

CONNECTIONS

ЕЖЕКВАРТАЛЬНЫЙ ЖУРНАЛ

СПЕЦИАЛЬНОЕ ИЗДАНИЕ CONNECTIONS



КОНСОРЦИУМ
«ПАРТНЕРСТВО РАДИ МИРА»
ВОЕННЫХ АКАДЕМИЙ И
ИНСТИТУТОВ ПО
ИЗУЧЕНИЮ ВОПРОСОВ
БЕЗОПАСНОСТИ

ВЕСНА 2021

КИБЕРПРЕСТУПНОСТЬ И ДЕЗИНФОРМАЦИЯ

РЕДАКТОРЫ:
ШОН КОСТИГАН, ТОДОР ТАГАРЕВ

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

Редакционный Совет Консорциума ПРМ

Шон С. Костиган	Главный редактор
Эд Кларк	Ответственный редактор
Аида Алымбаева	Институт анализа и развития инициативы, Бишкек
Пал Дунай	Центр им. Джорджа К. Маршалла, Гармиш-Партенкирхен
Филипп Флури	Женевский центр политики безопасности, Женева
Петр Гавличек	Варминьско-Мазурский университет в Ольштыне, Польша
Ганс-Йоахим Гиссманн	Бергхоф Фонд, Берлин
Динос Кериган-Кироу	Объединенный командно-штабной курс, Военный колледж, Силы обороны Ирландии
Крис Палларис	i-intelligence GmbH, Цюрих
Тамара Патарая	Кавказский институт мира, демократии и развития
Тодор Тагарев	Болгарская академия наук, София
Энекен Тикк	Институт киберполитики, Ювяскюля, Финляндия

Взгляды и статьи во всех публикациях *Connections* принадлежат исключительно авторам и не выражают официальную позицию Консорциума военных академий и институтов изучения проблем безопасности программы «ПрМ», организаций-участниц или издателей Консорциума.

Издание выходит при поддержке правительства США. Серия публикаций Консорциума доступна бесплатно по адресу <http://www.connections-qj.org>. Если вы хотите заказать для своей библиотеки печатные экземпляры или у вас есть вопросы касательно публикаций Консорциума, просим обращаться в Консорциум «Партнерства ради мира», PfPpublications2@marshallcenter.org.

Д-р Рафаэль Перл
Исполнительный директор

Шон С. Костиган
Главный редактор и председатель
редакционной коллегии



ISSN 1812-1101, e-ISSN 1812-2973

CONNECTIONS

THE QUARTERLY JOURNAL

том 20, № 2, весна 2021



Том 20, № 2, весна 2021 г.

Редакционная статья

- Борьба с преступностью, ненавистью и дезинформацией в киберпространстве 5
Шон Костиган, Тодор Тагарев

Рецензированные статьи

- Интернет: суверенный, или глобальный? Россия и Китай настаивают на заключении договора о киберпреступности 9
Шон Костиган
- Эволюция задач полиции по борьбе с киберпреступностью в Чехии, 2015-2020 гг. 15
Лукаш Вилим
- Доверие к провайдерам ИКТ: Помогут ли корпоративные меры кибердоверия? 21
Маттиас Клаус
- Пробелы в кибернавыках – системный обзор научной литературы 33
Гарри Руослахти, Джанель Кобёрн, Амир Трент, Илкка Тиканмяки
- Дезинформация: Политическая реакция для повышения устойчивости граждан 47
Инез Миямото
- Соцсети – Язык ненависти – Преступления на почве ненависти 57
Лукаш Вилим

Содержание

Коррупция как угроза кибербезопасности при новом мировом порядке	75
<i>Богдан Головкин, Алексей Таволжанский, Александр Лысодед</i>	
Дальнейшее развитие квантовых вычислений и их важность для НАТО	89
<i>Руперт Брэндмайер, Йорн-Александр Хайе, Клеменс Войвод</i>	



Ш. Костиган & Т. Тагарев, *Connections QJ* 20, № 2 (2021): 5-8
<https://doi.org/10.11610/Connections.rus.20.2.00>

Редакционная статья

Борьба с преступностью, ненавистью и дезинформацией в киберпространстве

Шон Костиган,¹ Тодор Тагарев²

¹ *Европейский центр исследований в области безопасности им. Джорджа Маршалла*, <https://www.marshallcenter.org/>

² *Институт информационно-коммуникационных технологий, Болгарская академия наук, София, Болгария*, <http://www.iict.bas.bg/EN>

Аннотация: Развитие связи и открытый доступ к Интернету дают злоумышленникам новые возможности для сбора информации, атак на уязвимые цели и формирования массового сознания и поведения. В редакционной статье этого выпуска *Connections* редакторы издания анализируют новые угрозы безопасности и реакцию на них. В центре внимания – рост киберпреступности, коррупция, распространение языка ненависти, пропаганды и дезинформации. Авторы также предлагают решения – усиление правового режима, в том числе международных норм, применение мер доверия и развитие кибернавыков, а также описывают вызовы для обороны, возникающие в результате развития квантовых вычислений.

Ключевые слова: киберпреступность, язык ненависти, дезинформация, стойкость, коррупция, квантовые вычисления.

