УДК 341 DOI: 10.31249 /iajpravo/2026.03.17

ГРОГОЛЬ А.Г.[1] РЕЦЕНЗИЯ НА КНИГУ: ЦИФРОВАЯ УСТОЙЧИВОСТЬ: МЕЖДУНАРОДНЫЕ И НАЦИОНАЛЬНЫЕ ПРАВОВЫЕ МЕРЫ ПО ОБЕСПЕЧЕНИЮ КИБЕРБЕЗОПАСНОСТИ И РАЗВИТИЮ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА / под ред. Д. Стивенса, М. Стаббса, С. Уайта.
GROGOL A.G. Book review: Digital Resilience: International and Domestic Legal Responses to Cyber Security and Artificial Intelligence / ed. D. Stephens, M. Stubbs, S. White. – 2025. – Singapore: Springer. – 209.

Ключевые слова: право Австралии; кибербезопасность; искусственный интеллект; правовое регулирование; киберугрозы; цифровой суверенитет; цифровая устойчивость; корпоративная ответственность.

Keywords: law of Australia; cybersecurity; artificial intelligence; legal framework; cyber threats; digital sovereignty; digital resilience; corporate responsibility.

Для цитирования: Гроголь А.Г. [Рецензия] // Социальные и гуманитарные науки. Отечественная и зарубежная литература. Сер. 5: Государство и право. – 2026. – № 1. – С. 228–236. – Рец. на кн.: Digital Resilience. International and Domestic Legal Responses to Cyber Security and Artificial Intelligence / ed. D. Stephens, M. Stubbs, S. White. – Singapore: Springer, 2025. – 209 p. – DOI: 10.31249 /iajpravo/2026.03.17

Исследование, опубликованное международной издательской компанией «Шпрингер», специализирующейся на издании академических журналов и книг, вышло в свет под редакцией двух профессоров юридического факультета Аделаидского университе-

[1] *Гроголь Анастасия Георгиевна,* младший научный сотрудник отдела правоведения ИНИОН РАН.

та (Австралия) – Дейла Стивенса, Мэтью Стаббса, и их помощника-ассистента Сэмюэла Уайта.

Эта книга написана по итогам конференции по кибербезопасности, проведенной 4 сентября 2023 г. в Университете Аделаиды, в которой приняла участие группа правительственных и академических экспертов. В ней представлены возможные меры, которые Австралия может предпринять для сдерживания угроз кибербезопасности и реагирования на них, рассматриваются вопросы юридической ответственности за кибербезопасность и применения искусственного интеллекта. В этом исследовании представлен всесторонний анализ правовой базы и политики кибербезопасности в Австралии, а также обзор угроз в сфере кибербезопасности и ИИ. Справедливо утверждение, что данная монография является авторитетным источником для выработки подходов в понимании границ дозволенного поведения субъектов, участвующих в кибероперациях, а подробное описание возможных угроз и рисков позволяет внести просветительский аспект в отношении основных пользователей, вовлеченных в цифровое пространство: индивидуальных пользователей, субъектов малого и среднего предпринимательства, высших учебных заведений, научных центров и органов государственного управления (p. 1).

Содержание книги разделено на 15 глав, различных по объему и содержанию, В каждой главе рассматривается определенное направление в рамках анализируемого авторами объекта исследования. Д. Стивенс и М. Стаббс придерживаются позиции, что современные государства сохраняют прагматичный подход в вопросах национальной кибербезопасности, понимая невозможность полного искоренения всех потенциальных угроз до полной адаптации цифровых систем к эффективному функционированию даже в случае кибератак и иных нежелательных последствий. А это означает поиск и внедрение государствами защитных, восстановительных и обучающих механизмов, позволяющих предупреждать и нейтрализовывать несанкционированные атаки (ibid).

Применительно к политико-правовому полю Австралии и мирового сообщества плодотворным представляется рассматривать такой переход с учетом двух ключевых факторов. Во-первых, данные, хранящиеся в основном в цифровом формате, уже к 2023 г. превратились в критический ресурс, при этом не был решен вопрос уязвимости цифровых систем. Это, вероятно, объясняет причину появления новых серьезных рисков цифровой безопасности в корпоративных и государственных структурах. В отчете

Австралийской комиссии по ценным бумагам и инвестициям (the Australian Securities and Investment Commission, ASIC) многократно указывается требование о необходимости противодействия киберрискам на уровне корпоративного руководства и через акты внутреннего корпоративного управления, а приведенный авторами результат опроса Австралийского института директоров компаний (Australian Institute of Company Directors, AICD) подтверждает, что кибербезопасность в корпоративном секторе является первостепенной проблемой. Во-вторых, авторы сходятся во мнении, что цифровые платформы являются орудием влияния на людей, а цифровая среда – ареной стратегического противоборства между национальными интересами и попытками иностранного вмешательства.

