рамках курса «Лидерство в области международной безопасности» (LISC).
E-mail: nziokiveronique@gmail.com

Connections: The Quarterly Journal
ISSN 1812-1101, e-ISSN 1812-2973

Мария Х. Морейра, *Connections QJ* 19, № 4 (2020): 102-113
https://doi.org/10.11610/Connections.rus.19.4.06

Рецензированная статья

Важность устойчивости для повестки дня по вопросам женщин, мира и безопасности, особенно во время пандемии Covid-19

Мария Хулия Морейра

Мирные женщины всей планеты, http://www.1000peacewomen.org/

Резюме: Женщины научились различным способам повышения устойчивости через свои действия в своих сообществах. Они развили устойчивость и лидерство. 2020 год – выдающийся год с точки зрения гендерного равенства и расширения прав и возможностей женщин, поскольку он знаменует собой годовщину беспрецедентных политических обязательств и рамок практических действий. COVID-19 кардинально изменил жизнь женщин, девочек и подростков во всем мире. Многие женщины, отвечающие за свои общины, находятся на передовой, защищая свой народ, и являются основой устойчивости общества. Несмотря на то, что на большинство из них вирус оказывает свое влияние, они продолжают упорно работать, стараясь сделать все возможное для своих людей. Крайне важно смотреть на внешнюю политику и через призму феминизма, и при реализации инициативы «Женщины, мир и безопасность» чрезвычайно важно учитывать, что женщины являются ключевыми акторами в построении жизнеспособных демократических обществ.

Ключевые слова: устойчивость, женщины-беженки, перемещенные женщины, Covid-19, резолюция 1325 СБ ООН, субъекты перемен, гендерное равенство, расширение прав и возможностей женщин, кризис.

Моей матери, лучшему примеру устойчивости

Введение

В данной статье рассматривается важная тема, с которой сталкивается человечество, в частности, в результате COVID-19. Устойчивость играет ключевую роль в программе «Женщины, мир и безопасность», которой в этом году исполняется 20 лет. Как будет показано в статье, женщины находятся на передовой, защищая свои сообщества от угрозы пандемии. В шести разделах будет проанализировано основное содержание данной повестки дня с упором на устойчивость женщин, на которую направлена Резолюция 1325 и последующие резолюции.

Очень важно проанализировать эволюцию концепции устойчивости, чтобы знать, какие уроки были извлечены и как передовой опыт применяется при реализации концепции устойчивости в этот сложный момент. Особо следует упомянуть две группы женщин, беженцев и перемещенных женщин, которые включены в Резолюцию 1325 и которые на протяжении всей своей тяжелой жизни демонстрировали устойчивость. Наконец, мы рассмотрим вопрос устойчивости женщин во всем мире после пандемии, а также то, как они всегда расставляют приоритеты в своих общинах.

Женщины, мир и безопасность

Единогласно принятая 31 октября 2000 года Резолюция 1325 является первой в истории резолюцией Совета Безопасности Организации Объединенных Наций, в которой признается необходимость в привлечении и вклад половины населения мира – женщин – в дело международного мира и безопасности.

Женщины и мужчины переживают жестокие конфликты как огромную человеческую трагедию. Но роли, опыт, потребности и интересы женщин, девочек, мужчин и мальчиков очень разные. Женщины более серьезно страдают от сексуального насилия и домашнего насилия, перемещения и социальной дискриминации, и им нужно быть очень стойкими, чтобы поддерживать себя и свои сообщества. Они несут тяжелую ношу.

Швейцарская организация *Мирные женщины всей планеты* (PWAG), возникшая после выдвижения 1000 женщин на Нобелевскую премию мира в 2005 году, признала 5 факторов мира, взятых из Резолюции:

- Участие: более широкое вовлечение женщин в миростроительство;
- Предотвращение конфликтов и гендерного насилия;
- Защита прав и потребностей женщин и девочек во время и после вооруженных конфликтов;

• Поддержание мира и миростроительство: учет гендерной проблематики на всех этапах и во всех мероприятиях.[1]

Самым важным аспектом резолюции 1325 СБ ООН является то, что в ней тысячи мирных женщин во всем мире признаются «участниками перемен». Когда условия для женщин становятся лучше, выигрывают целые сообщества.

Женщины из Балкан, Бурунди, Кот-д'Ивуара, Демократической Республики Конго, Гвинеи-Бисау, Гаити и Ирака, среди многих других, которые провели встречи с представителями Генерального секретаря Организации Объединенных Наций по случаю 10-й годовщины Резолюции 1325 СБ ООН, продемонстрировали большую устойчивость перед лицом препятствий и проблем, с которыми они сталкивались.

В последнем параграфе резолюции 1325 СБ ООН говорится, что Совет Безопасности «решает продолжать активно заниматься этим вопросом». Следуя этому обязательству, Совет Безопасности принял следующие Резолюции: 1820 (2008); 1888 (2009); 1889 (2009 г.); 1960 (2010); 2106 (2013); 2242 (2015); 2250 (2015). Резолюция 1820 Совета Безопасности Организации Объединенных Наций осуждает использование сексуального насилия в качестве средства ведения войны и заявляет, что «изнасилование и другие формы сексуального насилия могут представлять собой военные преступления, преступления против человечности или являться действием, попадающим под определение геноцида». В резолюции 1888 СБ ООН Совет безопасности постановил специально уполномочить миротворческие миссии защищать женщин и детей от жестокого сексуального насилия во время вооруженного конфликта, поскольку Совет просил Генерального секретаря назначить специального представителя для координации ряда механизмов борьбы с этим преступлением. В резолюции 1889 СБ ООН Совет Безопасности призвал принять широкий спектр мер по расширению участия женщин на всех этапах мирных процессов, уделяя особое внимание периоду после достижения мирных соглашений, поскольку он начал интенсивное однодневное обсуждение этой темы. В резолюции Совета Безопасности ООН 1960 г. Совет потребовал предоставлять ему информацию о сторонах, подозреваемых в сексуальном насилии во время вооруженного конфликта. Резолюция 2106 Совета Безопасности ООН повторяет, что все субъекты, включая не только Совет Безопасности и стороны в вооруженном конфликте, но и все государства-члены и органы Организации Объединенных Наций, должны делать больше для выполнения предыдущих мандатов и борьбы с безнаказанностью за эти преступления. Резолюцией 2242 Совета Безопасности ООН Совет решил включить в свою повестку дня вопросы женщин, мира и безопасности во всех ситуациях, характерных для каждой страны. В резолюции 2250 СБ ООН Совет безопасности призвал государства-члены

[1] *No Women – No Peace: 10 Years UN Resolution 1325* (Switzerland: PeaceWomen Across the Globe, 2010), 2.

рассмотреть способы увеличения инклюзивного представительства молодежи в процессе принятия решений на всех уровнях в местных, национальных, региональных и международных учреждениях и механизмах предотвращения и разрешения конфликтов, противодействия насильственным действиям, экстремизму, другим видам деятельности, способствующих терроризму и, при необходимости, рассмотреть возможности создания интегрированных механизмов для конструктивного участия молодежи в мирных процессах и разрешении споров.

Устойчивость и повестка дня по вопросам женщин, мира и безопасности во времена Covid-19

2020 год является важной вехой для гендерного равенства и расширения прав и возможностей женщин, поскольку он знаменует собой годовщину беспрецедентных политических обязательств и рамок практических действий. Пандемия COVID 19 резко нарушила планы по оценке прогресса в достижении этих целей, празднованию достижений и постановке новых целей или задач.[2]

Пандемия глубоко повлияла на жизнь людей. От вируса и мер, принимаемых для предотвращения его распространения, особенно пострадали женщины и девочки. Еще раз женщины показали, что они являются основой устойчивости общества. Движение «Женщины, мир и безопасность» (WPS) показало свои сильные и слабые стороны и проявило стойкость в этом кризисе. Структура «ООН-женщины» также быстро отреагировала на гендерные последствия пандемии. Обосновывая ответные меры, Структура «ООН-женщины» обозначила пять приоритетов: гендерное насилие, включая насилие в семье; пакеты социальной защиты и экономических стимулов, предназначенные для женщин и девочек; поддержка людей и практическое равное распределение работы по уходу; женщины и девушки, возглавляющие и участвующие в планировании ответных мер на COVID-19 и принятии решений; и механизм данных и координации для учета гендерных аспектов.[3]

Повестка дня WPS особенно актуальна в это непростое время. Как было сказано, женщины составляют основу устойчивых сообществ, поскольку они сами устойчивы и учат свое сообщество тому, как противостоять серьезным вызовам. Они работают с местными радиовещательными компаниями, чтобы распространять сообщения об угрозе вируса и соответствующих мерах гигиены. Они учат других женщин и девочек соблюдать меры по

[2] Palvina Makan-Lakha and Molly Hamilton, “Resilience and Determination: Women, Peace and Security in the Time of COVID–19,” ACCORD (African Centre for the Reconstructive Resolution of Disputes), July 22, 2020, по состоянию на 17 сентября 2020, https://www.accord.org.za/analysis/resilience-and-determination-women-peace-and-security-in-the-time-of-covid-19/.

[3] Makan-Lakha and Hamilton, “Resilience and Determination.”

предотвращению заражения вирусом. Короче говоря, они защищают свои общины. Даже в разгар хаоса у женщин сильный голос, и они стремятся сделать свои общества более мирными и устойчивыми.

Важно на повестку дня по вопросам женщин в области мира и безопасности посмотреть и через призму феминизма, учитывая, что женщины являются ключевыми акторами в построении жизнеспособных демократических обществ. Следовательно, их права и голоса должны быть защищены и неприкосновенны. В эти нестабильные и трудные времена очень важно обратиться за вдохновением к женщинам-лидерам со всего мира. Они создавали мир, когда их опустошила война; они продвигали инновации, несмотря ни на что; и они упорствовали перед лицом вызовов и настаивали на построении лучшего будущего. Их послания – настойчивость, надежда, устойчивость, сила, борьба с дискриминацией, стремление не сдаваться и быть вместе.

Концепция устойчивости

Устойчивость – это научный термин, который применяется к материалам, которые способны возвращаться к своей первоначальной форме после сгибания или растяжения. Однако со временем этот термин стал применяться и к людям – людям, у которых есть способность быстро восстанавливаться после болезни, депрессии, поражения или других невзгод.[4]

В этом анализе ключевую роль играет гендер, потому что в этой статье речь идет о женщинах, а также потому, что более широкая социальная среда четко разделена на гендерные аспекты. Уязвимость и устойчивость по-разному и сложным образом зависят от социального пола. Люди, страдающие от маргинализации и дискриминации, наиболее уязвимы перед их негативным воздействием.

В литературе хорошо отражено, как жизненный цикл (от младенчества до старости) пересекается с различными структурными уязвимостями с конкретным содержанием. Во всем человеческом обществе гендерная идентичность определяет роль женщины или мужчины в семье и обществе в целом. Другие аспекты идентичности, оказывающие серьезное влияние на устойчивость, включают этническую принадлежность, расу, инвалидность, возраст или социальный статус.[5]

Для многих женщин устойчивость – это сила, которую они могут использовать. И женщинам, и мужчинам нужна устойчивость, чтобы справляться с жизненными трудностями. Но женщинам часто необходимо быть более

---

[4] Rose Gantner, “Women and Resilience,” in *Guide to Good Health* (Summer 2012): 7, www.guidetogoodhealth.com/PDF/ArchivedIssues/GGH%20Sum12.pdf.

[5] Julie Drolet, Lena Dominelli, Margaret Alston, Robin Ersing, Golam Mathbor, and Hauriu Wu, “Women Rebuilding Lives Post-Disaster: Innovative Community Practices for Building Resilience and Promoting Sustainable Development,” *Gender & Development* 23, no. 3 (2015): 433-448, цитата на с. 438, https://doi.org/10.1080/13552074.2015.1096040.