Сегодня киберпространству серьёзно угрожает ряд проблем в основном политического характера. Такая гуманизация киберпространства может обрадовать тех, кто годами беспокоился о слабом политическом интересе “верхов” к единственному новому мировому «царству». Теперь, когда тема киберпространства так актуальна, легко забыть, что из-за своей условности кибернетика всегда считалась слишком технической сферой, чтобы привлечь внимание элиты – пока внезапно она не стала столь актуальной. Но по мере того, как кибернетика тихо развивалась и приобретала влияние, знающие

люди поняли, что кибернетика — не просто техническая проблема, и начали разрабатывать программы обучения и формировать новую область знаний, которая по своей природе является комплексной и междисциплинарной. Как не может быть кибернетики без технологий, точно так же не может быть кибернетики без людей.

Показательным примером служит этот выпуск *Connections*. Вниманию читателей предлагается восемь оригинальных статей о новых вызовах, выходящих за рамки организованных государствами киберопераций¹: это киберпреступность, коррупция, распространение языка ненависти, пропаганды и дезинформации в киберпространстве, а также решения в области технологий, политики, законодательства, образования и обучения.

Говорим ли мы о формировании доверия между частными компаниями² и людьми в киберпространстве или о развитии и вероятных последствиях квантовых вычислений,³ мы вступаем в уникальную эпоху изучения кибербезопасности. Технологии будут и дальше развиваться, порождая новые проблемы, но зрелая политика и наука, примеры чего мы видим в этом выпуске, помогут увидеть эти изменения и обеспечить надёжность. Технологии и политика неразрывно связаны. Кибербезопасность — уже не просто необходимая, но в значительной степени недостаточная техническая задача, направленная на то, чтобы сделать продукты более безопасными. Это сформировавшаяся область знаний с десятками взаимосвязанных, одинаково важных областей исследований.

С ростом проблем возрастает важность людей, их знаний и навыков.⁴ С каждым годом население мира всё больше зависит от киберпространства и кибербезопасности. Некоторые политические системы боятся мощи киберпространства, делая ставку на более сложные системы и сети для контроля мыслей своих граждан⁵ и формирования их поведения и политической

¹ Bilyana Lilly and Joe Cheravitch, "The Past, Present, and Future of Russia's Cyber Strategy and Forces," 12th International Conference on Cyber Conflict, CyCon 2020, online, May 26-29, 2020, pp. 129-155, <https://doi.org/10.23919/CyCon49761.2020.9131723>.

² Matthias Klaus, "Trusting ICT Providers – Can Corporate Cyber Confidence-Building Measures Help?" *Connections: The Quarterly Journal* 20, no. 2 (2021): 21-31, <https://doi.org/10.11610/Connections.20.2.03>.

³ Rupert A. Brandmeier, Jörn-Alexander Heye, and Clemens Woywod, "Future Development of Quantum Computing and Its Relevance to NATO," *Connections: The Quarterly Journal* 20, no. 2 (2021): 89-110, <https://doi.org/10.11610/Connections.20.2.08>.

⁴ Harri Ruoslahti, Janel Coburn, Amir Trent, and Ilkka Tikanmäki, "Cyber Skills Gaps – A Systematic Literature Review of Academic Literature," *Connections: The Quarterly Journal* 20, no. 2 (2021): 32-44, <https://doi.org/10.11610/Connections.20.2.04>.

⁵ Martti J. Kari and Katri Pynnöniemi, "Theory of Strategic Culture: An analytical Framework for Russian Cyber Threat Perception," *Journal of Strategic Studies* (in press), <https://doi.org/10.1080/01402390.2019.1663411>.

судьбы. Во многих странах ставят цель отделения от Интернета.⁶ Кампании дезинформации пересекают границы и точечно воздействуют на людей, подвергая испытаниям их стойкость и критическое мышление.⁷ Исследования этой проблемы показывают, насколько сейчас важны кибернавыки для деятельности общества.

Из-за демократизации инструментов и знаний киберпреступники сейчас могут иметь такие же возможности, как государства или большие корпорации. Многие некогда мелкие группировки выросли в преступные картели, некоторые даже предлагают совершение преступлений в качестве услуги, в то время как власть и полиция ведут борьбу с новым видом киберпреступности.⁸ Государства также используют новую угрозу киберпреступности, чтобы оправдать кардинально отличные воззрения на киберпространство.

Тем временем мировые проблемы с людскими ресурсами препятствуют нашей коллективной способности защитить киберпространство и усовершенствовать инфраструктуру, которой мы пользуемся.⁹ Чтобы удовлетворить эту потребность, программы кибербезопасности должны готовить специалистов, знающих все аспекты кибербезопасности: людей, процессы и технологии.

Этот выпуск *Connections* посвящён всем нашим неустанным специалистам в области кибербезопасности. Мы благодарны за ваши усилия и понимание своей миссии.

Наконец, большое спасибо – авторам издания за их терпение, позволившее наконец собрать этот интересный выпуск.

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.

⁶ Rongbin Han and Li Shao, “Scaling Authoritarian Information Control: How China Adjusts the Level of Online Censorship,” *Political Research Quarterly* (in press), <https://doi.org/10.1177/106591292111064536>.