Похвально то, что Д. Стивенс и М. Стаббс обратили внимание на возросшее число попыток замаскированного посягательства иностранных государств на национальные интересы Австралии и других государств через финансирование хакерских кибератак. По мнению ученых, такие специфические формы посягательства на цифровой суверенитет и попытки оказания давления на общественное мнение и политические настроения социальных групп через киберпространство являются прямым следствием информационной войны (p. 2).

Анализируя положения Стратегии кибербезопасности правительства Австралии на 2023–2030 гг. (Australia Cyber Security Strategy) (далее – Стратегия)[1], авторы отмечают взаимосвязь устойчивости цифровой экономики и безопасности персональных данных, инфраструктуры данных и стратегически важных систем. В Стратегии декларируется необходимость создания надежных основ кибербезопасности как в системе органов государственного управления, так и в промышленном секторе. Данная Стратегия содержит шесть способов повышения устойчивости в регионах Австралии: 1) образование для граждан и хозяйствующих субъектов с целью информирования о существовании киберугроз, 2) разработка безопасных технологий, 3) обмен информацией о киберугрозах между государством и корпоративным сектором, 4) защита инфраструктуры стратегического значения, 5) создание эффективной киберэкосистемы в сфере информационной безопас-

[1] 2023–2030 Australian Cyber Security Strategy: сайт. – URL: https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security/strategy/2023-2030-australian-cyber-security-strategy (дата обращения: 19.10.25)

ности, 6) поддержка международного сотрудничества через укрепление партнерских отношений с дружественными государствами и взаимообмен опытом с целью двустороннего повышения уровня кибербезопасности.

В соответствии с разд. 1 Стратегии в целях лучшей защиты граждан и предприятий от киберугроз и кибератак, необходимо определить уровень ответственности за обеспечение устойчивой кибербезопасности для тех физических и юридических лиц, которые способны в большей степени с ними справиться. Так, крупные компании и предприятия могут играть центральную роль в поддержании экономической безопасности. В связи с этим в книге большое внимание уделяется корпоративным, государственным и стратегическим компонентам киберустойчивости и двум аспектам этого понятия: инженерная устойчивость, выражающаяся в способности противостоять внешним факторам и быстрому возвращению систем в изначальное состояние, и экологическая устойчивость, характеризующаяся быстрой адаптацией системы к негативным последствиям и восстановлению ее нормального функционирования (p. 3).

Важно то, что С. Уайт в этой же главе пишет о роли и пользе применения норм международного права, а проводит анализ нескольких норм международного права на их способность регулировать вопросы кибербезопасности. Автор исследует потенциальные и фактические сложности в регулировании киберугроз международными актами, при этом отмечает неустойчивый их характер по двум вышеуказанным компонентам: инженерному и экологическому. По мнению С. Уайта, в современных реалиях международное право неспособно эффективно реагировать на угрозы кибербезопасности, особенно в контексте операций по предотвращению угрозы иностранного вмешательства (interference operations) (далее – IOs). Это демонстрирует ограниченность международного права в данной области и закладывает основу для поиска и изучения внутренних средств правовой защиты, так как IOs, по мнению Сэмюэла Уайта, следует рассматривать как прямое нарушение государственного суверенитета. Вместе с тем, как считает ученый, в научной литературе взаимосвязь IOs и суверенитета остаются малоизученными и составляют предмет научных споров. В связи с этим, автор подчеркивает, что, согласно доктрине международного права, любое несанкционированное вмешательство во внутренние и внешние дела другого государства запрещено. Этот запрет предусмотрен Декларацией ООН о принципах между-

народного права, касающихся дружественных отношений и сотрудничества между государствами в соответствии с Уставом ООН (Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States) принятой резолюцией 2625 (XXV) Генеральной Ассамблеи ООН 24 октября 1970 г.[1] В Декларации указывается, что ни одно государство не может использовать экономические, политические и иные меры с целью принуждения другого государства к подчинению или незаконного получения преимущества. Здесь автор успешно обращает внимание на то, что термин «принуждение» в международном праве имеет различные значения, но в контексте запрета на вмешательство он может быть интерпретирован как лишение государства свободы выбора (p. 7–8).