стойкими, чем мужчинам, чтобы преодолевать традиционные препятствия на их пути, чтобы продвинуться в деловом мире. Однако слишком многие женщины не осознают, насколько большой степенью устойчивости они обладают.

Доктор Гейл М. Вагнилд – основательница Центра устойчивости и эксперт по устойчивости, и она говорит, что, когда вы знаете свой потенциал устойчивости, это дает вам уверенность в том, что вы можете справиться с любой жизненной ситуацией. Устойчивость помогает вам справляться разными способами, будь то личные, профессиональные или социальные.[6]

Действительно, люди не контролируют определенные аспекты своей жизни, такие как несчастные случаи, стихийные бедствия и болезни и т.д., но у них есть сила реагировать на такие события и делать это со стойкостью. В число тем, связанных с устойчивостью, входят социальные связи, способность ставить себя на место других, движение вперед с развитием жизни; любопытство/вечный поиск; «лобовой» подход к вызовам; «независимость»; и духовная основа.[7]

В течение последних нескольких десятилетий наблюдается рост исследований по вопросам устойчивости, и эта концепция хорошо отражена в литературе. Тем не менее, что касается определения устойчивости, в литературе имеются разногласия относительно того, является ли устойчивость характеристикой/личным качеством, процессом или результатом.[8] Определяя устойчивость как личностное качество, Ахерн, Арк и Байерс утверждают, что устойчивость – это «адаптивное стрессоустойчивое личное качество»,[9] причем устойчивость определяется как «динамический процесс, на который влияют как нейронные, так и психологические самоорганизации, а также взаимодействие между контекстом среды и развивающимся организмом».[10] Однако, когда она определяется как результат, устойчивость рассматривается как «класс явлений, характеризующихся хорошими результатами, несмотря на серьезные угрозы адаптации или развитию».[11]

---

6 Gantner, “Women and Resilience.”

7 Beth I. Kinsel, *Older Women and Resilience: A Qualitative Study of Adaptation*, PhD Dissertation (Columbus, OH: Graduate School, Ohio State University, 2004).

8 Nancy R. Ahern, Pamela Ark, and Jacqueline Byers, “Resilience and Coping Strategies in Adolescents,” *Paediatric Nursing* 20, no. 10 (2008):32-36, https://doi.org/10.7748/paed2008.12.20.10.32.c6903.

9 Ahern, Ark, and Byers, “Resilience and Coping Strategies in Adolescents,” p. 32.

10 W. John Curtis and Dante Cicchetti, “Emotion and Resilience: A Multilevel Investigation of Hemispheric Electroencephalogram Asymmetry and Emotion Regulation in Maltreated and Nonmaltreated Children,” *Development and Psychopathology* 19, no. 3 (2007): 811-840, quote on p. 811, https://doi.org/10.1017/S0954579407000405.

11 Ann S. Masten, “Ordinary Magic: Resilience Processes in Development,” *American Psychologist* 56, no. 3 (2001): 227–238, https://doi.org/10.1037/0003-066X.56.3.227.

Важно указать на разные концепции устойчивости. Согласно Ангару, «устойчивость – это способность людей ориентироваться в психологических, социальных, культурных и физических ресурсах, которые создают и поддерживают их благополучие, так и их индивидуальная и коллективная способность добиваться предоставления этих ресурсов культурно значимыми способами».[12] Такое понимание устойчивости выходит за рамки индивидуального представления и основывается на более взаимосвязанном и целостном подходе.[13]

Тем не менее, несмотря на широкий диапазон определений, в этой области существует определенное согласие относительно определения того, демонстрирует ли кто-то устойчивый профиль/устойчивость. Должны присутствовать два элемента: а именно, неблагоприятная ситуация (то есть ситуация или угроза с высоким риском) и успешная адаптация/ компетентность.[14] Неблагоприятные условия оцениваются в связи с негативными жизненными обстоятельствами,[15] а адаптация определяется как успешное выполнение задач, связанных с возрастным развитием.[16]

Женщины и устойчивость

В жизни женщины сталкиваются с множеством своих достоинств и множеством трудностей. Они продолжают жить, осуществляя сильные инвестиции в будущую жизнь и позитивную ориентацию в жизни, несмотря на трудности и потери, которые они испытывают, особенно в сложные времена, такие как период, вызванный Covid-19. Они сталкиваются с общими проблемами, и есть потенциал для совместной работы с ними и уменьшения их уязвимости.

Женщины могут говорить о своих переживаниях, реакциях, преимуществах и трудностях. Это означает, что женщины устойчивые. Когда они устойчивы? Когда они сталкиваются со многими проблемами и изменениями в своей жизни, такими как конфликтное детство, несчастливые браки, физические заболевания, потеря мужей, и это лишь несколько примеров. В настоящее время они прилагают большие усилия для защиты своих сообществ от угрозы пандемии. Кроме того, на женщин влияют другие полити-

[12] Michael Ungar, Mehdi Ghazinour, and Jörg Richter, “Annual Research Review: What is Resilience within the Social Ecology of Human Development?,” *Journal of Child Psychology and Psychiatry* 54, no. 4 (2013): 348-366, https://doi.org/10.1111/jcpp.12025.

[13] Drolet, et al., “Women Rebuilding Lives Post-Disaster,” 435-436.

[14] See, for example, Masten, “Ordinary Magic: Resilience Processes in Development.”

[15] Tammy A. Schilling, “An Examination of Resilience Processes in Context: The Case of Tasha,” *Urban Review* 40, no. 3 (2008): 296-316, https://doi.org/10.1007/s11256-007-0080-8.

[16] Julie A. Pooley and Lynne Cohen, “Resilience: A Definition in Context,” *Australian Community Psychologist* 22, no. 1 (2010): 30-37, 30-31.

ческие, экономические и социальные факторы. Эти воздействия нельзя игнорировать. По этой причине очень важно, чтобы женщины могли делиться своим опытом и историями и чтобы их выслушивали.

Примеры устойчивости

Женщины, перенесшие тяжелую травму

Многие женщины, пережившие сексуальное насилие или нападение, очень устойчивые. Если у них есть окружающая среда, которая их поддерживает, они с большей вероятностью оправятся от этого травмирующего опыта, что окажет серьезное влияние на их жизнь. У них есть чувство надежды, способность превратить ущерб в преимущество и преодолеть невзгоды в своей жизни.

Эти факты по-разному влияют на женщин и мужчин в зависимости от конкретных гендерных ролей и отношений в конкретном сообществе. Из-за других аспектов идентичности жизненный опыт отдельных женщин заметно отличается от опыта других людей. Во многих странах мира женщины с большей вероятностью могут быть причислены к бедным, безземельным и недоедающим, и эта существующая уязвимость усиливается, когда случаются травмирующие события.

Они могут увидеть свои сильные стороны в случае болезненных переживаний. В некоторых случаях их вера добавляет смысла жизни. Кроме того, если они делятся своим опытом испытаний и невзгод, они получают возможность идти дальше и быть примером для других женщин, столкнувшихся с такими же травматическими переживаниями.

Оптимизм, независимость и способность преодолевать препятствия – характерные черты устойчивых женщин, которые рассматривают и воспринимают жизнь, как серию проблем. Они также выражают убеждение, что нужно строить планы и не ждать, пока что-то произойдет. Такое поведение помогает им в трудные времена и укрепляет веру в то, что они могут позаботиться о себе.

Положительные или отрицательные события, происходящие в определенный период жизни человека, могут повлиять на развитие устойчивости. В случае девочек, если они были устойчивыми на этом этапе своей жизни, они устойчивы и во взрослой жизни. Первые годы жизни – это начало накопления преимуществ и опыта трудностей. С этой точки зрения, люди, преодолевшие невзгоды в раннем возрасте, обретают уверенность и самоэффективность благодаря этому опыту; таким образом, они накапливают ресурсы, которые будут доступны в случае последующего вызова.

В некоторых случаях молодые девушки особенно уязвимы в плане того, что их исключают из системы образования, чтобы помогать в работе взрослым, в плане принудительных детских браков и торговли людьми.[17]

[17] Margaret Alston, *Women and Climate Change in Bangladesh* (London and New York: Routledge, 2015).

Воспоминания об их опыте отражают их способность адаптироваться от детства к взрослой жизни и влияют на их продолжительный процесс адаптации. Есть осознание поддержки в контексте их детства, которая позволила им выжить, а также признание индивидуальных характеристик, которыми они обладают. Понимание этих внутренних характеристик дает им уверенность в поиске стратегий выживания как в детстве, так и во взрослом возрасте.[18] Женщины находят свои собственные способы противостоять невзгодам, часто открываясь для риска, творческого решения проблем или присоединяясь к другим женщинам во взаимной поддержке.

Женщины беженцы и перемещенные женщины

> *Женщины знают о страданиях беженцев и судьбе перемещенных лиц.*
>
> – Активист Сафаа Элагиб Адам, Судан / Дарфур [19]

Концепция устойчивости применима к беженцам, поскольку они пережили серьезные жизненные потрясения и часто пытаются перестроить траектории личности, семьи и общества в целом.[20] То же самое и с перемещенными женщинами.

Очень важно использовать «призму» устойчивости, чтобы понять опыт беженцев и перемещенных женщин, которые в большинстве случаев являются матерями-одиночками и сталкиваются со многими трудностями, что увеличивает их уязвимость. Несколько исследований установили, что в категории внутренне перемещенных лиц (ВПЛ) женщины являются самыми уязвимыми среди уязвимых. Они сталкиваются со всеми типами потрясений, например, конфликтами и стихийными бедствиями, и противостоят им. Вышеупомянутые исследования учитывают факторы уязвимости, связанные с перемещением, такие как доступ к работе, жилью, земле и собственности, а также продуктам питания, и подчеркивают более высокий уровень бедности городских ВПЛ, чем остальной городской бедноты.[21] Женщины-беженцы и перемещенные женщины ставят благополучие своих детей на первое место, стремясь предоставить им наилучшие возможности в социальной, культурной, языковой, экономической и политической среде.

---

[18] Pooley and Cohen, “Resilience: A Definition in Context,” 33-34.

[19] *No Women – No Peace*, 17.

[20] Caroline Lenette, Mark Brough, and Leoni Cox, “Everyday Resilience: Narratives of Single Refugee Women with Children,” *Qualitative Social Work* 12, no. 5 (2013): 637-653.

[21] Nassim Majidi and Camille Hennion, “Resilience in Displacement? Building the Potential of Afghan Displaced Women,” *Journal of Internal Displacement* 4, no. 1 (January 2014): 78-91.

С точки зрения людей, ведущих привилегированную жизнь «первого мира», вопрос изучения благополучия женщин-беженцев может быть сведен к упрощенной дихотомии – либо патологизации в отношении травмы, либо высокой оценки в отношении устойчивости.[22]

Мы подчеркиваем эти вопросы в контексте управления повседневной жизнью, где распорядок дня – это не просто сосуд, в котором проживают жизни; скорее, это среда, в которой постоянно разыгрываются социальные процессы устойчивости. Устойчивость женщин, встроенная в повседневную рутину, ставит под сомнение направленность большей части дискурса устойчивости на «экстраординарные» события, в то время как социальный аспект устойчивости находится во взаимодействиях человека и окружающей среды, что дает понимание устойчивости как непрерывного процесса, осуществляемого с течением времени и в соответствие с контекстом, а не как нетипичная статическая внутренняя черта.

Несмотря на то, что многие женщины-беженки изолированы и испытывают значительные эмоциональные, финансовые и физические риски после переселения, они демонстрируют сильные стороны в своей повседневной жизни. Что касается женщин ВПЛ, концепция устойчивости все чаще используется для описания их способности адаптироваться к новой среде после шока перемещения на основе развития конкретных механизмов выживания.