⁷ Inez Miyamoto, “Disinformation: Policy Responses to Building Citizen Resiliency,” *Connections: The Quarterly Journal* 20, no. 2 (2021): 45-53, <https://doi.org/10.11610/Connections.20.2.05>.

⁸ Lukáš Vilím, “The Issue of Combating Cybercrime in the Czech Republic with Regard to the Last Five Years,” *Connections: The Quarterly Journal* 20, no. 2 (2021): 15-20, <https://doi.org/10.11610/Connections.20.2.02>.

⁹ Daniel Hulatt and Eliana Stavrou, “The Development of a Multidisciplinary Cybersecurity Workforce: An Investigation,” in *Human Aspects of Information Security and Assurance*, edited by Steven Furnell and Nathan Clarke, *IFIP Advances in Information and Communication Technology*, vol. 613 (Cham: Springer, 2021), pp. 138–147, https://doi.org/10.1007/978-3-030-81111-2_12.

Об авторах

Шон Костиган – профессор Европейского центра исследований в области безопасности им. Джорджа Маршалла и старший консультант рабочей группы по новым угрозам безопасности Консорциума программы «Партнерство ради мира».

Электронная почта: sean.costigan@marshallcenter.org

Д-р Тодор Тагарев – опытный политик в области безопасности и обороны с глубокими знаниями кибернетики, теории и практики управления. В настоящее время – профессор Института информационно-коммуникационных технологий Болгарской академии наук, где он возглавляет Центр управления безопасностью и обороной. Профессор Тагарев – член редколлегии *Connections: The Quarterly Journal* с 2004 года. <https://orcid.org/0000-0003-4424-0201>



Интернет: суверенный, или глобальный? Россия и Китай настаивают на заключении договора о киберпреступности

Шон Костиган

Европейский центр исследований в области безопасности им. Джорджа Маршалла, <https://www.marshallcenter.org/>

Аннотация: Под предлогом борьбы с киберпреступностью на международной арене борются два совершенно разных взгляда на киберпространство: модели киберпространства со свободным обменом, которую защищают демократические страны, противостоит так называемая суверенная модель. Продолжаются антидемократические инициативы по реформатированию киберпространства на сугубо национальных условиях, что может ослабить сотрудничество и повысить риски конфликтов и киберпреступности.

Ключевые слова: киберпреступность, киберпространство, суверенитет, сотрудничество, конфликт.

Хаос быстро становится нормой в киберпространстве, где киберпреступники действуют относительно безнаказанно, а новые технологии позволяют национальным государствам оттачивать практику мер воздействия. Компьютеры взламывают почти постоянно — согласно недавнему подсчету, в среднем каждые 39 секунд для устройств, подключенных к Интернету.¹ Если не бороться с киберпреступностью, под угрозой окажется вся вера в способность власти выполнить свои обещания в области безопасности. 61% европейцев обеспокоены возможностью манипуляций на выборах из-за кибератак. Каждый третий американец станет жертвой какого-то киберпреступ-

¹ “Hackers Attack Every 39 Seconds,” *Security Magazine*, February 10, 2017, <https://www.securitymagazine.com/articles/87787-hackers-attack-every-39-seconds>.

ления только в этом году, не говоря уже о риске государственного вмешательства.

Дезинформация занимает огромное место в новостях и политике, не меньше, чем во времена COVID-19. Российские кампании дезинформации регулярно распространяли пропаганду о вирусе через аналитические центры и сомнительные службы новостей.² Киберпространство стало средой национальной безопасности, влияющей на правительства, корпорации и отдельных граждан. Учитывая такое положение, от универсального договора о киберпреступности, кажется, выиграли бы все.

Под предлогом борьбы с киберпреступностью на международной арене борются два совершенно разных взгляда на киберпространство. Первый в целом можно описать как модель киберпространства со свободным обменом, которую защищают демократические страны. Ему противостоит вторая, так называемая «суверенная модель», где главное внимание уделяется контролю государства над информацией и в конечном счёте над людьми.

18 ноября 2019 г. Комитет ООН 88 голосами против 58 одобрил поддержанную Россией резолюцию о киберпреступности, 34 страны воздержались. Этим успешным для России голосованием была создана Рабочая группа открытого состава для проведения всестороннего исследования проблемы киберпреступности и ответных мер. Хотя это событие может показаться потенциально выгодным, оно несёт прямые последствия для Будапештской конвенции о киберпреступности³ и существующих механизмов совершенствования борьбы с киберпреступностью, международных и национальных правовых мер, а также долгосрочные внешнеполитические последствия во многих сферах, помимо киберпространства.

Будапештская конвенция – единственная конвенция о киберпреступности, но на неё постоянно оказывает давление Россия и её внешнеполитические партнёры, утверждающие, что само её существование нарушает суверенитет. (Заметим, что Будапештская конвенция открыта для присоединения стран, не входящих в Совет Европы, и является инструментом международного сотрудничества по борьбе с киберпреступностью.)