Заслуживает внимание судебный прецедент, приведенный С. Уайтом в качестве обоснования своей позиции. Дело Никарагуа против США (Nicaragua vs United States of America) демонстрирует, что вмешательство США во внутренние дела государств через поддержку повстанцев является прямым нарушением принципа невмешательства в дела, касающиеся государственного суверенитета. Исходя из обстоятельств рассматриваемого судебного дела, автор приходит к выводу, что вмешательство внешних акторов во внутренние дела другого государства становится противоправным лишь в тех случаях, когда удается доказать применение методов принуждения (политического, экономического, социального, культурного и др.), что может включать применение силы, военные действия или поддержку деятельности, посягающей на общественный порядок и безопасность (p. 8–10).

В главе 5 о защите персональных данных как способа обеспечения устойчивости к дезинформации «Data Protection Regulation as Disinformation Resilience» С. Уайт совместно с ассистентом Дж. Смолл представляют уникальный взгляд на происхождение и развитие несанкционированных онлайн-кампаний по на дезинформированию общества в цифровой среде. Особое внимание уделяется рассмотрению маркетинговых и рекламных тактик и стратегий, направленных на распространение заведомо ложных сведений через различные СМИ. Институт защиты персональных данных в цифровом формате преследует две основные задачи:

[1] Declaration on Principles of International Law Concerning Friendly Relations and Co-operation among States: сайт. – URL: https://www.un.org/ru/documents/decl_conv/declarations/intlaw_principles.shtml (дата обращения: 20.11.25).

1) он гарантирует сохранность персональной информации; 2) выступает в качестве ограничителя доступа к персональным данным, которые часто становятся объектом посягательства и дезинформации в Интернете. В качестве эффективного регулятора в отношении данной проблемы авторами приводится принятый Европейским Советом Общий регламент о защите данных (GDPR)[1], так как данный нормативный акт продемонстрировал практическую значимость, ограничивая масштабы и интенсивность дезинформации и устанавливая четкие правила при сборе, обработке, хранении и распространении персональных данных на территории стран – членов ЕС. Интересным в работе следует признать предпринятый авторами детальный анализ основных характеристик GDPR и других законодательных актов Австралии, регулирующих защиту персональных данных, позволяющий С. Уайту сделать справедливый вывод о том, что меры по защите персональных данных пользователей являются ключевым механизмом сокращения рисков, связанных с распространением дезинформации (p. 51–57).

В центре внимания С. Уайта и Дж. Смолла находятся также проблемы регулирования Интернета на макроуровне. В то время как одни государства контролируют интернет-контент, другие атакуют соцсети запросами на предоставление личной информации пользователей. СМИ, будучи в большей своей массе частными компаниями, соглашаются на «секретное» сотрудничество с государствами, запрашивающими услуги о предоставлении личной информации о пользователях или об ограничении доступа к определенному контенту, что создает этическую дилемму в регулировании потока данных. Саморегулирование цифровых платформ и СМИ, хотя и номинально, является предпочтительным подходом со стороны многих государств: такая позиция позволяет обеспечить быстрое реагирование и адаптацию к внешним вызовам, внедрение инноваций, но влечет критику из-за непрозрачности операций по обмену данными. Авторами приводится известный пример с компанией Facebook, которая по собственному решению заблокировала доступ австралийским гражданам к новостным ресурсам из-за вступления в 2021 г. «Кодекса ведения переговоров со СМИ» (News Media and Digital Platforms Mandatory Bargain

[1] The Regulation on the Protection of Natural Persons with Regard to the Processing of Personal Data: сайт. – URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng (дата обращения: 15.08.25).

Code, NMBC)[1], согласно которому крупные технологические платформы обязаны были платить медиа за используемый ими контент. Это правило коснулось и копаний, входящих в экосистему Meta (признана Тверским районным судом г. Москвы по иску Генпрокуратуры России, поддержанному Роскомнадзором и ФСБ экстремистской) и Google, которые в борьбе с дезинформацией заблокировали более 200 операций и каналов с недобросовестным контентом. Таким образом, авторы пришли к выводу о том, что совместное регулирование доступа к цифровому контенту и контролю над дезинформацией, сочетающее гибкость саморегулирования со стороны частных цифровых платформ и внешний контроль со стороны государства, является оптимальным, но не лучшим решением в регулировании данного вопроса на текущий момент (р. 71–79).