Быть устойчивыми во времена Covid-19

Пройдя через эти пандемические трудности, женщины обретают чувство собственного достоинства и контроля. Когда женщины делятся своими трудностями, они учат других, как им удалось справиться, по душам обсуждая свои проблемы. Диалог и обмен опытом являются важными показателями повышения устойчивости и могут применяться к пандемии.

COVID-19 показал, что женщины обладают способностью к социальной компетентности, способностью быть гибкими, чуткими, а также способностью планировать и мыслить критически и рефлексивно. Женщины восстанавливают свою жизнь посреди этой сложной обстановки и способствуют устойчивому развитию. Женщины прекрасно знают, что для повышения устойчивости требуется больше, чем просто снижение уязвимости. Устойчивость нуждается в расширении возможностей реагирования на бедствия и травмы, которые направлены на поддержку и укрепление жизнестойкости женщин, повышая их способность реагировать на травмирующие эпизоды.

Крайне важно, чтобы правительства повышали потенциал устойчивости, уделяя особое внимание женщинам (главным героям этой статьи) и связывая это с целями Устойчивого развития, в достижении которых они участвуют. Хотя уязвимость женщин в трудные времена, с которыми человечество сталкивается в настоящее время из-за пандемии, очевидна, очевидна

[22] Lenette, Brough, and Cox, “Everyday Resilience,” 638.

и их устойчивость. Важно признать способность женщин заботиться о своих детях и членах семьи, в то время как, в зависимости от социального контекста, женщины участвуют в различных видах деятельности и выполняют различные задачи в производственной, репродуктивной и общественной сферах.

Необходимость решать разнообразные проблемы, с которыми сталкиваются женщины, является неотъемлемой частью более целостного подхода к повышению устойчивости и устойчивого развития в разрушенных сообществах. Эта пандемия показывает, что устойчивость расширяет возможности женщин, которые перестают быть молчаливой группой в обществе, что оказывает глубокое влияние на их представления о праве, справедливости и человеческом достоинстве. Их навыки и лидерство играют важную роль в повышении устойчивости. Принципиально важно, чтобы международные соглашения продвигали гендерное равенство и права человека для повышения устойчивости женщин и девочек в их сообществах. Пандемия ставит женщин и все человечество перед необходимостью развивать чувство цели, настойчивости, невозмутимости, равновесия и уверенности в своих силах.

Заключение

Как мы могли понять из настоящей статьи, в настоящее время начинают проявляться некоторые важные соображения в отношении устойчивости. Определенные ключевые внутренние ресурсы способствуют устойчивости, такие как самоэффективность, способность справляться с трудностями и чувство принадлежности. После углубленного изучения предмета можно считать, что устойчивость представляет собой взаимодействие между факторами риска (уязвимость) и защитными ресурсами (защита). Устойчивость строится на основе экономической и социальной безопасности. Жизнь в бедности в составе маргинализованной группы создает мало возможностей для накопления ресурсов, необходимых для спасения во время бедствия. Инициативы социальной защиты, которые обеспечивают доступ к основным услугам и доходам, включая защиту от рисков стихийных бедствий, являются универсальным правом человека и способствуют повышению устойчивости за счет повышения экономической безопасности, здоровья и благополучия.[23]

Вне всякого сомнения, женщины являются участниками перемен, поскольку они справляются, используя разные стратегии. Устойчивость – ключевой фактор для женщин, переживших травмы в своей жизни. Они передают нам следующее послание: «*Верьте и верьте в себя*».

Два последних соображения, учитывая, что еще многое предстоит сделать. Как сказала Элеонора Рузвельт, бывший делегат США при Организации Объединенных Наций: «Мы призываем правительства всего мира поощрять женщин во всем мире принимать более сознательное участие в

[23] Drolet, et al., “Women Rebuilding Lives Post-Disaster,” 445.

национальных и международных делах, а женщин – выступать и участвовать в работе по миростроительству и восстановлению, как они делали во время войны и сопротивления». Эти слова как никогда применимы к тому моменту, который человечество переживает из-за COVID-19. Устойчивость – это та рана, через которую проникает свет и которая появляется после столкновения с неблагоприятными фактами.

Отказ от ответственности

Выраженные здесь взгляды являются исключительно взглядами автора и не отражают точку зрения Консорциума оборонных академий и институтов изучения безопасности ПрМ, участвующих организаций или редакторов Консорциума.

Об авторе

Мария Хулия **Морейра** – аргентинский юрист. Имеет степень магистра международных отношений (FLACSO, Аргентина). В настоящее время она является сотрудником Министерства по делам женщин, гендерной политики и сексуального разнообразия провинции Буэнос-Айрес, Аргентина. С 2009 года она является региональным координатором по Латинской Америке и Карибскому бассейну швейцарской организации Мирные женщины всей планеты (PWAG). Г-жа Морейра является стипендиатом мира 2016 года (Центр мира Ротари, Университет Чулалонгкорн, Таиланд), активистом позитивного мира (Латинская Америка) и послом Института экономики и мира (Сидней, Австралия). Она является тренером курса «Предотвращение торговли людьми с сексуальными целями», предназначенного для учителей средних школ в Уругвае, приглашенным Ротари-клубом Монтевидео из-за ее опыта по этой теме. Она специализируется на теме «Женщины, мир и безопасность», регулярно выступает на национальных и международных конференциях, публикует ряд книг и статей по вопросам своей специальности. E-mail: mujeresdepazenelmundo@gmail.com

Connections: The Quarterly Journal
ISSN 1812-1101, e-ISSN 1812-2973

Джулия Ферраро, *Connections QJ* 19, № 4 (2020): 114-126
https://doi.org/10.11610/Connections.rus.19.4.07

Рецензированная статья

После кризиса: роль устойчивости для того, чтобы вернуться более сильными

Джулия Ферраро

Женевский центр политики безопасности, https://www.gcsp.ch/

Резюме: Мир вступил в период усиления напряженности, отмеченной более тяжелыми и частыми бедствиями, широко распространенным социально-экономическим кризисом и растущим чувством недоверия к институтам и международным правовым структурам. В эти непростые времена идея устойчивости привлекла внимание, особенно западного мира, который был шокирован пандемией Covid-19. Цель этой статьи – поместить слово «устойчивость» в контекст современных кризисов так, чтобы у международного сообщества не возникло соблазна перенаправить часть своих средств, зарезервированных на предотвращение и готовность к чему-то «новому». В частности, в статье приводятся три аргумента. Во-первых, понятие устойчивости следует правильно понимать, как проявление гибкости. Во-вторых, устойчивость – это не альтернатива предотвращению и обеспечению готовности к бедствиям, а скорее, их результат, как правильно определено в Сендайской рамочной программе. В-третьих, современные кризисы и проблемы, которые они создают, дают возможность улучшить нашу работу, вдохнуть новую жизнь в международные и внутренние системы и отношения, и в конечном итоге, двигаться вперед.

Ключевые слова: устойчивость, антикризисное управление, Сендайская рамочная программа**.**

Введение

Существует широко распространенное заблуждение относительно термина «устойчивость». Отправной точкой является то, что его значение меняется в зависимости от того, говорит ли человек в техническом или нетехническом смысле. Таким образом, идея устойчивости, рассматриваемая в инженерном деле, отличается от той, которую имеют в виду в социальных науках. В

этой статье автор проводит анализ, основанный на последнем значении, и рассматривает устойчивость в контексте глобальных кризисов и чрезвычайных ситуаций. Автор объясняет, как этот термин часто используется неопределенно в антикризисном управлении, вероятно, из-за нечеткого различения фаз циклов кризисного управления. Устойчивость – это не «зонтичная концепция», которая охватывает явления до, во время и после драматических событий; вместо этого она имеет место на заключительном этапе циклов кризисного управления. Такое грубое толкование термина имеет важные практические последствия, поскольку средства и ресурсы, которые следует выделять на профилактику и обеспечение готовности, могут быть неэффективно и преждевременно перенаправлены на укрепление или повышение устойчивости. Наконец, автор приходит к выводу, что устойчивость является важным понятием, поскольку оно побуждает нас изучать реальность. Другими словами, под предлогом создания или улучшения нашей способности адаптироваться к трудным ситуациям и выживать в них, мы даем себе возможность выбрать время, чтобы поразмышлять о нашем состоянии и о том, как мы хотим двигаться вперед.

В целом, статья состоит из трех частей. Во-первых, концепция устойчивости представлена через объяснение ее значения и причины, по которой она привлекла так много внимания. Во-вторых, устойчивость рассматривается в контексте кризисного менеджмента и утверждается, что Сендайская рамочная программа может быть интересной основой для дальнейшей работы по этой теме. В третьей части говорится о том, где мы находимся и куда мы идем, как взаимосвязанное и взаимозависимое общество, и в заключение включены некоторые конечные замечания.

Эластичность и кризис

Устойчивость – это умение. Хотя у всех нас разные уровни способности к такому умению, никто не рождается устойчивым. Напротив, это то, что мы приобретаем через время и опыт. Таким образом, столкнувшись с трудностями жизни в кризисные времена, международное сообщество решило изучить вопрос устойчивости и избрало ее в качестве незаменимого инструмента для нашего выживания.

Качество эластичности

Слово «устойчивость» происходит от латинского глагола *resilire* – *re* является префиксом, а *salire* – это глагол прыгать, что означает подскакивать, отпрыгивать назад или отскакивать.[1] С научным прогрессом XVII века латинское прилагательное *resiliens* начало означать не только то, что отскакивает, но и

[1] James Morwood, *The Pocket Oxford Latin Dictionary* (Oxford: Oxford University Press, 2012).

то, что может растягиваться и восстанавливать свою форму.[2] Таким образом, в своем первоначальном значении – которое до сих пор применяется в технических областях, таких как инженерное дело, – устойчивость представляет собой способность тела поглощать энергию от удара другим телом, сгибаться или сжиматься, а затем возвращаться к своей исходной физической структуре.[3] Однако, со временем слово «устойчивость» перешло в другие, не связанные с техническими науками, области, в конечном итоге превратившись в нечто большее, чем присущее неодушевленным предметам свойство эластичности. В частности, оно стало символизировать качество сохранения целостности и цели, несмотря на драматические события. В корпоративном управлении устойчивость стала «внутренней способностью организации (системы) поддерживать или восстанавливать динамически стабильное состояние, которое позволяет ей продолжать работу после серьезного происшествия и/или в условиях постоянного стресса»;[4] в экологии – «способность системы, предприятия или человека сохранять свою основную цель и целостность перед лицом резко изменившихся обстоятельств».[5] Однако, одна из самых интересных точек зрения представлена в психологии, где устойчивость была определена, как нечто большее, чем способность восстанавливаться и обновляться сталкиваясь с трудностями. Здесь ожидается, что устойчивые субъекты сохраняют свою целостность и возвращаются в свое первоначальное состояние, *по крайней мере*, таким же сильными, какими они были до того, как произошло существенное событие.[6] Эта интерпретация несет в себе аспект потенциального улучшения – *становления лучше и сильнее* – через способность людей использовать негативные события и реализовать позитивные и устойчивые изменения внутри и вокруг них.

Независимо от сферы использования, качество эластичности остается фундаментальным фактором, когда мы говорим об устойчивости. Таким образом, важно провести четкое различие между устойчивостью и сопротивлением, которые часто используются как синонимы, хотя имеют разное значение. Последнее указывает на гибкость. Оно предполагает приложение

---

2 "L'elasticità di Resilienza," Risposta ai Questiti, Accademia della Crusca, last modified December 14, 2014, https://accademiadellacrusca.it/it/consulenza/lelasticit%C3%A0-di-resilienza/928.

