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

Б. Головкин, А. Таволжанский, А. Лысодед
Connections QJ 20, № 2 (2021): 75-87
https://doi.org/10.11610/Connections.rus.20.2.07

Рецензированная статья

Коррупция как угроза кибербезопасности при новом мировом порядке

Богдан Головкин, Алексей Таволжанский, Александр Лысодед

Кафедра криминологии и уголовно-исполнительного права, Национальный юридический университет имени Ярослава Мудрого, https://nlu.edu.ua/

Аннотация: Важная тема кибербезопасности применительно к борьбе с коррупцией в контексте глобальных проблем пандемийного и пост-пандемийного мира требует дальнейших исследований. Цель этой статьи – показать и проанализировать нынешние и будущие проблемы кибербезопасности в данном контексте, применяя общенаучные и специализированные юридические методы познания. Использование диалектического метода, теоретических основ и современных взглядов на обеспечение кибербезопасности позволило изучить главные проблемы сегодняшнего дня. Формально-правовые и сравнительные методы дают возможность рекомендовать меры усиления кибербезопасности с учётом массовой информатизации и общественных трансформаций. Авторы подчёркивают необходимость разработки национальной политики кибербезопасности на основе информационной грамотности и культуры населения, сочетая уважение к традиционным историческим ценностям с современным пониманием мультикультурных обменов и благополучия.

Ключевые слова: кибербезопасность, коррупция, борьба с коррупцией, угрозы кибербезопасности, пандемия COVID-19, пост-пандемийные условия.

Вступление

Обеспечение безопасности исторически зависело от мощи государства, его экономического и военного потенциала. Сегодня государство должно добавить к перечню своих обязательств ещё один пункт: защиту цифровых элементов государственной и общественной деятельности.[1] Обеспечение кибербезопасности – одна из обязательных функций современных стран по поддержанию и совершенствованию системы комплексной защиты общества государством. В условиях массовой коррупции фокус смещается с защиты прав и свобод на некую денежную прибыль или иные выгоды.[2] Поэтому при коррупции едва ли возможно обеспечить какую-либо безопасность. С одной стороны, коррупция концептуально определена и рассматривается как угроза для любой страны. С другой, в процессе глобализации, информатизации, быстрого развития технологий и инноваций, а также пандемии коррупция остаётся характерной чертой современных государств, общественного диалога и коммуникации.[3] Состояние кибербезопасности той или иной страны зависит от этого явления, негативного по своей природе и деструктивного для стабильного функционирования государственной власти, от которой ожидают адекватного выполнения своих функций и завоевания доверия людей.[4]

Традиционные инструменты, имеющиеся у правоохранительных органов, уже не могут эффективно побороть коррупцию. В последнее время интерес сместился к новому организационному подходу к борьбе с коррупцией, при снижении роли карательно-репрессивных механизмов.[5]

Каждая правовая система имеет свои цели, задачи и создаёт механизмы их достижения.[6] Снижение коррупции считается одним из главных шагов на пути к устойчивому развитию и инклюзивному обществу путём создания

---

1 Mykola O. Ovcharenko et al., "Combating Illegal Drugs Trafficking Using the Internet by Means of the Profiling Method," *Journal of Advanced Research in Law and Economics* 11, no. 4 (2020): 1296-1304, https://doi.org/10.14505//jarle.v11.4(50).26.

2 Victoria V. Tsypko et al., "Information Policy of the Enterprise as the Basis for the Reproduction of Human Potential in the Structure of Public Social Interaction," *Journal of Advanced Research in Law and Economics* 10, no. 6 (2019): 1664-1672.

3 Viacheslav V. Vapniarchuk et al., "Protection of Ownership Right in the Court: The Essence and Particularities," *Asia Life Science* 21, no. 2 (2019): 863-879, http://dspace.nlu.edu.ua/handle/123456789/18141.

4 Yu. Tavolzhanska et al., "Severe Pain and Suffering as Effects of Torture: Detection in Medical and Legal Practice," *Georgian Medical News* 10 (307) (October 2020): 185-193, http://ir.librarynmu.com/bitstream/123456789/2160/1/GMN_62-68.pdf.

