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.

Благодарность

Connections: The Quarterly Journal, Vol. 19, 2020, вышел при поддержке правительства США.

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