Россия также активно пытается физически перенести некоторые дискуссии о киберпреступности из Вены, Австрия (где решения принимаются консенсусом) в Нью-Йорк, где голосование большинством голосов может дать России и Китаю существенное преимущество при дальнейших обсуждениях.⁴

² Julian E. Barnes and David E. Sanger, “Russian Intelligence Agencies Push Disinformation on Pandemic,” *The New York Times*, July 28, 2020, <https://www.nytimes.com/2020/07/28/us/politics/russia-disinformation-coronavirus.html>.

³ Council of Europe, “Convention on Cybercrime,” Treaty No. 185, Budapest, November 23, 2001, www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185.

⁴ U.S. Department of State, “State Department Official on Multilateral Cyber Efforts,” Special Briefing, Office of the Spokesperson, Press Correspondents Room, December

Более того, Россия и Китай могут использовать такие победы в ООН не только для достижения своих далеко идущих целей, бросающих вызов всеобщим правам человека и идеалам открытого, свободного и неделимого Интернета, а также установленному после Второй мировой войны мировому порядку, который Россия и, главное, Китай считают в основном западной конструкцией, по их мнению, несправедливо выгодной западным государствам.

Учитывая эти шаги, в статье утверждается, что Западу нужно готовиться к будущим международным переговорам, которые могут пойти не по плану, включая дальнейшие успехи Китая и России в получении контроля над информацией и изменении киберпространства, каким мы его знаем.

Российское предложение глобальной конвенции о киберпреступности и стремление России продвигать «Рабочую группу открытого состава по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности»⁵ – это прежде всего политические шаги к достижению цели России: создать «систему международной информационной безопасности».⁶ Система, которую Кремль стремится создать, будет основана на «Конвенции о международной информационной безопасности», где важные роли отводятся ООН и Международному союзу электросвязи. Кроме того, российская концепция опирается на сильный, даже абсолютный государственный суверенитет, что перечёркивает реальные или предполагаемые международные обязательства государства.⁷

Аргументы России в пользу так называемого суверенного Интернета («Рунета») выделяют несколько аспектов автономной безопасности. Задача создания отдельного российского Интернета была поставлена в Доктрине информационной безопасности 2017 г.⁸ – «развитие национальной системы управления российским сегментом сети 'Интернет'». Контекст этой задачи

19, 2019, <https://web.archive.org/web/20191220024014/https://www.state.gov/state-department-official-on-multilateral-cyber-efforts/>.

⁵ United Nations Office for Disarmaments Affairs, “Developments in the Field of Information and Telecommunications in the Context of International Security,” <https://www.un.org/disarmament/ict-security/>.

⁶ “Basic Principles for State Policy of the Russian Federation in the Field of International Information Security to 2020,” approved by the President of the Russian Federation on 24 July, 2013, доступ на 29 сентября 2020, <http://en.ambruslu.com/highlights-in-russia/basic-principles-for-state-policy-of-the-russian-federation-in-the-field-of-international-information-security-to-2020.html>.

⁷ Alena Epifanova, “Deciphering Russia’s ‘Sovereign Internet Law’: Tightening Control and Accelerating the Splinternet,” *German Council on Foreign Relations*, January 16, 2020, <https://dgap.org/en/research/publications/deciphering-russias-sovereign-internet-law>.

⁸ *Доктрина информационной безопасности Российской Федерации*, утверждена Указом Президента Российской Федерации № 646 5 декабря 2016 г.

– «формирование системы международной информационной безопасности, направленной на достижение стратегической стабильности и равноправного стратегического партнерства, что не прямо, но фактически намекает на угрозу информационной безопасности, ощущаемую со стороны США. Цель «национального сегмента Интернета», как его ещё называют – защита собственно информации и критической информационной инфраструктуры России в случае угрозы стабильности, безопасности и функциональности.

Иногда русские оправдывают кажущуюся необходимость удержать внутрироссийский трафик в пределах территориальных границ финансовыми аргументами: с учетом этого стоимость международной маршрутизации в будущем может сильно вырасти.⁹ Требование предварительной установки российского программного обеспечения для «отслеживания, фильтрации и перенаправления интернет-трафика»¹⁰ можно рассматривать в контексте информационной безопасности, защиты критической инфраструктуры и поощрения отечественных исследований и разработок.¹¹ Очевидно, что расширение сферы действия федеральных (Роскомнадзора) правоприменительных механизмов с маршрутизации трафика на все устройства ИКТ тоже усиливает политический и информационный контроль над людьми.

Похоже, что цель этих шагов – создать неопределенность, чтобы разрушить проделанную работу и консенсус в отношении международных норм в киберпространстве, подрывая при этом базовые ценности открытого, бесплатного и доступного Интернета. По мнению многих экспертов, Россия и Китай рука об руку стараются навязать жёсткий подход к киберпространству под контролем государства. Это реализация их авторитарной политики, резко противоречащей демократическому порядку и подрывающей основы глобального экономического порядка и деловых интересов в долгосрочной перспективе.

Хотя голосование в 3-м Комитете ООН показало отсутствие консенсуса о начале переговоров или создании нового правового инструмента по киберпреступности, нужно понимать, что эти попытки не одиноки. Более того, нет консенсуса в отношении сферы регулирования такого нового договора по этому вопросу. Кроме того, страны Западной Европы, похоже, признают, что этот процесс отвлечёт внимание от реформ национального законодательства и развития потенциала, по сути срывая эти усилия.