5 Sergey Vorontsov et al., "The Use of Artificial Intelligence to Combat Corruption," *Media Education* (Mediaobrazovanie) 60, no. 4 (2020): 757-763, https://doi.org/10.13187/me.2020.4.757.

6 Dimitra Markopouloua, Vagelis Papakonstantinoua, and Paul de Hert, "The New EU Cybersecurity Framework: The NIS Directive, ENISA's Role and the General Data Protection Regulation," *Computer Law and Security Review* 35, no. 6 (November 2019): 1-11, https://doi.org/10.1016/j.clsr.2019.06.007.

действенных, подотчётных и инклюзивных институтов на всех уровнях.[7] На практике для глобальной борьбы с коррупцией нужны не новые правила, а скорее их лучшее исполнение. Правозащитный подход может помочь закрыть этот пробел в исполнении. Полное осознание того, что коррупция подрывает реализацию прав человека, позволит авторитетным мировым правозащитным организациям вплотную заняться коррупцией, не выходя за пределы своего мандата. Способствуя изменению взглядов и открывая новые возможности для мониторинга и судопроизводства, правозащитный подход может удачно дополнить уголовно-правовой подход к коррупции и тем самым помочь достижению целей развития Повестки 2030 г.[8]

Поэтому цель этой статьи – описать текущие проблемы и перспективы обеспечения кибербезопасности в пандемийном и пост-пандемийном мире в условиях борьбы с коррупцией. Для этого необходимо:

1) рассмотреть теоретико-правовые основы коррупции, как угрозы кибербезопасности;
2) проанализировать нынешнее состояние, проблемы и задачи кибербезопасности в современных условиях борьбы с коррупцией;
3) изучить особенности и спрогнозировать перспективы обеспечения кибербезопасности при борьбе с коррупцией в пандемийных и пост-пандемийных реалиях,

принимая во внимания правоотношения и деятельность в сфере кибербезопасности и борьбы с коррупцией.[9]

Для этого применялись общенаучные и специализированные юридические методы познания. Тема была исследована и современные вызовы обозначены с помощью диалектического метода, теоретического обоснования и анализа текущих проблем. Формально-догматический метод помог авторам объяснить коррупцию как угрозу кибербезопасности. Формально-правовые и сравнительные методы позволили выработать рекомендации по усилению кибербезопасности.

---

[7] Giulia Mugellini and Jean-Patrick Villeneuve, “Monitoring the Risk of Corruption at International Level: The Case of the United Nations Sustainable Development Goals,” *European Journal of Risk Regulation* 10 (March 2019): 201-207, https://doi.org/10.1017/err.2019.16.

[8] Anne Peters, “Corruption as a Violation of International Human Rights,” *European Journal of International Law* 29, no. 4 (November 2018): 1251-1287, https://doi.org/10.1093/ejil/chy070.

[9] O.E. Kostyuchenko et al., “Robotization of Manufacturing Process: Economic and Social Problems and Legal Ways of Their Solution,” *Financial and Credit Activity: Problems of Theory and Practice* 3, no. 30 (2019): 454-462, https://doi.org/10.18371/fcaptp.v3i30.179847.

Правовые основы коррупции как угрозы кибербезопасности

Обеспечение кибербезопасности нужно изучать с учётом коррупции как угрозы при глобализации и росте информатизации. Для повышения эффективности и функциональности кибербезопасности при борьбе с коррупцией в условиях пандемийного и пост-пандемийного мирового порядка, Чернявский с соавторами дают ряд рекомендаций.[10]