3 Krista S. Langeland, David Manheim, Gary W. McLeod, and George Nacouzi, *How Civil Institutions Build Resilience: Organizational Practices Derived from Academic Literature and Case Studies* (Santa Monica, CA: RAND Corporation, 2016), 5-9.

4 Karl E. Weick and Kathleen M. Sutcliffe, *Managing the Unexpected, Resilient Performance in an Age of Uncertainty* (San Francisco, CA: John Wiley, 2001), 14, citing Constance Perin, *Shouldering Risks: The Culture of Control in the Nuclear Power Industry* (Princeton: Princeton University Press, 2006), 267.

5 Langeland, et al., *How Civil Institutions Build Resilience*, 5.

6 "L'elasticità di Resilienza."

силы к объекту, который сопротивляется этой силе, например к дереву, которое сгибается, чтобы противостоять сильному ветру. Однако, если давление будет слишком большим, тело может сломаться. Первое, как объяснялось выше, является формой эластичности. Тело не сопротивляется удару, а скорее поглощает энергию, гасит ее и в конечном итоге принимает первоначальную форму. Еще одно важное соображение касается интерпретации устойчивости применительно к не-неодушевленным объектам, таким как люди, и всем субъектам, которые органически связаны с людьми и зависят от них, например, к организациям и государствам. В этом контексте устойчивость становится умением, которое позволяет нам адаптироваться к сложным ситуациям и выходить из них более совершенными. Это не вопрос о теле, которое может физически сгибаться, а затем приходить в нормальную форму; скорее, это подразумевает более абстрактное представление об эластичности. Это способность поддерживать основную целостность и цель, делать выводы и адаптироваться к ситуации, реорганизовывать и затем начинать заново. Это не что-то врожденное для людей или человеческих субъектов. Напротив, это зависит от объема работы и усилий, которые на это затрачиваются. Это также подтверждается языком, который обычно ассоциируется с устойчивостью: вы не раскрываете свою устойчивость; вы *создаете* или *улучшаете* ее. Таким образом, устойчивость позволяет нам двигаться вперед после разрушительных событий в качестве улучшенных организаций, при условии, что мы инвестируем в это. Устойчивость требует работы и самоотверженности, поэтому мы должны стремиться к ней. Если для ее достижения не прилагается никаких усилий, то мы не становимся сильнее, и мы остаемся в той же точке, в которой были до того, как нас потрясло драматическое событие.

Открытие устойчивости во времена кризиса

Заголовки новостей яростно привлекают наше внимание к растущему числу кризисов, чрезвычайных ситуаций и угроз, с которыми мы сталкиваемся. Существенные разрушительные события происходят чаще, с большей силой и часто одновременно.[7] В таком сложном ландшафте призыв к устойчивости неизбежно достиг области социальных наук.[8] В 2016 году члены Организации Североатлантического договора (НАТО) согласовали подход, ориентированный на устойчивость, чтобы противостоять крупным потрясениям и угрозам и восстанавливаться после них.[9] Они подписали Обязательство по повышению устойчивости, в котором устойчивость определяется в параграфе 1 как «основа надежного сдерживания и эффективного выполнения

[7] United Nations Office for the Coordination of Humanitarian Affairs, *Global Humanitarian Overview 2020* (Geneva: OCHA Geneva, 2019), 17-19.

[8] Eugenio Cusumano and Stefan Hofmaier, *Projecting Resilience Across the Mediterranean* (Cham: Palgrave Macmillan, 2020), 5.

[9] "Commitment to Enhance Resilience," *E-Library*, NATO, последнее изменение 8 июля 2016, https://www.nato.int/cps/en/natohq/official_texts_133180.htm.

основных задач Североатлантического союза».[10] Организацию Объединенных Наций (ООН) также увлекла идея устойчивости. В 2013 году Центральный фонд реагирования на чрезвычайные ситуации Организации Объединенных Наций опубликовал документ с изложением позиции, в котором устойчивость описывается как «желательное конечное состояние» для сообществ и домашних хозяйств, которые могут переживать стрессы и потрясения,[11] а в 2011 году Программа развития ООН опубликовала отчет, в котором обсуждалась роль устойчивости для обеспечения стабильности экономики в развивающихся странах.[12] Европейский союз (ЕС) также включил устойчивость в свою Глобальную стратегию Европейского союза от 2016 года, при этом устойчивость повышена до статуса руководящего принципа внешних действий ЕС.[13]

Это лишь некоторые из множества примеров того, как концепция устойчивости стала частью работы международного сообщества. К сожалению, такое большое количество идей и обязательств также привело к большой путанице. Это связано с тем, что способ толкования термина «устойчивость» и то, что она должна обеспечивать, различаются от одной организации к другой.[14] Для НАТО устойчивость служит цели сохранения способности ее членов противостоять нападениям, тем самым выполняя статью 3 Вашингтонского договора.[15] При таком понимании устойчивость – это податливость и гибкость, а не эластичность, что приводит к утрате основных характеристик поглощения и демпфирования энергии.

Более того, такая интерпретация не несет в себе идеи способности позитивного роста перед лицом трудностей, оставаясь зацикленной на жестких гарантиях защиты. У ЕС и ООН, похоже, другая миссия. Они приветствовали более широкое понятие устойчивости, поднимая некоторые вопросы о том,

---

10 "Commitment to Enhance Resilience."

11 "Position Paper on Resilience," l*United Nations Office for the Coordination of Humanitarian Affairs,* последнее изменение 11 мая 2013, https://cerf.un.org/sites/default/files/resources/OCHA%20Position%20Paper%20Resilience%20FINAL_0.pdf.

12 "Towards Human Resilience: Sustaining MDG Progress in an Age of Economic Uncertainty," *United Nations Development Programme,* последнее изменение 3 ноября 2015, https://www.undp.org/content/undp/en/home/librarypage/poverty-reduction/inclusive_development/towards_human_resiliencesustainingmdgprogressinanageofeconomicun.html.

13 "Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the European Union's Foreign and Security Policy," European External Action Service, EUGS, последнее изменение, 2016, https://eeas.europa.eu/sites/eeas/files/eugs_review_web_0.pdf.

14 Cusumano and Hofmaier, *Projecting Resilience Across the Mediterranean*, 5.

15 «Для более эффективного достижения целей настоящего Договора стороны, по отдельности и совместно, посредством постоянной и эффективной самопомощи и взаимопомощи, будут поддерживать и развивать свою индивидуальную и коллективную способность противостоять вооруженным нападениям». North Atlantic Treaty art 3, Apr. 4, 1949, 63 Stat. 2241, 34 U.N.T.S. 243.

может ли это слово иметь разные значения в зависимости от контекста, в котором оно используется.[16] Также стоит отметить, что и ООН, и ЕС обязались использовать концепцию устойчивости во всех обществах и регионах, что является очень амбициозной целью.

Устойчивость после кризисов

Между готовностью и устойчивостью существует тесная связь. Соответственно, они определяют начало и конец циклов антикризисного управления. Однако устойчивость часто неверно истолковывают, как «сплошное» понятие для всех фаз. Такая ошибка означает, что ресурсы тратятся впустую, в то время как мы также упускаем возможность для улучшения. Хотя идеальных схем пока нет, Сендайская рамочная программа может стать интересным шагом в правильном направлении.

Циклы антикризисного управления и устойчивость

О кризисе можно говорить, когда есть три элемента.[17] Во-первых, должна существовать угроза целостности/охвату объекта. Во-вторых, время на принятие решения ограничено. В-третьих, объем производимой информации настолько велик, что ее систематическая обработка оказывается сложной задачей. Однако время *само по себе* не определяет, наступит ли кризис.[18] Как внезапные (например, кибератаки), так и затяжные (например, изменение климата) события могут удовлетворять условиям, упомянутым выше, и привести к разрушительным обстоятельствам. Чтобы разрешать такие ситуации организованным и эффективным образом, можно использовать схемы антикризисного управления. Идея состоит в том, чтобы разделить задачи по трем временным рамкам: «до», «во время» и «после» кризиса.[19] Само собой разумеется, что распределение времени и задач не установлено, но во многом зависит от суждений и чувствительности тех, кто участвует в реализации этих циклов. То есть вы переходите к следующему этапу плана антикризисного управления всякий раз, когда это уместно, исходя из конкретных обстоятельств рассматриваемого дела. Хотя это заявление может показаться расплывчатым и необязательно полезным, оно дает нам возможность задуматься над тем фактом, что кризисы, подобные тем, которые проверяют охват задач и целостность государств и населения, являются исключительными обстоятельствами, которые требуют руководителей и профессионалов высокого уровня, чтобы с ними справлялись должным образом.

Предкризисный этап начинается с предотвращения [потенциальных ситуаций] и обеспечения готовности и заканчивается предупреждением о

[16] Cusumano and Hofmaier, *Projecting Resilience Across the Mediterranean*, 7.

[17] Christer Pursiainen, *The Crisis Management Cycle* (London: Routledge, 2017), 2.

[18] Pursiainen, *The Crisis Management Cycle*.

[19] Pursiainen, *The Crisis Management Cycle*.

кризисе.[20] Этой фазой предвидения часто пренебрегают, поскольку широко распространено мнение, что лучше воздержаться от вмешательства до тех пор, пока не возникнут какие-либо потенциальные ситуации.[21] Хотя каждый, безусловно, имеет право организовать свои ресурсы по своему усмотрению, и в идиоме «*Я перейду через этот мост, когда дойду до него*» есть мудрость, решение не вкладывать средства в дальновидное планирование обходится дорого. Серьезный подход к предотвращению кризисов и обеспечению готовности может значительно смягчить непосредственное воздействие и последующие последствия драматических событий.

Вторая фаза связана с ответом.[22] Этот этап может развиваться очень быстро и охватывает время от раннего предупреждения до реакций и действий по восстановлению. Хотя некоторые решения могут быть основаны на предыдущих результатах действий по предотвращению и готовности (например, активация планов обеспечения непрерывности бизнеса), наиболее важные решения принимаются именно на этом этапе. Работать по многим важным вопросам одновременно (например, ставить стратегические цели, распределять и перераспределять ресурсы, возглавлять команды, узнавать об изменении интересов и соответствующим образом корректировать ответные меры) очень обременительно, и это, вероятно, является причиной того, почему именно эта фаза привлекает больше внимания. Затем идет третий этап, посвященный восстановлению и учебе.[23] В отличие от предыдущей динамической фазы, это момент адаптации к новым условиям, когда возобновляется коммуникационный поток и извлекаются уроки. Именно в контексте этой последней фазы мы находим устойчивость. Ведь это может быть только эластичность и возврат к исходной форме после того, как событие произошло.

Тем не менее, если верно, что устойчивость – это способность «рассеять энергию и отскочить обратно» от сложных обстоятельств, это только одна часть картины. Как было показано в предыдущем параграфе, устойчивость не-неодушевленных субъектов также влечет за собой идею вернуться сильнее, чем раньше. Чтобы обрести такую силу, субъекту нужно сделать паузу, оценить ситуацию, адаптироваться к новой реальности и оценить, как все можно изменить к лучшему. Таким образом, устойчивость – это качество, для развития которого необходимо время и понимание, а это предварительные условия, которые очень трудно осуществить во время кризиса. С другой стороны, слишком долгое ожидание, чтобы выполнить такое упражнение на рефлексию и обновление, обычно приводит к тому, что его вообще не делают. По этим причинам было бы неэффективно размещать

[20] Pursiainen, *The Crisis Management Cycle*.

[21] Patric Lagadec and Benjamin Topper, “How Crises Model the Modern World,” *Journal of Risk Analysis and Crisis Response* 2, no. 1 (2012): 21-33.

[22] Lagadec and Topper, “How Crises Model the Modern World.”

[23] Lagadec and Topper, “How Crises Model the Modern World.”