⁹ По словам экспертов Касперского, сейчас всего 2% внутрироссийского трафика пересекает границы страны.

¹⁰ "Russia Internet: Law Introducing New Controls Comes into Force," *BBC*, November 1, 2019, <https://www.bbc.com/news/world-europe-50259597>.

¹¹ For an opposite view see Alexandra Prokopenko, "Russia's Sovereign Internet Law Will Destroy Innovation," *The Moscow Times*, April 21, 2019, www.themoscowtimes.com/2019/04/21/russias-sovereign-internet-law-will-destroy-innovation-a65317.

Новый международный правовой инструмент по киберпреступности будет дублировать нынешнюю работу и сорвет решение открытой межправительственной экспертной группы ООН (intergovernmental expert group, IEG)¹² о проведении всестороннего исследования проблемы киберпреступности и реакции на неё стран-участниц.

Россия не только продолжает, но и усиливает призывы к «системе международной информационной безопасности». Тем временем ряд экспертов утверждает, что Западу не удаётся убедить и привлечь на свою сторону другие страны.¹³ Москва и Пекин, по-видимому, равнодушны к попыткам «пристыдить» их, обвинениям в кибератаках и шпионаже, например, взломе при помощи SolarWinds.¹⁴ Тем временем на власти западных стран-единомышленников обрушиваются утечки в результате иностранного шпионажа,¹⁵ сообщения о массовой слежке,¹⁶ ухудшение шифрования,¹⁷ и особенно правительственные ожидания помощи корпораций. Чтобы эффективно парировать антидемократические инициативы, Западу нужно устранить одну из трех основ стратегии Кремля: общее недоверие к ИКТ, пробелы в существующем международном праве, или нарратив об экзистенциальной угрозе. Другой путь повышения киберустойчивости – определить общие национальные интересы и задачи разных лагерей и континентов, например, в рамках Основ ответственных действий государств в киберпространстве¹⁸ и Парижского призыва к доверию и безопасности в киберпространстве.¹⁹ Чтобы идти вперед, Запад должен готовиться к

¹² IEG – главный процесс в области киберпреступности на уровне ООН.

¹³ Sally Adee, “The Global Internet Is Disintegrating: What Comes Next?” *BBC*, May 15, 2019, www.bbc.com/future/article/20190514-the-global-internet-is-disintegrating-what-comes-next.

¹⁴ Sean S. Costigan, “Charting a New Path for Cybersecurity after SolarWinds.” *Diplomatic Courier*, January 4, 2021, www.diplomaticcourier.com/posts/charting-a-new-path-for-cybersecurity-after-solarwinds.

¹⁵ Patricia L. Bellia, “WikiLeaks and the Institutional Framework for National Security Disclosures,” *Yale Law Journal* 121, no. 1448 (2012), April 2, 2012, Notre Dame Legal Studies Paper No. 12-59, <https://ssrn.com/abstract=2033207>.

¹⁶ Zygmunt Bauman et al., “After Snowden: Rethinking the Impact of Surveillance,” *International Political Sociology* 8, no. 2 (June 2014): 121-144.

¹⁷ Aaron Brantly, “Banning Encryption to Stop Terrorists: A Worse than Futile Exercise,” *CTC Sentinel* 10, no. 7 (August 2017): 29-33, https://ctc.usma.edu/wp-content/uploads/2017/08/CTC-Sentinel_Vol10Iss7-10.pdf.

¹⁸ “Joint Statement on Advancing Responsible State Behavior in Cyberspace,” United States Department of State, September 23, 2019, <https://www.state.gov/joint-statement-on-advancing-responsible-state-behavior-in-cyberspace/> and “Eleven Norms of Responsible State Behaviour in Cyberspace,” Federal Department of Foreign Affairs FDFA, April 7, 2021, <https://www.eda.admin.ch/eda/en/fdfa/fdfa/aktuell/newsuebersicht/2021/04/uno-cyber-normen.html>.

¹⁹ “Paris Call for Trust and Security in Cyberspace – Paris Call,” <https://pariscall.international/en/>.

возможному обсуждению договора. Если подготовиться к такому худшему сценарию, можно найти возможность избежать его.

Примечание

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

Об авторе

Шон Костиган – см. резюме на стр. 8 этого издания, <https://doi.org/10.11610/Connections.rus.20.2.00>.



Эволюция задач полиции по борьбе с киберпреступностью в Чехии, 2015-2020 гг.

Лукаш Вилим

Министерство внутренних дел Чешской Республики,

<https://www.mvcr.cz/mvcren/>

Аннотация: В статье рассматриваются расширенные задачи чешской полиции по борьбе с киберпреступностью. Автор подчёркивает важность концептуальных и стратегических факторов появления нового законодательства, финансового обеспечения закупок новой техники и создания новых рабочих мест для специалистов по киберпреступности. Кроме того, крайне важна разработка новых стратегий, соответствующих угрозам, вызовам и возможностям киберпространства. Тесное сотрудничество на всех уровнях системы безопасности может помочь выработке стратегий и тем самым сделать киберпространство более безопасным.

Ключевые слова: киберпреступность, Будапештская конвенция, система безопасности, стратегия, координатор, критическая информационная инфраструктура.