Кибербезопасность как область безопасности государства опирается на те же требования, которые передовые страны используют при функционировании и развитии систем безопасности. В то же время кибербезопасность существует и развивается в определённой среде, поскольку кибератаки направлены на цифровой потенциал государства. Последствия кибератак опасны для устройств, сетей, систем, данных и программного обеспечения и могут разрушать государство не только виртуально, но и физически. Среди множества киберугроз коррупция – одна из главных. Она может ослабить систему защиты страны и даже разрушить её. Правовое регулирование процессов, уязвимых для коррупции, всегда было достаточно важным делом. Во время пандемии выросла компьютеризация разных услуг, процессов и видов деятельности, а обеспечение кибербезопасности, как и раньше, включает постоянную борьбу с коррупцией. Отсюда возникает необходимость научного анализа угроз кибербезопасности. В частности, для борьбы с явлением коррупции государства в лице своих судебных органов решают следующие задачи:

1) создание правовой системы, нацеленной на противостояние давлению коррупционных преступлений;
2) усиление возможностей борьбы с коррупцией и сопутствующими преступлениями, что снижает распространённость коррупции;
3) создание профессионального специализированного органа для всех сфер деятельности, особенно публичной;
4) эффективное обеспечение правосудия согласно принципам уважения к закону и человеческому достоинству;
5) внедрение действенных судебных механизмов по уголовным делам для выполнения функций уголовного судопроизводства.[11]

Стоит подчеркнуть, что общепринятого определения коррупции нет. Есть тенденция к широкому, всеохватывающему использованию термина

[10] Serhii S. Cherniavskyi et al., “International Cooperation in the Field of Fighting Crime: Directions, Levels and Forms of Realization,” *Journal of Legal, Ethical and Regulatory Issues* 22, no. 3 (2019): 1-11, https://www.abacademies.org/articles/international-cooperation-in-the-field-of-fighting-crime-directions-levels-and-forms-of-realization-8346.html.

[11] Delia Magherescu, “Criminal Investigation of the Corruption Crimes: Evidence and Procedure in an Interdisciplinary Approach,” *Revista Brasileira de Direito Processual Penal* 6, no. 3 (2020): 1239-1270, https://doi.org/10.22197/rbdpp.v6i3.394.

«коррупция». Также имеются серьёзные расхождения в том, какие именно деяния являются коррупцией. Наверное, самое употребимое сейчас определение принято неправительственной организацией Transparency International: «коррупция – это злоупотребление вверенными полномочиями для личной выгоды».[12] Популярное определение коррупции с учётом государственной службы, как «злоупотребление государственной должностью для личной выгоды», конечно, тоже верно.[13]

Роль и значение коррупции, как угрозы кибербезопасности

Теоретическое определение коррупции как угрозы кибербезопасности основано на её общем понимании международным сообществом. Её специфика проявляется в связи с конкретной средой реализации этого негативного явления, то есть киберпространством, использование которого должно быть максимально безопасным. Безопасность – важная общемировая проблема, проявляющаяся в таких задачах, как защита киберинфраструктуры от нападений преступников и других государств; защита своих портов, аэропортов, общественного транспорта и другой критической инфраструктуры страны от террористов; защита своей фауны и лесов от браконьеров и контрабандистов; и пресечение нелегального потока оружия, наркотиков и денег через международные границы.[14]

Международным мерам борьбы с коррупцией не хватает точности в определениях. Поскольку представления о коррупции в разных странах различны, большинство международных исследований жертвуют широтой ради глубины. Примеры тут всегда важны, потому что они позволяют глубже и чётче понять, как и почему коррупция работает.[15] Коррупция – распространённое явление, всё более нормативное поведение, которое можно ограничить, реализуя различные планы усиления, наказаний, открытости, подотчётности, информирования, моделирования и психологические стратегии понимания и борьбы с коррупцией.[16] Коррупцию как угрозу кибербезопасности можно понимать как потенциально деструктивное явление с видимыми и невидимыми ретроспективными последствиями в виде уязвимостей безопасности в киберпространстве, что исключает гарантию

---

[12] Julio Bacio-Terracino, “Corruption as a Violation of Human Rights” (International Council on Human Rights Policy, January 2008), 1-36, https://ssrn.com/abstract=1107918.

[13] Mark J. Farrales, “What is Corruption?: A History of Corruption Studies and the Great Definitions Debate” (June 2005), https://ssrn.com/abstract=1739962.