устойчивость где-либо, кроме как в конце цикла антикризисного управления. Устойчивость – это то, над чем мы можем и должны работать, но мы должны инвестировать в нее в нужное время. Было бы нежелательно выделять и тратить ресурсы на проекты по обеспечению устойчивости в то время, когда мы заняты другими не менее важными задачами.

Сендайская рамочная программа

В 2015 году Организация Объединенных Наций приняла Сендайскую рамочную программу по снижению риска бедствий на 2015–2030 годы.[24] В соглашении, состоящем из семи глобальных целей [25] и четырех приоритетов для действий,[26] содержится призыв к более инклюзивному и последовательному подходу к урегулированию кризисов. Задача двоякая. С одной стороны, программа направлена на то, чтобы переключить внимание с реагирования на чрезвычайные ситуации (второй этап) на снижение рисков и управление ими (первый этап). С другой стороны, она стремится обеспечить глобальное согласование способов антикризисного управления. Другими словами, Сендайская рамочная программа направлена на содействие универсальному подходу, при котором движущие силы кризисов («опасности, уязвимости и уязвимые стороны») [27] выявляются, предотвращаются и уменьшаются до возникновения серьезных событий. Идея состоит в том, что кризисов можно избежать, предотвратить или, по крайней мере, ограничить, уделяя больше внимания их коренным причинам, требуя от всех участников объединения усилий.

В контексте Сендайской рамочной программы устойчивость упоминается как третий приоритет действий – *инвестирование в снижение риска бедствий для обеспечения устойчивости*.[28] Идея состоит в том, что важно инвестировать в работу, направленную на устранение движущих сил кризисов для повышения силы и способности «людей, сообществ, стран и их активов, а также окружающей среды», восстанавливаться после бедствий.[29] В

[24] “Sendai Framework for Disaster Risk Reduction 2015-2030,” United Nations Office for Disaster Risk Reduction, последнее изменение 18 марта 2015, www.undrr.org/publication/sendai-framework-disaster-risk-reduction-2015-2030.

[25] i) снижение смертности от стихийных бедствий к 2030 году; ii) уменьшить количество людей, пострадавших к 2030 году; iii) уменьшить экономические потери; iv) уменьшить ущерб от стихийных бедствий для основных товаров и услуг; v) увеличить количество государств со стратегиями снижения риска; vi) расширять международное сотрудничество; vii) расширять и улучшать ранние предупреждения.

[26] i) понимать риск бедствий; ii) усиление управления рисками стихийных бедствий для менеджмента рисков стихийных бедствий; iii) инвестировать в снижение риска бедствий для повышения устойчивости; iv) повысить готовность к стихийным бедствиям для эффективного реагирования и восстановления.

[27] “Sendai Framework.”

[28] “Sendai Framework.”

[29] “Sendai Framework.”

таком понимании устойчивость – это не альтернатива профилактике и обеспечению готовности, а их результат. Устойчивость – это «игра на конечный результат», и то, насколько хорошо пострадавшие смогут продвигаться вперед после удара кризиса, во многом зависит от работы, проделанной до того, как событие даже произошло. К сожалению, формулировка Сендайской рамочной программы расплывчата, когда речь идет об устойчивости, вероятно, потому, что в основе соглашения лежит управление рисками, а не устойчивость *как таковая*.

Далее, Сендайская рамочная программа не предлагает прямых инвестиций для повышения устойчивости; скорее, средства следует направить на мероприятия по обеспечению готовности и предупреждению, а оттуда – на проекты, связанные с обеспечением устойчивости. В условиях глобального финансового кризиса, подобного тому, который мы переживаем, можно с полным основанием усомниться в том, реалистично ли полагать, что какие-либо инвестиции дойдут до последней стадии антикризисного управления и выполнят третий приоритет для действий.[30] Более того, можно предвидеть, что по крайней мере некоторые из тех, кого Сендайская рамочная программа критикует за невыполнение своего обещания по устранению коренных причин бедствий, также начнут проявлять скептицизм в отношении устойчивости.[31] Тем не менее, способность Сендайской рамочной программы привлекать внимание к более широкому спектру антикризисного управления представляет собой ценный шаг вперед и может служить основой для дальнейшей работы над подходами, ориентированными на устойчивость.

Возможность

Хотя кризисы являются константой человеческих обществ, мы становимся свидетелями растущего числа бедствий, типа черного лебедя, которые бросают вызов нашим системам и способности реагировать. В течение последнего десятилетия мы были поглощены задачей улучшения нашего понимания кризисов и связанных с ними рисков. Сегодня у нас есть возможность завершить картину, выделив пространство для устойчивости. Если не ради того, чтобы стать сильнее, мы должны это делать, потому что это хорошее упражнение на осведомленность.

«Черные лебеди» – это новая норма

В прошлом считалось, что кризисы редко бывают непредсказуемыми, и «черные лебеди» оставались исключением.[32] Затем, десять лет назад, мы

[30] Mami Mizutori, “Reflections on the Sendai Framework for Disaster Risk Reduction,” *International Journal of Disaster Risk Science* 11 (2020): 147–151.

[31] Ben Wisner, “Five Years Beyond Sendai—Can We Get Beyond Frameworks?” *International Journal of Disaster Risk Science* 11 (2020): 239–249.

[32] Lagadec and Topper, “How Crises Model the Modern World,” 23.

поняли, что все меняется, и черные лебеди появляются чаще, чем ожидалось. Таким образом, мы стали свидетелями войн, социальных волнений, финансовых кризисов, кризисов в области здравоохранения, стихийных бедствий, технологических катастроф и промышленных катастроф, даже совпадающих друг с другом. Главный фактор, который следует учитывать при размышлениях об этой смене тенденций, – это взаимосвязанная и взаимозависимая природа сложного общества, в котором мы живем. В результате, последствия кризисов, происходящих где угодно, имеют тенденцию выходить за географические и политические границы.[33] Пандемия Covid-19 – хороший тому пример. Вспышка неизвестной болезни в Китае в конце 2019 года распространилась по миру за считанные месяцы, охватив всех – от удаленных сообществ до жителей самых доступных стран. Этот кризис в области здравоохранения также привел к возникновению гуманитарных и экономических проблем, усугубив и без того тяжелое положение многих уязвимых людей. Более того, кризис разворачивается вместе с другими чрезвычайными ситуациями, такими как сезон ураганов в Атлантике, который превышает норму, эндемический социальный беспорядок и систематические кибератаки, и это лишь некоторые из них.

Суть в том, что мы чувствуем себя хрупкими.[34] Мы понимаем, что будут происходить исключительные события, которые преобразуют нашу жизнь и целостность наших обществ. Чтобы ограничить головокружение от ощущения зависимости от неожиданности, мы решили изменить свое мышление и инвестировать в меры по обеспечению готовности и профилактике. К сожалению, похоже, что прогнозирования рисков и устранения факторов кризисов недостаточно. Итак, чтобы вселить больше уверенности, мы обратились к устойчивости. Действительно, утешительно думать, что мы выживем в любой чрезвычайной ситуации, мы извлечем из нее максимум пользы и выйдем из нее еще сильнее. Таким образом, представленная и контекстуализированная в нашем глобальном обществе, устойчивость становится упражнением по укреплению коммуникационных систем стран,[35] соглашений между организациями и альянсами,[36] а также готовности сообществ.[37]

---

[33] Daniel S. Hamilton, ed., *Forward Resilience: Protecting Society in an Interconnected World* (Washington, D.C.: Center for Transatlantic Relations, 2016).

[34] Arjen Boin, Louise K. Comfort, and Chris C. Demchak, "The Rise of Resilience," in *Designing Resilience: Preparing for Extreme Events* (Pittsburgh, PA: University of Pittsburgh Press, 2020), 1-12.

[35] P.H. Longstaff and Sung-Un Yang, "Communication Management and Trust: Their Role in Building Resilience to "Surprises" Such as Natural Disasters, Pandemic Flu, and Terrorism," *Ecology and Society* 13, no. 1 (2008): 3, https://doi.org/10.5751/ES-02232-130103.

[36] Anna Wieslander, "How NATO and the EU Can Cooperate to Increase Partner Resilience," in *Forward Resilience: Protecting Society in an Interconnected World,* ed. Daniel S. Hamilton (Washington: Center for Transatlantic Relations, 2016), 137-148.

[37] "Sendai Framework."

Это, несомненно, важные начинания, но насколько серьезно мы относимся к повышению устойчивости?

Не забыли ли мы что-то?

Слишком часто мы по второму разу используем уже известные данные, новости и информацию для разговоров об устойчивости. Мы также делаем это, используя время и ресурсы. То есть мы еще не уверены, что устойчивость заслуживает отдельного места. Конечно, мы говорим об этом, но между реакцией на кризис А и предотвращением/подготовкой к кризису В мы редко выделяем значимое время, чтобы подумать о том, как изменились наше состояние и окружающая среда, и как мы хотим двигаться вперед. Вместо этого мы берем часть средств из следующих программ профилактики и обеспечения готовности, по возможности резервируем время, извлекаем уроки, и это конец нынешних подходов, ориентированных на устойчивость. Автор утверждает, что этого недостаточно и, что еще хуже, это упущенная возможность. Выделить время для создания или повышения устойчивости означает найти место, где мы можем поработать над теми умениями, которые помогут нам восстановить нашу стабильность после отката от драматического события. Это не место, где вы планируете следующий кризис, это то место, где организация, система, человек или сообщество глубоко вздыхают и тщательно размышляют о том, что произошло, и о том, как они хотят двигаться вперед.

Между тем кризисы будут продолжаться. Если мы не предпримем сознательных усилий по включению устойчивости в нашу рутину антикризисного управления, мы все равно будем двигаться вперед, только немного более слепыми и более слабыми. Однако, к сожалению, мы еще не готовы серьезно отнестись к этому потенциалу для улучшения. Конечно, даже если мы будем больше инвестировать в устойчивость, нам все равно придется иметь дело с черными лебедями и спрогнозированными кризисами. Однако, если мы примем этот подход, у нас будет возможность воспользоваться этими негативными событиями и способствовать позитивному и устойчивому развитию внутри и вокруг наших систем. В частности, мы могли бы подойти к современным кризисам и проблемам, которые они порождают, как к возможности улучшить и вдохнуть новую жизнь в международные и внутренние системы и отношения. Мы должны выйти за пределы наших задних дворов и работать вместе как международное сообщество для развития транснациональных каналов обмена и поддержки, чтобы предотвратить, подготовиться и в конечном итоге выйти сильнее из сложных кризисов, с которыми мы сталкиваемся. Пока мы не осознаем, что устойчивость играет ключевую роль в обеспечении значимых и всеобъемлющих циклов антикризисного управления, наше кризисное планирование и меры реагирования на них, к сожалению, будут неполными.

Заключение

Слово «устойчивость» стало популярным в последнее десятилетие. Применительно к разным областям оно принимает нюансы, которые снова и снова придают ему немного разные значения. Тем не менее, идея, лежащая в основе устойчивости, остается неизменной, где бы ее ни применяли, и ее можно резюмировать словом «эластичность». В этой статье автор сосредоточился на идее устойчивости применительно к глобальным кризисам и поставил вопрос, что именно она означает и действительно ли она нужна в данном контексте. Признавая, что для ее достижения требуется тяжелая работа, автор пришел к выводу, что устойчивость является незаменимой и к ней следует стремиться, поскольку было бы прискорбно, если бы мы выйдем из текущих и будущих кризисов неизмененными.