Важным этапом борьбы с киберпреступностью в Чехии стало утверждение правительством 10 июля 2017 г. Концепции развития возможностей чешской полиции по расследованию киберпреступлений (далее – Концепция) под № 502.

Конечно, в этой связи мы не можем не упомянуть о профессионалах, которые занимались киберпреступностью ранее, на местном, региональном и национальном уровне. Определённые изменения в подходах к этому вопросу были внесены ещё в октябре 2015 г., когда Отдел по борьбе с организованной преступностью (*Útvar pro odhalování organizovaného zločinu – ÚOOZ*) начал активно заниматься киберпреступностью. В 2016 г. борьба с киберпреступностью стала частью концептуальной программы созданного

национального подразделения Национального управления по борьбе с организованной преступностью (*Národní centrála proti organizovanému zločinu – NCOZ*). Следует также отметить, что правоохранительные органы обращали внимание на преступную деятельность в киберпространстве с появления Интернета.

Однако вышеупомянутая Концепция впервые в Чехии подошла к проблеме комплексно. Она охватывает разные сферы, существенно усиливая способность чешской полиции бороться с такого рода преступлениями – от наращивания и обучения персонала до законодательных изменений, повлиявших на всю полицию Чехии. В тексте решения об утверждении Концепции, опубликованном также на сайте чешского правительства, сказано, что Концепция

меняет организацию и штат чешской полиции с 1 сентября 2017 г. Добавляются 30 должностей в чешской полиции, с соответствующим увеличением бюджета для оплаты труда персонала сил безопасности на 4 595 280 чешских крон в 2017 г. Это решение будет иметь долгосрочный эффект в последующие годы, с выполнением требований в 2018 г. и в среднесрочной перспективе на 2019-2020 гг. Выделенный бюджет превысит ранее утвержденные лимиты Министерства внутренних дел ... и в 2018 г. появятся 73 новых должности.

Концепция выдвинула высокие требования ко всем, кто участвовал в её реализации и работал над выполнением её условий. Её заслуга в том, что она чётко задала направление выявления, документирования и расследования этого нового вида преступной деятельности. Был усилен персонал, за чем последовала новая система образования, чтобы обучать и готовить сотрудников полиции, занимающихся этой проблемой на всех уровнях.

В законодательстве был изменён Закон № 141/1961 Coll. об уголовном процессе (Уголовно-процессуальный кодекс), касающийся сбора, хранения, использования, обмена и уничтожения данных. Также уделено внимание обнаружению, документированию и расследованию атак на критическую информационную инфраструктуру, включая её защиту от терактов, путем изменений в Законе № 40/2009 Coll., Уголовный кодекс. Конкретно было добавлен новый пункт (e) к первой части Статьи 311 – серьёзные атаки на компьютерные системы, важные для деятельности общества и государства (включая важные информационные системы и критическую информационную инфраструктуру).

Важность Статьи 311 e) заключается в её направленности на теракты в киберпространстве и, соответственно, необходимость защиты конституционной системы и обороны Чехии, а также основных политических, экономических и общественных структур, граждан и международных организаций от политического насилия и экстремизма. Такой теракт может нарушать закон путём ввода данных в компьютерную систему или базу данных либо удаления или повреждения данных, хранящихся в компьютерной системе (базе данных), снижая их качество или приводя их в негодность. Атака на

компьютерную систему может влиять на функционирование государства, здоровье людей, безопасность, экономику или обеспечение базовых потребностей населения. Кроме того, атака с применением специального вредоносного ПО может повредить множество компьютерных систем и нанести большой ущерб.¹

В 2019 г. ускорили сохранение данных на компьютерной системе или носителе информации в интересах уголовного процесса, добавив в Уголовно-процессуальный кодекс § 7b, позволивший, при определённых условиях, отдать приказ об ускоренном сохранении данных, важных для уголовного процесса. Согласно § 7b, хранение данных – временная мера, дающая полиции нужное время для защиты данных.²

Ещё одна важная норма была введена изменением Закона № 104/ 2013 Coll. «О международном правовом сотрудничестве в уголовных делах». Новый § 65a разрешил ускоренную передачу данных, хранящихся на компьютерной системе на территории другого государства. Этот закон прямо регулирует задачи координатора по вопросам киберпреступности чешской полиции при направлении запросов о предоставлении данных за рубежом с согласия Прокуратуры. У европейских стран хранимые данные запрашивают Европейским следственным ордером. Такой запрос выдаёт или утверждает судебный орган одной страны ЕС, разрешая следственные действия для сбора или использования улик в уголовных делах в другой стране ЕС. Он действует во всём ЕС, кроме Дании и Ирландии.³ За пределами Евросоюза данные запрашивают на основании договора о взаимной правовой помощи – соглашения между двумя или несколькими странами о сборе и обмене информации во исполнение общего или уголовного законодательства. Запрос в рамках взаимной правовой помощи обычно используют для официального допроса подозреваемого в уголовном преступлении, если подозреваемый живет в другой стране.⁴

Был назначен национальный координатор по вопросам киберпреступности для упорядочения помощи в сотрудничестве и, соответственно, выполнения задач, возникших для Чехии в связи с Конвенцией о киберпреступности Совета Европы (Конвенция о киберпреступности, Будапешт, 23 ноября 2001 г., ETS № 185). Поставленные задачи выполняются круглосуточно и без выходных. Этот координатор также существенно помогает вы-

¹ Act No. 40/2009 Coll., “The Criminal Code of the Czech Republic,” section 311, letter e).