[14] Arunesh Sinha et al., “From Physical Security to Cybersecurity,” *Journal of Cybersecurity* 1, no. 1 (September 2015): 19-35, https://doi.org/10.1093/cybsec/tyv007.

[15] Farrales, “What is Corruption?”

[16] Divyanshi Chugh, “Psychology of Corruption,” *The Learning Curve*, July 25, 2012, Lady Shri Ram College for Women Finalist, Young Psychologist 2012, National Paper Presentation Competition, Christ University, Bangalore, India, 1-11, https://ssrn.com/abstract=2117247.

недопущения кибератак и действенное снижение их негативных последствий.

Классические государства в разные исторические периоды боролись с разными угрозами для сохранения своего суверенитета, территориальной целостности и обеспечения социально-экономической стабильности и процветания. Из-за высокого уровня информатизации и быстрого развития технологий большинство современных государств сталкиваются с новыми видами угроз кибернетического характера. Поэтому современные страны должны проводить эффективную государственную политику сохранения информационного суверенитета, стабильности и дальнейшего существования в изменённой цифровой реальности. Явление коррупции опасно и для виртуальной реальности. Развитие информационного государства, а не только его экономического и технологического компонентов, сегодня зависит от решений государственной власти. Если власти страны учитывают коррупцию при принятии решений, этот факт позволяет нам видеть в коррупции угрозу кибербезопасности. Её роль весьма важна, в связи с продолжением в мире информатизации и общим переходом с традиционных на цифровые технологии. Чем сильнее коррупция, тем уязвимее системы кибербезопасности в отдельных странах и во всём мире.

Интернет играет важную роль в повседневной жизни. Повсеместность киберсистем влечёт далеко идущие последствия кибератак. Кибератаки угрожают физической, экономической, общественной и политической безопасности. Они могут нарушить, помешать и даже парализовать работу критической инфраструктуры, включая электросети, связь, больницы, финансовые учреждения, оборонные и военные системы.[17] В частности, коррупция может существенно нарушить даже такую форму демократии, как выборы. Выборы входят в новую цифровую эпоху, с новыми возможностями и угрозами для проведения и оспаривания выборов. Хотя многие из них не совсем новы и могут быть продолжением старых проблем, произошёл качественный скачок в характере вызовов.[18]

Некоторые контрмеры могут повредить обществу, мешая доступу к информации и ограничивая открытость и подотчётность. Политическая шумиха вокруг дезинформации, возможно, слишком раздула проблему в глазах общественности. Регуляторы должны избегать зарегулированности, поскольку политические дебаты важны для информирования электората и

[17] Jonathan Z Bakdash et al., "Malware in the Future? Forecasting of Analyst Detection of Cyber Events," *Journal of Cybersecurity* 4, no. 1 (2018): tyy007, https://doi.org/10.1093/cybsec/tyy007.

[18] Holly Ann Garnett and Toby S. James, "Cyber Elections in the Digital Age: Threats and Opportunities of Technology for Electoral Integrity," *Election Law Journal: Rules, Politics, and Policy* 19, no. 2 (2020): 111-126, https://doi.org/10.1089/elj.2020.0633.

поддержки демократических принципов.[19] Новая концепция, не ограниченная государственным сектором и правовыми рамками, рассматривает коррупцию как сделку между людьми для обмена услугами в течение какого-то времени. В наиболее характерном примере услугами обмениваются два участника, один из частного, другой – из государственного сектора, при чём представитель государственного сектора использует свой доступ к государственному финансированию.[20]

По нашему мнению, деструктивную роль коррупции как угрозы кибербезопасности можно понять лишь тогда, когда проявится её негативное воздействие на государство. Это воздействие может сделать очевидной уязвимость кибербезопасности государства и критическую угрозу не только безопасности людей, но самому существованию страны. Невосприятие и непонимание коррупции как потенциального поэтапного разрушения всего государства – ошибочный подход и одна из главных черт кибервойны.