Обнадеживает то, что мы достаточно заинтересованы, чтобы продолжить этот разговор. Это не просто вопрос формулировок или абстрактного мышления. То, как мы принимаем решение об интерпретации и обеспечении устойчивости, оказывает реальное влияние на жизнь многих людей, целостность многих систем, планы распределения средств и, что наиболее важно, на глобальный ландшафт безопасности в целом. Мы должны обмениваться идеями, искать обратную связь и слышать, что говорят другие, поскольку это способ обострить наше критическое мышление и внести правильные изменения, чтобы способствовать прогрессу в качестве глобального и тесно взаимосвязанного сообщества.

По мнению автора, Сендайская рамочная программа представляет собой интересную возможность для того, чтобы внести ясность по вопросам устойчивости. Хотя можно утверждать, что она еще не достигла своих собственных целей и что идея устойчивости в ней несколько расплывчата, Сендайская рамочная программа является одним из немногих доступных инструментов, которые предоставляют всеобъемлющий подход к кризисам. Посредством этой концепции можно сделать больший акцент на различие между приоритетами антикризисного управления до (предотвращение и готовность) и после (устойчивость). В свою очередь, это могло бы помочь более осмысленно реагировать, по крайней мере, на некоторые проблемы, связанные с кризисами, такие как распределение ресурсов и потребность в более устойчивых решениях.

Отказ от ответственности

Выраженные здесь взгляды являются исключительно взглядами автора и не отражают точку зрения Консорциума оборонных академий и институтов изучения безопасности ПрМ, участвующих организаций или редакторов Консорциума.

Благодарности

Автор благодарит членов редакционной коллегии *Connections: The Quarterly Journal*, а также доктора Маттео Тондини, полковника (ГЩ) Лорана Куррита, дона Риккардо Баттоккио и г-на Дома Джонсона за их ценную и всегда высоко ценимую поддержку.

Об авторе

Джулия Ферраро имеет образование и опыт в сфере международного права. Она начала свою карьеру в частном секторе и работала в коммерческой юридической фирме в Мельбурне, Австралия, до 2018 года, когда перешла в гуманитарную сферу. С тех пор она работала по вопросам мира и безопасности в Шри-Ланке, Колумбии и Швейцарии. На момент написания данной статьи Джулия – научный сотрудник Женевского центра политики безопасности в Швейцарии, где она участвует в проекте по обеспечению устойчивости и безопасности, а также ищет новые партнерские отношения и возможности. Джулия имеет степень магистра права в Университете Мельбурна, Австралия, и интегрированную степень магистра в Университете Каттолика дель Сакро Куоре ди Милано, Италия. Также она изучала право в Великобритании и Литве. Джулия говорит по-итальянски, по-английски, на хорошем уровне испанский, а сейчас изучает французский. *E-mail*: fg.ferrarogiulia@gmail.com

Connections: The Quarterly Journal
ISSN 1812-1101, e-ISSN 1812-2973

Б. Манойлович, *Connections QJ* 19, № 4 (2020): 127-140
https://doi.org/10.11610/Connections.rus.19.4.08

Рецензированная статья

Устойчивость к конфликтам и имидж другого среди жителей Северной и Южной Кореи

Борислава Манойлович

Школа им. Картера по вопросам мира и разрешения конфликтов, Университет им. Джорджа Мейсона, https://carterschool.gmu.edu/

Резюме: Статья призвана сформулировать ключевые факторы на микроуровне, которые способствуют устойчивости к конфликту южнокорейских и северокорейских общин, проживающих в столичной области Сеула. Концепция устойчивости на микроуровне определяется как имеющая три аспекта: признание коллективной и индивидуальной взаимозависимости, качество взаимодействия и представления, способствующие сотрудничеству и доверию. Семинар по решению проблем, проведенный с членами северокорейской диаспоры и их южнокорейскими партнерами, предоставил возможность оценить устойчивость общин к конфликту. Результаты показывают, что устойчивость можно повысить за счет обеспечения качественного взаимодействия между членами сообщества и внедрения образования, которое способствует пониманию, терпимости и уважению.

Ключевые слова: устойчивость к конфликту, решение проблем, Северная Корея, Южная Корея.

Введение

Статья призвана сформулировать ключевые факторы на микроуровне, которые способствуют устойчивости к конфликту южнокорейских и северокорейских общин, проживающих в области столицы Сеула. Идеологически, социально и экономически разнообразные сообщества представляют собой микрокосм проблем и возможностей, которые могут появиться в результате интеграции двух Корей. Концепция устойчивости к конфликту рассматривается через призму динамических систем. В частности, для изучения факторов микроуровня для обеспечения устойчивости к деструктивным конфлик-

там используется вложенная модель компонентов устойчивого мира.[1] Концепция устойчивости на микроуровне определяется как имеющая три аспекта: 1) признание общественной и индивидуальной взаимозависимости; 2) качество взаимодействия и 3) представления, способствующие сотрудничеству и доверию. Семинар по решению проблем (СРП), проведенный с членами диаспоры Северной Кореи и их южнокорейскими партнерами, послужил возможностью оценить устойчивость общин. Упражнения и анкетирование участников во время семинара по решению проблем позволили понять общую устойчивость двух сообществ, которые сталкиваются с проблемами социально-экономической интеграции и негативным восприятием друг друга.

Семинар проходил в Сонгдо, Южная Корея, с 14 участниками, которые принадлежали к северным и южнокорейским общинам, проживающим в Южной Корее. Хотя общественная устойчивость требует продольного и многоуровневого исследования, эта статья дает представление о восприятиях участников, выявленных с помощью опросов и упражнений по решению проблем. Семинар по решению проблем был сосредоточен на выявлении проблем, с которыми общины сталкиваются в повседневном взаимодействии, на том, как они справляются с различиями и проблемами. Результаты показывают некоторые предварительные выводы о том, как сообщества могут стать более устойчивыми к конфликтам за счет качественного взаимодействия между членами сообщества и внедрения образования, которое способствует пониманию, терпимости и уважению.

Семинары по решению проблем

С 28 по 29 сентября 2019 года Азиатский центр исследований мира и конфликтов (PACSC Asia) провел двухдневный семинар по решению проблем (СРП) на Корейском кампусе IGC в Сонгдо с участием 14 жителей южнокорейских и северокорейских общин в Южной Корее. Семинар – это устоявшаяся практика по вопросам миростроительства и урегулирования конфликтов, которая предоставляет неформальный, с низким уровнем риска, ни к чему не обязывающий форум, на котором неофициальные представители могут в частном порядке анализировать различные вопросы, выявлять проблемы и участвовать в процессах активного решения этих проблем.[2] Целью семинара было дать представление о ключевых идеях и взглядах жителей Северной и Южной Кореи, проживающих в Южной Корее, о лучших способах решения проблем интеграции и сосуществования по мере продвиже-

[1] Robin R. Vallacher, Peter T. Coleman, Andrzej Nowak, Lan Bui Wrzosinska, Larry Liebovitch, Katharina Kugler, and Andrea Bartoli, *Attracted to Conflict: Dynamic Foundations of Destructive Social Relations* (New York: Springer, 2014).

[2] Dean Pruitt, Sung Hee Kim, and Jeffrey Z, Rubin, *Social Conflict: Escalation, Stalemate, and Settlement* (Boston, MA: McGraw-Hill, 2004).

ния процесса воссоединения. Семинар предоставил членам северокорейской диаспоры безопасное место, чтобы поделиться своим опытом и пообщаться с другими людьми, столкнувшимися с аналогичными проблемами при адаптации к южнокорейскому обществу. Участники обсуждали актуальные вопросы в неформальной, конфиденциальной, безопасной и сдержанной обстановке.

СРП проводился в течение двух дней. Он состоял из лекций, групповой работы, а также структурированных упражнений и дискуссий, в ходе которых были выработаны конкретные идеи по основным вопросам и стратегиям решения проблем, которые могли послужить источником информации для политики в отношении будущих усилий по миростроительству и способствовать устойчивости общества к конфликтам. Вместе с коллегами и студентами семинар провела д-р Борислава Манойлович, которая разработала конкретные программные мероприятия, чтобы помочь участникам выявлять и анализировать проблемы, находить решения, создавать команды и использовать навыки разрешения конфликтов для более глубокого понимания сути вопросов и предлагать креативные идеи. Студенты университета Джорджа Мейсона из PACSC Asia работали переводчиками, ведущими дискуссий, стенографистами и логистами во время семинара.

Чтобы результаты имели статистическую значимость, потребуется большее количество участников семинара. Тем не менее, вклад этого исследования заключается в его предварительных выводах, полученных на уникальной площадке – семинарах по решению проблем, – в которых участники из обеих сообществ могли общаться лицом к лицу и вести углубленное обсуждение ключевых вопросов. Такого места для свободных и открытых дискуссий между двумя общинами в обеих корейских государствах практически не существовало. Таким образом, СРП предоставили уникальное и безопасное место для сбора как качественных, так и количественных данных на меньшей выборке, что позволило получить первоначальное представление об общих проблемах. Хотя выборка была ограниченной, объем и глубина собранных данных были значительными. Результаты этого исследования показывают, что восприятие людей друг друга в первую очередь формируется в результате межобщинного взаимодействия, и качественный контакт может существенно повлиять на будущие отношения в сообществах.

Обзор литературы

Прежде чем углубляться в данные, собранные во время СРП, важно обсудить уже проведенные исследования отношений и настроений северных и южных корейцев друг к другу и возможности интеграции. Ким и Чан рассказывают о растущей апатии южнокорейцев к северокорейцам, живущим на

юге.[3] Национальный опрос Корейского института национального объединения в 2005 году показал, что южнокорейцы испытывают меньшую степень чувства соотечественничества и враждебности по отношению к северокорейским беженцам по сравнению с результатами предыдущих лет. Большинство из них сообщили, что у них «не было особых эмоций» по отношению к другому. С другой стороны, северокорейцы, живущие в южнокорейском обществе, сообщали, что чувствуют себя «эмоционально далекими» от своих южнокорейских соседей. Авторы объясняли, что такое безразличие друг к другу часто может вызвать взаимное недоверие, а случаи, когда южнокорейцы совершали мошенничества против северных корейцев, только усиливали негативное представление северокорейцев.

Статья Чо анализирует Южную Корею с точки зрения Северной Кореи по трем направлениям. Во-первых, «воображаемое я» Южной Кореи неотделимо от Северной Кореи.[4] Фраза «Мы такие же корейцы» обобщает мнение о том, что северокорейцы подчеркивают исторические корни, общие с южнокорейцами. Второй образ Южной Кореи – это «испорченное, но сильное я», в котором Южная Корея рассматривается как общество, которое необходимо спасти от империализма США. Северокорейские СМИ часто описывают Южную Корею как колонию западного мира.

Следовательно, люди Юга считаются наивными и склонными к забыванию. Наконец, Южная Корея считается «угрожающим другим», обладающим опасными и враждебными качествами, которые бросают вызов северокорейскому режиму. Важно помнить, что образы, которые Северная Корея представляет себе об Юге, коммуникируются и подвергаются цензуре северокорейским правительством, но существует пробел в знаниях о взглядах самих жителей Северной Кореи на свои Южные партнеры.

Согласно данным опросов общественного мнения, проведенных Азиатским институтом общественных исследований, похоже, что у южнокорейцев разные поколения имеют разное отношение к северокорейцам.[5] Сообщалось, что более негативное восприятие сильнее среди людей в возрасте 20 лет и пожилых людей (60 лет и старше). Промежуточные возрастные группы обычно считали северных корейцев «соседями» и «одними из нас», в то время, как более молодое и старшее поколения воспринимали их как «врагов» или «чужих». Более пристальный взгляд на результаты опроса показал, что многие молодые люди в Южной Корее выступают против государственного финансирования Северной Кореи и не испытывают сочувствия к социально-экономическому положению большинства людей там.

---

[3] Jihun Kim and Dongjin Jang, “Aliens among Brothers? The Status and Perception of North Korean Refugees in South Korea,” *Asian Perspective* 31, no. 2 (2007): 5-22.