² Act. No. 141/1961 Coll., “The Criminal Procedure of the Czech Republic.”

³ Eurojust, European Union Agency for Criminal Justice Cooperation, “European Investigation Order,” доступ на 18 апреля 2021, <https://www.eurojust.europa.eu/judicial-cooperation/eurojust-role-facilitating-judicial-cooperation-instruments/european-investigation-order-eio>.

⁴ European Commission, “Mutual Legal Assistance and Extradition. Combating Crime Across Borders,” https://ec.europa.eu/info/law/cross-border-cases/judicial-cooperation/types-judicial-cooperation/mutual-legal-assistance-types-and-extradition_en.

явлению киберпреступлений и помогает спасению жизней в случае возможных угроз жизни и здоровью в киберпространстве. Чешский национальный координатор по вопросам киберпреступности руководствуется следующими законами и конвенциями:

- Национальный координатор по вопросам киберпреступности согласно Статье 35 Конвенции о киберпреступности (Будапештская конвенция, ETS № 185);
- Координатор согласно Статье 13 Директивы Европейского парламента и Совета ЕС 2013/40/ЕС от 12 августа 2013 г. об атаках на информационные системы – совместно с национальным следственным органом;
- Координатор согласно Протоколу действий правоохранительных органов ЕС в чрезвычайных ситуациях по отражению крупных трансграничных кибератак – совместно с национальным следственным органом;
- Координатор Чешской банковской ассоциации (CBA), администратора домена .cz и национальной группы CSIRT (CZ.NIC);
- Координатор сети G7 24/7 НТС.

Главные задачи, согласно Статье 35 Конвенции о киберпреступности:

- технические консультации;
- хранение данных;
- сбор доказательств;
- предоставление правовой информации;
- установление местоположения подозреваемых и пропавших лиц;
- оперативная связь с другими координаторами.

Четыре года борьбы с киберпреступностью на основе представленной Концепции были успешными. Это подтвердила Резолюция Совета национальной безопасности Чешской Республики от 8 июня 2020 г., одобрявшая Итоговый доклад о выполнении задач Концепции развития возможностей чешской полиции по расследованию киберпреступлений. Он же принял решение о разработке новой стратегии борьбы с киберпреступностью.

Судя по дальнейшей динамичной эволюции киберпреступности и по более чем заметному росту преступности в виртуальном мире, для победы над киберпреступностью в будущем понадобится ещё больше усилий. Она потребует внимания со стороны правоохранительных органов и других специалистов в области безопасности, представляющих государство и частный сектор. Киберпространство стало элементом нашей повседневной жизни, который несёт ряд рисков и должен быть надёжно защищён.

В XXI веке придётся заниматься не только общими преступлениями, совершаемыми в виртуальном мире, но и защитой критической информационной инфраструктуры. Это комплексная задача, влияющая на все уровни

системы безопасности и включающая кризисное управление. Нужно понимать, что критическая инфраструктура важна для общества и функционирования демократического государства и является краеугольным камнем процветающей экономики. Поэтому её защита жизненно важна для недопущения перерастания инцидентов в кризисы.

Защиту критической информационной инфраструктуры в киберпространстве можно разделить на три основных уровня: киберзащита, кибербезопасность и киберпреступность. В организационном плане обеспечение безопасности требует эффективных и скоординированных действий вооружённых сил, профильного ведомства кибербезопасности (Национальное управление кибернетической и информационной безопасности; *Národní úřad pro kybernetickou a informační bezpečnost – NÚKIB*), сил безопасности (особенно чешской полиции) и, наконец, разведслужб, а также частного сектора.

Роль государства также заключается в установлении базовых стандартов безопасности и их юридическом распространении на частный сектор. Однако эти меры должны быть финансово обеспечены, и государство обязано обеспечить адекватную защиту киберпространства. Следует помнить, что значительная часть критической инфраструктуры государства не является его исключительной собственностью. Государство лишь участвует в её управлении, в мажоритарной или миноритарной роли.

С этим связана дальнейшая потребность классифицировать киберпреступность, чтобы дать специалистам по компьютерным технологиям возможность выявлять, документировать и расследовать серьёзные киберпреступления, в частности, разного рода атаки на информационную инфраструктуру и важные информационные системы, включая самые серьёзные – терроризм и шпионаж.

Для этого киберпреступность получила новое определение:

- преступление, совершенное в среде информационно-коммуникационных технологий, включая компьютерные сети, где основным объектом нападения является сама область информационно-коммуникационных технологий и содержащиеся в ней данные; отсюда следует, что основное внимание экспертов будет направлено на соответствие установленным критериям – примерами являются § 230 «Несанкционированный доступ к компьютерной системе или носителю информации» и § 231 «Получение и кодирование устройства доступа и пароля к компьютерной системе и другим подобным данным»;
- любое другое преступление, совершённое в киберпространстве, определяемое как преступление, совершённое при значительном использовании информационно-коммуникационных технологий, где главным объектом атаки является жизнь, здоровье, имущество, свобода, человеческое достоинство и мораль.