Текущие проблемы и перспективы кибербезопасности в рамках борьбы с коррупцией

Во время пандемии кибербезопасность и управление ею приобрели особую важность. В то же время коррупция – традиционное явление, отражающее новые отношения с появлением кибер-черт, по ряду причин. Проблемы национального управления и коррупции традиционно считаются:

- особенно острыми в бедных странах, а более благополучный мир рассматривается как образец или эталон,
- связанными с правовой системой и качеством официальных институтов;
- проблемой государственного сектора; и
- изолированными от глобальных проблем управления и безопасности; они рассматриваются, как отдельная сфера.[21]

Управление и коррупция остаются противоречивыми и малопонятными темами, но теперь они приобрели более высокий приоритет для органов развития и корпораций, включая транснациональные.[22] План борьбы с ор-

[19] Elizabeth F. Judge and Amir M. Korhani, “Disinformation, Digital Information Equality, and Electoral Integrity,” *Election Law Journal: Rules, Politics, and Policy* 19, no. 2 (2020): 240-261, https://doi.org/10.1089/elj.2019.0566.

[20] Daniel Kaufmann and Pedro C. Vicente, “Legal Corruption,” November 24, 2005, https://ssrn.com/abstract=829844.

[21] Daniel Kaufmann, “Corruption, Governance and Security: Challenges for the Rich Countries and the World,” *SSRN Electronic Journal* (October 2004), https://doi.org/10.2139/ssrn.605801.

[22] Daniel Kaufmann, “Myths and Realities of Governance and Corruption,” *SSRN Electronic Journal* (November 2005), https://doi.org/10.2139/ssrn.829244.

ганизованной коррупцией – это в значительной мере формирование правил и процедур, определяющих, что следует считать коррупцией, а не просто недопущение поведения, которое уже считается коррупционным.[23] Но «взлом» демократий, о котором так много говорят ученые и практики в последние годы, имеет довольно мало общего с прямым использованием киберинструментов для подрыва, ослабления или шпионажа. Вместо этого угроза демократическим политическим системам возникает из-за несоответствия новых систем, лежащих в основе дискурса, и тех правил и норм поведения, которые должны быть приняты в ближайшие годы для обеспечения неподкупности национальной политики.[24]

По нашему мнению, явление коррупции предопределяется внутренним развитием общества, движущегося к реализации своего демократического выбора. Коррупция – всегда угроза, которую невозможно контролировать или уменьшить, если общество принимает её как форму коммуникации. Главная проблема коррупции для кибербезопасности кроется во внутренних потребностях и интересах обществ, становящихся всё более «оцифрованными». Если они пойдут по демократическому пути развития, они должны убрать коррупцию из своей реальности.

Концентрация усилий на сдерживании пандемии отвлекла внимание от постоянной необходимости бороться с коррупцией. Но это явление усиливается в условиях пандемии, в первую очередь из-за ослабления общественного контроля в результате социального дистанцирования. Сейчас традиционные вызовы для безопасности государства распространяются в киберпространстве в связи с расширением использования киберпространства и связанных с ним технических возможностей. Мы замечаем типичные взаимосвязанные ситуации в области безопасности:

- любой посетитель информационных и социальных сетей – международных, государственных, гражданских – может стать жертвой кибератак;
- кибератаки могут иметь серьёзные последствия для национальной безопасности, экономики и угрожать повседневной жизни общества;
- необходима защита от угроз на международном, национальном и индивидуальном уровне.[25]

[23] Dennis F. Thompson, “Two Concepts of Corruption,” Edmond J. Safra Working Papers, No. 16 (August 2013): 1-24, https://ssrn.com/abstract=2304419.

[24] Christopher Whyte, “Cyber Conflict or Democracy ‘Hacked’? How Cyber Operations Enhance Information Warfare,” *Journal of Cybersecurity* 6, no. 1 (2020): tyaa013, https://doi.org/10.1093/cybsec/tyaa013.

[25] Zsolt Szabó, “The Effects of Globalization and Cyber Security on Smart Cities,” *Interdisciplinary Description of Complex Systems* 17, no. 3-A (2019): 503-510, https://doi.org/10.7906/indecs.17.3.10.