[4] Young Chul Cho, “North Korea’s Nationalistic Discourse: A Critical Interpretation,” *Korea Observer* 42, no. 2 (Summer 2011): 311–43.

[5] Ji-yoon Kim, Chung-ku Kang, and Kil-dong Kim, “To South Korean Youth, North Korea Is Not ‘One of Us’,” *The Korea Times*, May 1, 2018, www.koreatimes.co.kr/www/nation/2018/05/103_248242.html.

Более того, среди 20-летних и пожилых людей существует общее опасение, что в любой момент между двумя Кореями может вспыхнуть война. Основываясь на этой вере, их образ друг друга в первую очередь формировался недоверием и опасениями.

Недоверие между двумя общинами также было показано в некоторых популярных телешоу. Например, «На нашем пути к встрече с вами» – это телевизионная программа в Южной Корее, в которой северокорейских беженцев приглашают рассказать о своем опыте жизни и адаптации на юге. В эпизоде под названием «Южнокорейские стереотипы по отношению к северным корейцам»[6] бывшие северокорейцы подчеркнули, что их часто воспринимают как сторонников режима Кима. Один из собеседников поделился, что всякий раз, когда появлялись заголовки новостей о северокорейских ракетных испытаниях, его соседи критиковали и избегали его только потому, что он был с Севера. Однако он обратил внимание на то, что режим и народ не являются «одним целым».

Обзор литературы показывает, что на большую часть межобщинных представлений влияние оказывали повседневные события и публичный дискурс, исходящий из средств массовой информации, новостей и других общественных платформ, а не личное взаимодействие. Однако результаты этого исследования показывают, что восприятие людей по отношению к друг другу в первую очередь формируется через взаимодействие, а не через средства массовой информации. Хотя текущая политическая ситуация затрудняет взаимодействие между северокорейцами и южнокорейцами через государственные границы, усилия по мирной интеграции могут начаться через взаимодействие с членами северокорейской диаспоры, которые уже находятся в Южной Корее. Как показывают результаты этого исследования, высокий уровень неуверенности и недоверия к другому может быть устранен за счет более качественных контактов и образование, которое способствует пониманию, терпимости и уважению.

Участники

В семинаре участвовало четырнадцать человек. Большинство участников, десять, принадлежали к северокорейской диаспоре, а четверо были членами принимающей южнокорейской общины. Участники были набраны через контакты с неправительственными организациями, образовательными учреждениями и через рекламу, размещенную в социальных сетях. Поскольку участники в разной степени владели английским языком, на протяжении всех занятий студенты Университета Джорджа Мейсона выполняли синхронный перевод. Что касается пола и возраста, то было десять женщин и четыре мужчины; восемь участников принадлежали к возрастной группе

[6] "South Korean Stereotypes towards North Koreans," *On Our Way to Meet You*, Channel A, September 10, 2017. https://tv.naver.com/v/2048839.

18-35 лет, а 6 участников – к возрастной группе от 36 до 60 лет. По уровню образования большинство участников имели степень бакалавра.

Сбор данных

Семинар по разрешению проблем с участием членов северокорейской диаспоры и их южнокорейских коллег предоставил двум общинам возможность активно взаимодействовать и оценить устойчивость общин к конфликту. СРП были сосредоточены на выявлении проблем, с которыми общины сталкиваются в повседневном взаимодействии, и на том, как они справляются с различиями. Данные были собраны с помощью опроса и упражнений по решению проблем. Чтобы получить более подробные и качественные ответы, участники были разделены на три группы примерно по пять человек, которые участвовали в упражнениях «дерево решения проблем». Каждая группа создавала свое собственное дерево, указав основные проблемы, которые они помещали в ствол дерева. Затем они перечисляли причины и, наконец, связывали проблемы с результатами в ветвях дерева.

Участникам было предоставлено достаточно времени, чтобы построить дерево по теме устойчивости к конфликтам и интеграции как группы, и на следующий день участники делились результатами. Собранные данные были проанализированы путем изучения индикаторов трех аспектов устойчивости на микроуровне:

1) признание общественной и индивидуальной взаимозависимости и интеграции
2) качество взаимодействия
3) представления, способствующие сотрудничеству и доверию.

Анализ данных

Упражнения по решению проблем

В этом разделе я исследую проблемы, основные причины и результаты, выявленные участниками упражнений по решению проблем. Многие проблемы, связанные с трудностями в достижении мирного сосуществования и интеграции, связаны с культурными различиями между северными и южными корейцами. Хотя эти две общины имеют общую историю и этнические традиции, 70-летнее разделение при очень разных системах управления привело к культурному разделению. Различия в стилях общения были названы одной из важных проблем, с которыми столкнулись сообщества. Например, северокорейцы, как правило, более прямолинейны и склонны говорить откровенно, в то время как южнокорейцы более уклончивы и используют высоко контекстный язык, который показывает их социально-экономический статус, положение и возрастную группу.

Еще одна проблема, указывающая на культурные различия, заключалась в том, как северокорейцы относились к оплачиванию счета в ресторане. Для северных корейцев обычай «каждый платит за себя» кажется довольно

«бессердечным», отстраненным и даже грубым. В то время как среди южнокорейцев принято оплачивать свои счета, платя отдельно или разделяя причитающуюся сумму, северные корейцы более привыкли к тому, что по очереди покупают еду или расплачиваются другими способами. «Культурный шок», который испытывают северокорейцы по прибытии в Южную Корею, аналогичен опыту иностранца, приехавшего в Корею. Один участник отмечает, что «умственные и эмоциональные проблемы, с которыми мы сталкиваемся, напоминают типы проблем, которые дети третьей культуры (ДТК), например дети-миссионеры, испытывают при репатриации». Различные культурные, коммуникативные и языковые практики в повседневной жизни сообществ свидетельствуют об отсутствии взаимозависимости и интеграции между общинами и отдельными людьми, что может негативно сказаться на устойчивости общества к конфликтам.

Другие вопросы, которые были подняты участниками, показали отсутствие доверия, с которым оба сообщества сталкиваются на личном и родственном уровне. Например, северокорейцы указали, что они ежедневно общались и разговаривали со своими южнокорейскими соседями, но при этом им казалось, что между ними все еще существует «стена», которую они не могут преодолеть. Один северокорейский участник использовал термин «ориентализм», чтобы объяснить отношение к нему жителей Южной Кореи, когда они впервые узнали, что он «дезертировал с Севера». Участники из Северной Кореи отметили, что существует мнение о том, что они «нецивилизованные», «необразованные», «неискушенные» или даже что они «получали слишком много сочувствия» из-за сильной травмы, которую они, должно быть, перенесли, когда жили при режиме Кима. Как раз наоборот, большинство северокорейских участников семинара имели как минимум степень бакалавра, и многие из них учились, чтобы получить степень магистра в Южной Корее. Кроме того, некоторые были выходцами из довольно богатых семей и не описывали свою жизнь в Северной Корее как «травмирующую». Как отметил один участник, «северокорейский коллективизм сильнее южнокорейского коллективизма». Под этим он имел в виду, что отношение Северной Кореи к корейской культуре и самобытности было более консервативным и старомодным. Он также говорил о необходимости северокорейцев принадлежать к внутренней группе, которая обеспечивала безопасность, в то время как посторонним обычно не доверяли не только потому, что они жили изолированно до прихода на юг, но и потому, что они считали южных корейцев более вестернизированными и, следовательно, по умолчанию менее надежными.

По мнению участников, первопричины, которые создали условия для межобщинного недоверия и стереотипов, включают изоляцию Северной Кореи от остального мира и разрыв поколений, который мешает южнокорейцам и северокорейцам иметь последовательное отношение или знание о другом. Важный вывод заключался в том, что восприятие южнокорейцами северокорейской диаспоры было основано на недостатке информации и

знаний, которые могут быть получены только при личном общении. Это привело к формированию стереотипов и недоверия, которые могут создать угрозу устойчивости общества и прочному миру.

Язык, на котором говорят в Южной Корее, полон недавно принятых западных слов, которые северокорейцам не только трудно понять, но и трудно принять. Например, некоторые повседневные южнокорейские слова, заимствованные из английского языка, такие как «псевдоним», «личность» и «тур», имеют свои эквиваленты в корейском языке, но люди в Южной Корее предпочитают использовать западную версию. Как упоминалось в обзоре литературы, молодое поколение южнокорейцев проявляло очень мало интереса к сосуществованию и совместной жизни со своими северокорейскими сверстниками. Участники утверждали, что отсутствие интереса было связано с плохим образованием в отношении интеграции среди молодежи. Как отметил один участник:

> … Постоянно слышатся голоса о сосуществовании и интеграции двух Корей, это голоса международных организаций и Южной Кореи, но голоса и мнения, исходящие от северокорейцев или молодежи, не слышны.

Следовательно, возможное мирное решение и воссоединение не могут стать реальностью, пока все нынешние и будущие заинтересованные стороны не получат право голоса по этому вопросу.

Из-за социальных, экономических и культурных различий, связанных с воспитанием в разных системах, среди членов сообщества наблюдалось острое непонимание, что часто приводило к негативному восприятию и недоверию по отношению к другим. Однако отдельные члены обоих сообществ постоянно пытались сбалансировать свое личное и коллективное «я», особенно когда сталкивались с предполагаемой угрозой. Им нужно было отличаться от группы, чтобы сохранить части своей индивидуальной уникальности и идентичности, особенно когда их групповая идентичность не считалась выгодной. Как выразился один из участников, «северные корейцы не все одинаковые. Мы хотим, чтобы нас воспринимали как субъектов, отличных от нашего лидера и его режима». Другими словами, восприятие южнокорейцев, что все северные корейцы являются «детьми Ким Чен Ына», и восприятие северокорейцев, что все южнокорейцы «дерзки, эгоистичны и пассивны», были препятствием на пути к улучшению отношений между двумя группами. Это явление называется «унитарной ловушкой», что означает тенденцию помещать целую группу людей в одну коробку, которая блокирует сообщества в борьбе за идентичность. Выход из унитарной ловушки это разоблачение стереотипов, неточностей и слухов, что является ключевым шагом на пути к достижению устойчивости к конфликтам.

Опрос

Данные опроса позволили получить дополнительное представление о восприятии северокорейцев и южнокорейцев друг о друге. Вывод из упражнений СРП о том, что личное взаимодействие является ключевым фактором,

формировавшим отношение участников к другим, был подтвержден в опросе большинством участников (см. Таблицу 1).

Таблица 1. Что оказало влияние на ваше отношение к южным/северным корейцам?

#	Ответ	%	Число респондентов
1	Личное взаимодействие с ними	50	8
2	Новости и документальные фильмы	18.75	3
3	Политическая идеология	12.5	2
4	Развлекательные СМИ (фильмы, музыка, искусство, спорт и т. д.)	6.25	1
	Всего	100	14

Большинство участников из Южной и Северной Кореи (82 %) указали, что слова, которые лучше всего описывают их восприятие другой группы, были «один из нас» и «сосед», в то время как 16 % участников воспринимали членов другой группы, как «чужие» (см. Таблицу 2).

Таблица 2. Какое слово лучше всего описывает ваше отношение к южным/северным корейцам?

#	Ответ	%	Число респондентов
1	Один из нас	41.67	5
2	Сосед	41.67	5
3	Чужой	16.67	2
4	Враг	0	0
5	Неприменимо (нейтральный)	0	0
	Всего	100	12

Участники определяли остальных как «чужих», потому что были различия в языке, культуре и происхождении, в то время как большинство подчеркнули, что, поскольку все они в настоящее время живут на Юге, было естественно думать, что «мы были одним целым». Южнокорейские участники отметили разницу между северокорейцами, живущими на юге, и теми, что живут на Севере:

> Благодаря личному общению с северокорейской диаспорой я чувствую, что мы одно целое. Однако я чувствую это только по отношению к северокорейцам, которые находятся в Южной Корее. Для тех, кто на Севере, я бы считал их иностранцами.