В главе 8, под названием «Сила народа – устойчивость рабочей силы» («People Power – A Resilience Working Power») С. Уайт в соавторстве с С. Гиатракосом из Университета Аделаиды исследуют уникальный подход к изучению роли служб разведки и онлайн-консультационных подразделений в вопросе повышения устойчивости и противодействии киберугрозам. На основе зарубежной и отечественной (австралийской) литературы авторы исследуют стратегии и тактики, применяемые такими организациями в борьбе с дезинформацией и кибератаками, а также предлагают читателям особый взгляд на кибербезопасность с позиции военных. Поскольку Интернет стал неотъемлемо частью повседневной жизни, они отмечают возросшее в последние годы злоупотребление Интернетом как ключевым цифровым ресурсом. Заслуживает внимание позиция С. Уайта и С. Гиатракоса о том, что операции по иностранному вмешательству (IOs) используют глобальную доступность Интернета для доставки персонализированных сообщений с содержанием незаконного характера конкретным пользователям через различные мессенджеры. Они подчеркивают, что эти методы хоть и просты по форме, но представляют не менее серьезную угрозу. В данном отношении речь идет не о физическом ущербе, а о возможности незаметного подключения к отдельным людям в любое время суток. Эта концепция, как отмечают исследователи, была наиболее точно сформулирована Валерием Гера-

[1] News Media and Digital Platforms Mandatory Bargain Code: сайт. – URL: https://treasury.gov.au/sites/default/files/2022-11/p2022-343549.pdf (дата обращения: 15.11.25).

симовым, начальником российского Генерального штаба в 2013 г., отметившим изменение правил и методов ведения войны в современных реалиях и возросшую роль невоенных средств достижения политико-экономических целей (p. 105–106).

В главе 9 «Повышение социальной устойчивости» («Building Social Resilience») Сэмюэл Уайт и Мэтью Стаббс описывают различные подходы к поддержанию социальной киберустойчивости. По мнению авторов, инвестиции в образовательные инициативы и программы самопомощи повышают социальную киберустойчивость. Значительное место в работе посвящено вопросам угрозы от государственных информационных кампаний и кибератак, анализу моделей и стратегий укрепления защищенности цифровых технологий без применения «мягких» правовых механизмов («soft» options). Помимо образования и просветительской деятельности ключевыми инструментами повышения социальной устойчивости авторами признаются повышение авторитета государственных учреждений и укрепление социальной сплоченности (p. 117–123).

Последняя составляющая концепции устойчивости раскрывается в главе, посвященной изучению корпоративных правовых мер по повышению устойчивости («Corporate Legal Responses to Promote Resilience»). С. Уайт и Элизабет Уэтфорд из Университета Аделаиды, анализируют механизмы корпоративного управления, направленные на повышение устойчивости к цифровым угрозам в Австралии. Взаимосвязь между законодательством о кибербезопасности, корпоративными обязанностями и ответственностью директоров компаний достаточно сложная. Это обусловлено наличием нескольких регулирующих органов, которые уполномочены инициировать судебные процессы. Первым регулятивным органом в стране выступает Австралийская комиссия по ценным бумагам (Australian Securities and Investments Commission, ASIC), отвечающая за регулирование финансовой деятельности компаний и защиту потребителей, инвесторов и кредиторов, вторым Управление австралийского информационного комиссара (Office of the Australian Information Commissioner, OAIC), занимающееся вопросами конфиденциальности, свободы информации и государственной информационной политики. Основная сложность заключается в том, что деятельность данных учреждений регулируется разными нормативными правовыми актами, например Австралийская комиссия по ценным бумагам может действовать в соответствии с Законом о корпорациях, а Управление австралийского информационного комиссара – в рамках Закона Австралии о конфиденци-

альности 1988 г. Ситуацию осложняет недостаточная осведомленность граждан о ценности своих данных, тогда как компании, обладающие ресурсами и доступом к большим массивам данных должны были бы самостоятельно обеспечивать такую защиту. Именно поэтому требуется усиление корпоративных и управленческих компетенций и обязательств в сфере кибербезопасности. Однако, как замечают авторы, отсутствие исков против руководящего состава компании, пострадавших от кибератак, несмотря на их фидуциарную обязанность по сокращению таких рисков, является фактом. С учетом повышения роли бизнеса в поддержании киберустойчивости и эффективной реализации Стратегии кибербезопасности Австралии до 2030 г., усиление корпоративного регулирования, как подчеркивают С. Уайт и Э. Уэтфорд, неизбежно (p. 170–171).

Монография, представленная учеными Аделаидского университета и основанная на материалах конференции по киберустойчивости, представляет комплексный анализ современных цифровых угроз и правовых механизмов их регулирования. Принципиально важным следует признать предложение авторов книги о необходимости перехода от абсолютной защиты киберпространства к модели устойчивости, позволяющей нейтрализовать иностранное вмешательство в цифровое пространство страны, защитить цифровой суверенитет и выстроить слаженное государственное и частное регулирование.