В реальности сложность специализированного программного обеспечения может сделать результаты атаки непредсказуемыми, скрывая происходящее при вмешательстве или нарушении работы программных систем. Во-вторых, поскольку большинство компьютерных систем подключены к другим компьютерным системам через Интернет, некоторые атаки могут вестись разными системами. Из-за сложности каждой системы и её связей трудно спрогнозировать масштаб и скорость распространения и воздействия. В-третьих, сбой компьютеров может дать физические эффекты, которые выйдут за пределы киберпространства и сами по себе труднопредсказуемы.[26]

Применение искусственного интеллекта (ИИ) для обеспечения кибербезопасности тоже может быть объектом коррупционных манипуляций, поэтому борьба с этим явлением важна и здесь. Сейчас ИИ – не чудо и не интеллект в «человеческом» смысле этого слова, но сегодняшняя технология ИИ может давать «умный» результат и без интеллекта, используя шаблоны, правила и эвристические алгоритмы, позволяющие ему принимать ценные решения в конкретном, узком контексте. Однако нынешняя технология ИИ имеет свои ограничения. Он особенно слаб в абстракциях, понимании значений, переносе знаний из одного вида деятельности в другой и решении задач без инструкций или с неопределённым результатом.[27] В результате коррупция может негативно влиять даже на инвестиции в безопасность. Так, чиновник, скептичный к инвестициям в безопасность, может считать, что раз фирму взламывают каждый год, ежегодные инвестиции в защиту её ИТ – пустая трата денег, если взлома не произошло. Или же это может означать, что фирма может ожидать потери эквивалента своих затрат на информационную безопасность после каждой утечки данных или нарушения безопасности.[28]

Потери от киберпреступности включают порчу и уничтожение данных, судебную экспертизу, восстановление и удаление взломанных данных и систем, мошенничество, нарушение нормальной деятельности после атак, хищение денег, падение производительности, кражу личных и финансовых

[26] Henry Farrell and Charles L. Glaser, “The Role of Effects, Saliencies and Norms in US Cyberwar Doctrine,” *Journal of Cybersecurity* 3, no. 1 (March 2017): 7-17, https://doi.org/10.1093/cybsec/tyw015.

[27] Harry Surden, “Artificial Intelligence and Law: An Overview,” Georgia State University Law Review 35, no. 4 (2019), https://readingroom.law.gsu.edu/gsulr/vol35/iss4/8.

[28] Sasha Romanosky, “Examining the Costs and Causes of Cyber Incidents,” *Journal of Cybersecurity* 2, no. 2 (December 2016), 121-135, https://doi.org/10.1093/cybsec/tyw001.

данных, растрату, потерю репутации и кражу интеллектуальной собственности.[29] Но главная сложность в поддержании бинарного соотношения «законный/злонамеренный» — а следовательно, в создании стабильного фундамента самой кибербезопасности — заключается не в технологическом, социальном и экономическом давлении, открыто признанном экспертами по кибербезопасности, а в скрытом продвижении «кибер-нуара».[30] Поэтому с одной стороны, нынешняя реальность – использование технологий в цифровом мире, а с другой, коррупция в этой сфере – вечная проблема, способная разрушить государство. А значит, мировое сообщество должно бороться с этим негативным явлением не только в физическом мире, но и в невидимой киберреальности.

Перспективы обеспечения кибербезопасности при угрозе коррупции

Перспективы обеспечения кибербезопасности при системной борьбе с коррупцией сегодня зависят от экономических показателей страны. Экономический фактор в первую очередь влияет на развитие всех сфер безопасности, включая кибернетическую. Коррупционная среда, не учитывающая интересов общества и государства, не может гарантировать ни кибер-, ни иную безопасность. Коррупция остаётся угрозой развитию технологий и инновациям. Надо понять, что она потенциально и реально угрожает не только кибербезопасности, но и безопасности государства.