На вопрос о будущей совместной жизни и сосуществовании 50 % участников были нейтральны, а 50 % согласились, что совместное будущее возможно (Таблица 3). Это интересное наблюдение, которое указывает на неоднозначность статуса их стран и недоверие, которое существует среди сообществ. По словам участников, основными препятствиями на пути к интеграции и совместной жизни были режим в Северной Корее, неудачные переговоры, доступ к информации о каждой стране и культурные различия. Положительные стороны интеграции были теми же – язык, те же национальные корни, конфуцианские культурные обычаи и история, которые веками связывали народ Корейского полуострова.

Таблица 3. Возможно ли мирное сосуществование Северной и Южной Кореи в будущем?

#	Ответ	%	Число респондентов
8	Категорически согласен	7.14	1
9	Согласен	42.86	6
10	Нейтрален	50	7
11	Не согласен	0	0
12	Категорически не согласен	0	0
	Всего	100	14

Однако общая национальная и этническая идентичность не была достаточно сильным стимулом для участников, чтобы договориться о возможности мирного сосуществования двух государств. Хотя большинство участников считали северных и южных корейцев одной и той же нацией (см. Таблицу 4), обе общины не имеют однозначного ответа и не уверены, могут ли два национальных государства сосуществовать.

Качественные ответы участников показали, что природа двух государств настолько различалась, что даже люди, принадлежащие к одной этнической и культурной среде, не могли увидеть, чтобы две системы работали бы бок о бок или были бы объединены, если не произойдет серьезных идеологических изменений.

Таблица 4. Считаете ли вы, что северные и южная корейцы - одна и та же нация?

#	Ответ	%	Число респондентов
1	Категорически согласен	50	7
2	Согласен	42.86	6
8	Нейтрален	7.14	1
9	Не согласен	0	0
10	Категорически не согласен	0	0
11	Другое	0	0
	Всего	100%	14

Еще один интересный результат опроса заключался в том, что большинство перебежчиков из Северной Кореи чувствовали, что они подвергаются дискриминации в Южной Корее (см. Таблицу 5).[7]

Table 5. Have You Ever Experienced Discrimination in South Korea as a North Korean?

#	Вопрос	%	Число респондентов
1	Категорически согласен	12.5	1
2	Согласен	50	4
3	Нейтрален	25	2
6	Не согласен	0	0
7	Категорически не согласен	12.5	1
	Всего	100	8

Непонимание часто происходило из-за разницы между языком хангыль в Южной Корее, с его большим притоком западной лексики, и северокорейским диалектом, который подчеркивает чистоту языка. Один участник заявил:

[7] Обратите внимание, что общее количество ответов на разные вопросы разное, потому что участники пропустили некоторые вопросы в опросе. Например, несмотря на 14 участников, только 8 или 12 ответили на определенный вопрос. Более того, некоторые вопросы (таблица 5) были адресованы только конкретному сообществу, например, северокорейцам.

> Я постоянно слышал, как они уничижительно отзывались о северокорейских перебежчиках и ставили под сомнение наши истинные мотивы перехода на юг. Тон голоса людей меняется, когда они понимают, что разговаривают с перебежчиком из Северной Кореи, что сразу же ставит нас в невыгодное положение во время собеседований и публичных мероприятий.

Другая участница подтвердила предыдущий пункт, заявив: «Когда я сказала директору детского сада моего ребенка, что я перебежчик из Северной Кореи, ее отношение изменилось. Она стала холодной и нелюбезной».

Отвечая на вопрос об их надеждах и целях на будущее, участники из Северной Кореи отметили важность недискриминации и свободы жизни в Южной Корее. В то время как надежды южнокорейцев были шире и более общими, у северокорейцев, казалось, были более конкретные надежды и мечты, которые варьировались от улучшения ухода за своими пожилыми родственниками и создания в Южной Корее системы образования об объединении до посещения своих родных городов и семей на Севере. Обе группы возлагали большие надежды на то, что боль разделения и проблема разлученных семей будет решена в ближайшем будущем.

Выводы и заключения

Разговоры о сосуществовании, устойчивости и интеграции ограничиваются очень немногими пространствами в нынешнем южнокорейском обществе. Несмотря на одинаковое этническое и культурное происхождение, жители Северной и Южной Кореи не могут увидеть две политические системы, работающие бок о бок или объединенные, если не произойдет серьезных политических и социальных изменений, особенно в Северной Корее. Более 30 000 северокорейских перебежчиков, которые в настоящее время проживают в Южной Корее, постоянно напоминают о том, что есть другое общество всего в нескольких милях от Сеула, которое изгнало этих перебежчиков и заставило их стать беженцами. В новом обществе северокорейцы часто сталкиваются с трудностями, пытаясь быть принятыми и понятыми своими хозяевами. Различные культурные, коммуникативные и языковые практики в повседневной жизни сообществ показывают отсутствие взаимозависимости и интеграции.

Это исследование также показывает, что восприятие людей друг другом в основном формируется через взаимодействие. Качественное взаимодействие крайне необходимо для продвижения справедливости и непредвзятого отношения. Расширение контактов и сотрудничества между общинами Северной и Южной Кореи через такие платформы, как СРП, может укрепить потенциал для сотрудничества и устойчивости к конфликтам на общинном

уровне, что является предварительным условием для более широкого процесса интеграции. Согласно гипотезе о контакте Олпорта,[8] межгрупповые отношения могут быть улучшены за счет качественного контакта при соответствующих обстоятельствах. Качественный контакт может бросить вызов изначальному предубеждению, которое порождало непонимание, плохую коммуникацию и иррациональный страх перед другим.[9]

Поскольку практика разрешения конфликтов все еще относительно нова для Кореи, необходимо больше экспертов и активистов, которые готовы привлекать сообщества и выполнять работу на низовом уровне. Приоритетом должно оставаться наличие опытных фасилитаторов, которые понимают местные потребности, контекст и ситуации для проведения будущих семинаров и диалогов. Хотя текущая политическая ситуация затрудняет взаимодействие между северокорейцами и южнокорейцами через государственные границы, усилия по мирному сосуществованию могут начаться через взаимодействие с членами северокорейской диаспоры, которые уже находятся в Южной Корее. Как показывают результаты этого исследования, высокий уровень неуверенности и недоверия друг к другу может быть устранен за счет более качественного контакта и обучения на низовом уровне, которое способствует пониманию культурных различий, терпимости и уважения.

Помимо качественного взаимодействия, система образования выиграет от включения новой учебной программы по воссоединению в программы начальных и средних школ в Южной Корее. Цель обучения по воссоединению – не заставить учащихся думать, что воссоединение необходимо и должно произойти любой ценой, а побудить их думать самостоятельно о будущем и той роли, которую они, возможно, захотят сыграть в процессе миростроительства.

Одним из самых интересных аспектов семинара было активное участие в обсуждениях как южных, так и северных корейцев. Люди стремились выразить свои взгляды и горячо доносили свои мысли. Более того, они не боялись задавать вопросы другим и фасилитаторам. Участники не казались запуганными, не чувствовали себя неудобно в новой обстановке, и были счастливы открыто делиться своими историями. Хотя общее влияние СРП невозможно было измерить на данном этапе, участники сочли этот формат расширяющим возможности. Рассказывая о своем опыте, участники продемонстрировали устойчивость, сильную волю и настойчивость. Таким образом, они могли организовать свои воспоминания, обработать эмоции и понять, кто они. Поскольку цель СРП заключалась не в том, чтобы предложить прямые решения или ответы, а в том, чтобы способствовать пониманию и

---

8 Gordon W. Allport, *The Nature of Prejudice: 25th Anniversary Edition*, Unabridged (New York: Basic Books, 1979).

9 Buhle Zuma, “Contact Theory and the Concept of Prejudice: Metaphysical and Moral Explorations and an Epistemological Question,” *Theory & Psychology* 24, no.1 (2014): 40-57.

осознанию ключевых проблем, семинар дал участникам новую возможность, предоставив им безопасное место для обмена своими историями.

Отказ от ответственности

Выраженные здесь взгляды являются исключительно взглядами автора и не отражают точку зрения Консорциума оборонных академий и институтов изучения безопасности ПрМ, участвующих организаций или редакторов Консорциума.

Об авторе

Борислава Манойлович, доктор философии, ассистент Школы мира и разрешения конфликтов им. Картера Университета им. Джорджа Мейсона. Она является экспертом в области миростроительства, правосудия переходного периода, обращения с прошлым, образования по вопросам мира и предотвращения зверств. До того, как присоединиться к академическим кругам, она более сми лет работала с Организацией Объединенных Наций и Организацией по безопасности и сотрудничеству в Европе по вопросам меньшинств и примирения как в Хорватии, так и в Косово. Ее книга «*Образование для устойчивого мира и устойчивых к конфликтам сообществ*» была опубликована Palgrave Macmillan в 2018 году. Профессор Манойлович получила степень магистра в Университете Брандейса и докторскую степень в Школе мира и разрешения конфликтов имени Джимми и Розалин Картер Университета Джорджа Мейсона.
E-mail: bmanojlo@gmu.edu

Connections: The Quarterly Journal
Правила подачи рукописей

Журнал *Connections* принимает рукописи в объеме от 2 000 до 5 000 слов, в ясном стиле, для целевой аудитории, включающей компетентные лица, занимающиеся практикой или академической деятельностью, связанной с обороной и безопасностью. Все рукописи подаются в редакционный отдел журнала *Connections* в электронном виде по адресу PfPCpublications2@pfp-consortium.org. В верхней части первой страницы должны быть указаны имя автора, учреждение, с которым в настоящее время связан автор и предварительное название статьи. В случае необходимости рукопись снабжается подстрочными замечаниями. Кроме того, авторы должны предоставить рукопись резюме и ключевых слов.

В число предпочтительных тем для будущих выпусков журнала входят:

- Эксплуатация и безопасность Арктики
- Контроль над вооружениями и перевооружение Европы
- Вызовы и возможности общего использования разведывательных ресурсов
- Противодействие и превенция насильственного экстремизма
- Кибербезопасность
- Строительство институций обороны
- Будущие сценарии безопасности
- Гибридная война
- Ограничения военно-морской мощи
- Миграция и беженцы
- Нестабильная периферия НАТО
- Россия Путина: угроза миру или угроза для себя?
- Терроризм и иностранные боевики
- Тенденции в организованной преступности

По вопросам, касающимся подстрочных замечаний и ссылок, пожалуйста, используйте *Chicago Manual of Style*. Инструкции на оформление можно найти по адресу: www.chicagomanualofstyle.org/tools_citationguide.html.

Рукописи, выходящие за рамки приоритетных тем, принимаются в порядке поступления по усмотрению Редакционного совета.

Мнения, выраженные во всех публикациях Connections, являются исключительно точками зрения авторов и не являются официальными точками зрения Консорциума военных академий и институтов по изучению вопросов безопасности в рамках программы «Партнерство ради мира», участвующих организаций или редакторов Консорциума.

Оперативный отдел Консорциума военных академий и институтов по изучению безопасности в рамках программы «Партнерство ради мира» расположен в Европейском центре по изучению вопросов безопасности им. Джорджа К. Маршалла.

По всем вопросам, касающимся журнала CONNECTIONS, пожалуйста связывайтесь с:

Partnership for Peace – Consortium
Managing Editor – LTC Torsten Stauffer
Gernackerstrasse 2
82467 Garmisch-Partenkirchen, Germany
Phone: +49 8821 750 2333
E-Mail: PfPCpublications2@marshallcenter.org

ISSN 1812-1101