Современный подход к кибербезопасности должен основываться на понимании того, что коррупция должна находиться под постоянным контролем. Когда речь идёт о коррупции, гражданское общество должно контролировать свою страну всеми возможными путями, чтобы устранить потенциальную угрозу для развития и процветания государства. С другой стороны, коррупция всегда будет побуждать граждан к активному участию в управлении государством. С этой точки зрения доходы от коррупции, даже небольшие, мотивируют граждан участвовать в борьбе с коррупцией. Тем самым граждане помогают общей цели развития и благополучия.

Сегодня подход к обеспечению кибербезопасности должен быть рациональным и практичным. Он должен включать два компонента: образованные, идеологически подготовленные органы управления, с одной стороны, и таких же членов общества, с другой. Контроль кибербезопасности и прогнозирование угроз прямо зависит от технических возможностей. Кибербезопасность при борьбе с коррупцией должна обеспечиваться защитой

[29] Tabrez Ahmad, “Corona Virus (COVID-19) Pandemic and Work from Home: Challenges of Cybercrimes and Cybersecurity” (April 5, 2020), http://dx.doi.org/10.2139/ssrn.3568830.

[30] James Shires, “Cyber-noir: Cybersecurity and Popular Culture,” *Contemporary Security Policy* 41, no. 1 (2019): 82-107, https://doi.org/10.1080/13523260.2019.1670006.

данных, устройств, сетей и программного обеспечения. Доступ коррумпированных структур к их работе должен быть ограничен.

Предотвращение кибератак и устранение их негативных последствий для критических объектов инфраструктуры должно пребывать под постоянным контролем не только государства, но и общественных организаций и граждан, поскольку коррупция в этой сфере может заблокировать доступ к финансовым и медицинским учреждениям и электростанциям в случае стихийного бедствия или военного конфликта. Передовые системы кибербезопасности основаны на взаимодействии людей, технологий и процессов предупреждения и защиты от кибератак. Создание и системная поддержка национальной стратегии кибербезопасности должны дополняться постоянным обучением населения знанию и соблюдению принципов кибербезопасности и взглядом на коррупцию как на атрибут не только экономически слабых, но и идеологически дезорганизованных обществ.

С коррупцией борются на нескольких фронтах. При безусловной важности законов и правоохранительной деятельности, страны, серьёзно борющиеся с коррупцией, должны также обращать внимание на реформирование роли правительства в экономике, особенно в тех сферах, где чиновники имеют широкие полномочия. Наём и повышение гражданских служащих за их заслуги и выплата им зарплат, сравнимых с частным сектором, помогают привлечь квалифицированных и честных гражданских служащих. Международное давление на коррумпированные страны, включая уголовное преследование за взятки международных компаний иностранным чиновникам – тоже действенная мера. Но успех любой антикоррупционной кампании в конечном счёте зависит от реформирования внутренних институтов коррумпированных стран.[31] Изучение тенденций, факторов и последствий для кибербезопасности в Канаде[32] позволяет предложить следующие рекомендации.

1) Разработать и внедрить процедуры и инструменты постоянного мониторинга для отслеживания развития цифровой экосистемы и изучения разных участников и их взаимодействия, а также оценки влияния этих изменений на кибербезопасность;
2) Согласовать режимы регулирования, применимые к инфраструктуре, приложениям и контенту, с ресурсами и стратегиями, реализуемыми всё большим числом государственных субъектов и их частных партнеров, для быстрого обнаружения возникающих цифровых рисков и ограничения их влияния на постоянно развивающуюся экосистему;

[31] Shang-Jin Wei, “Corruption in Economic Development: Beneficial Grease, Minor Annoyance, or Major Obstacle?” (February 1999), https://ssrn.com/abstract=604923.

[32] Benoit Dupont, “The Cyber Security Environment to 2022: Trends, Drivers and Implications” (2012), https://ssrn.com/abstract=2208548.

3) Начать углубленные консультации и обсуждение для выработки предложений о том, как реорганизовать существующие или создать новые государственные институты, чтобы адаптировать действия и координационные усилия правительства Канады к новым потребностям;
4) Активизировать эмпирические исследования изменения рисков, стандартов и практик, связанных с защитой конфиденциальности в цифровой сфере;
5) Усилить координацию и инициативы обмена информацией национальных и региональных властей для ускорения и стандартизации развития возможностей на местах.[33]

Таким образом, при необходимости борьбы с коррупцией, поступательную и эффективную реализацию политики кибербезопасности может поддерживать и совершенствовать общество с должным уровнем информационной грамотности и культуры при глубоком уважении к традиционным и историческим ценностям своего народа в рамках идеологии национального развития и благополучия. Только глубокое уважение к своей стране, ее наследию, ценностям и культуре, а также современное понимание межкультурных обменов для дальнейшего личного и национального развития и благополучия могут создать надёжную платформу для кибербезопасности.

Обеспечение кибербезопасности – сложная задача. То же можно сказать и о создании кибернорм. Желаемые результаты остаются эфемерными, пока не появятся нормы (среди прочих инструментов), формулирующие социальные ожидания поведения для их достижения. Возникновение этих конструкций может быть сложным, но ни киберпространство, ни его нормы не настолько непроницаемы, чтобы участники могли игнорировать различные ситуации, элементы и инструменты этого процесса. Наоборот, понимание реальных процессов формирования, распространения и развития кибернорм может повлиять на будущий образ кибербезопасности.[34]

Выводы, рекомендации и ограничения

Очевидно, что существующая система кибербезопасности рассматривает коррупцию как угрозу. Современное концептуальное понимание кибербезопасности при борьбе с коррупцией во время и после пандемии опирается на ряд технических, экономических, политических и даже психологических инструментов и средств защиты данных, устройств, сетей и программного обеспечения, снижения угрожающего им риска коррупции и обеспечения безопасных условий для конструктивной деятельности.

[33] Dupont, “The Cyber Security Environment to 2022.”

[34] Martha Finnemore and Duncan B. Hollis, “Constructing Norms for Global Cybersecurity,” *American Journal of International Law* 110, no. 3 (2016): 425-479, https://doi.org/10.1017/S0002930000016894.

Этот процесс включает два обязательных компонента: образованные, идеологически подготовленные органы управления, с одной стороны, и такие же члены общества, с другой. Техническая сторона кибербезопасности зависит от экономического развития государства и определяет соответствующие модели. В то же время, учитывая необходимость борьбы с коррупцией во время и после пандемии, только общества с надлежащим уровнем информационной грамотности, культуры и глубоким уважением к традиционным ценностям и современному развитию могут поддержать и усовершенствовать поступательную действенную реализацию политики национальной кибербезопасности.

Материалы этой статьи могут быть полезны для исследователей, желающих модернизировать существующую систему кибербезопасности для реагирования на новые угрозы. Однако в процессе исследований возникают новые вопросы и проблемы, которые приходится решать. Поэтому нужно продолжать изучение методов и деталей действенной практической реализации политики кибербезопасности и её совершенствования в условиях развития технологий и рисков коррупции.

Примечание

Представленные здесь взгляды принадлежат исключительно авторам и не выражают официальную позицию Консорциума военных академий и институтов изучения проблем безопасности программы «Партнерство ради мира», организаций-участниц или издателей Консорциума.

Благодарность

Connections: The Quarterly Journal, Vol. 20, 2021, вышел при поддержке правительства США.

Об авторах

Богдан Головкин – доктор права, профессор Кафедры криминологии и уголовно-исполнительного права Национального юридического университета имени Ярослава Мудрого (Харьков, Украина).
https://orcid.org/0000-0002-0333-9806

Алексей Таволжанский – сотрудник Кафедры криминологии и уголовно-исполнительного права Национального юридического университета имени Ярослава Мудрого (Харьков, Украина).
E-mail: tavolzhanskyi8020@sci-univ.com

Александр Лысодед – сотрудник Кафедры криминологии и уголовно-исполнительного права Национального юридического университета имени Ярослава Мудрого (Харьков, Украина).