Заклучение

В силу упомянутых выше причин в ближайшем будущем должна быть разработана новая стратегия противодействия киберпреступности, которая должна учесть множество факторов, включая тесное сотрудничество разных партнёров, обеспечивающих безопасность киберпространства. Новая стратегия должна быть представлена Совету безопасности Чешской Республики в 2021 г. Нельзя исключать, что на неё повлияет пандемия COVID-19, вынудившая большую часть общества работать и проводить свободное время в Интернете; для кого-то он стал вторым домом. Наконец, она может касаться киберзащиты от вирусных атак организованных преступных групп и враждебных стран на критическую информационную инфраструктуру, а также их расследование. Другим серьёзным вызовом будущего станет борьба с дезинформацией, что, однако, потребует более тесного взаимодействия всей системы безопасности, и не только в Чехии.

Будапештская конвенция о киберпреступности может служить хорошим примером подхода к другим проблемам безопасности в киберпространстве. Поэтому я могу с уверенностью сказать, что Чехия находится на верном пути в борьбе с киберпреступностью, и верю, что в будущем она усилится.

Примечание

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

Благодарность

Статья написана при поддержке Министерства внутренних дел Чешской Республики, проект № VI20192022117, «Выявление радикализации в контексте защиты населения и незащищённых объектов от насилия».

Об авторе

Лукаш Вилим – подполковник Национального управления по борьбе с организованной преступностью Министерства внутренних дел Чешской Республики, офицер отдела киберпреступности уголовной полиции и службы расследований в Праге. Получил докторскую степень в Полицейской академии в Праге. Д-р Вилим – выпускник программы кибербезопасности и семинара восточноевропейской безопасности Центра им. Джорджа Маршалла. Электронная почта: lukas.vilim@email.cz



Доверие к провайдерам ИКТ: Помогут ли корпоративные меры кибердоверия?

Маттиас Клаус

Аннотация: Доверие в киберпространстве важно для укрепления безопасности, и оно ещё важнее, когда страны привлекают частные компании для разработки, строительства, обслуживания и функционирования своей информационно-коммуникационной инфраструктуры. В данной статье предлагается новый формат мер кибердоверия для достижения этой цели путём привлечения частного сектора, как равного партнёра. Страны могут использовать этот метод для проверки своих потенциальных поставщиков, чтобы снизить восприятие риска, а также установить и поддерживать доверительные отношения с ними.

Ключевые слова: доверие, безопасность цепочек поставок, киберриск, инфраструктура ИКТ, меры кибердоверия.

Вступление

Странам нужно либо доверять подрядчикам, либо запретить им строить и обслуживать инфраструктуру информационно-коммуникационных технологий (ИКТ). В мире, где технические знания и средства для разработки, эксплуатации и обслуживания инфраструктуры ИКТ почти всецело принадлежат частным компаниям, страны всё больше зависят от частного сектора. Поскольку защищённость поставляемого программного обеспечения и техники определить невозможно, доверие между клиентом и поставщиком имеет огромное значение, как и классическое доверие между гражданами, правительством и корпорациями.¹ Чтобы защитить свои интересы от угроз безопасности, страна выберет компанию, которой она доверяет. Она будет оценивать ИКТ провайдеров на основе доверия и прозрачности. Даже если

¹ George Cvetkovich and Ragnar E. Löfstedt, eds., *Social Trust and the Management of Risk* (London: Earthscan, 1999).

у страны нет заслуживающих доверия вариантов, ей всё равно нужно выбрать компанию. В Пражских предложениях 2019 г. (результаты международной конференции по безопасности 5G) это названо одним из самых важных политических рисков безопасности при управлении ИТ-инфраструктурой страны.² Эта задача критична и все более сложна, особенно учитывая, что один из главных кандидатов, Huawei, подозревают в контроле со стороны Компартии Китая (КПК).

Цель этой статьи — предложить меры укрепления доверия на основе уроков опыта работы с Huawei. Конкретно в ней предложена модель для не пользующихся доверием стран и компаний в виде скорректированных мер доверия для снижения риска потенциальных покупателей. Странам-покупателям это может дать гарантии при выборе подходящего ИКТ-провайдера, а поставщикам — возможность доказать свою прозрачность и независимость. В мире, где больше нет доверия, такое прозрачное и активное общение может помочь восстановить доверие и сохранить связь между участниками противоборствующих политических систем.³

Пример Huawei

Huawei — ведущая ИКТ-компания, которая поднялась за счёт крупных государственных субсидий и преференций на внутреннем рынке Китая.⁴ Статус Huawei как «национального лидера» в такой высокотехнологичной отрасли, как ИКТ,⁵ позволил ей стать крупнейшим в мире производителем телекоммуникационного оборудования и вторым производителем смартфонов.⁶

В Huawei утверждают, что это частная компания,⁷ но её организация отличается от классической. Главный аргумент Huawei — то, что сотрудники компании одновременно являются её собственниками, почти 87 000 акционеров выбирают Представительскую комиссию. Комиссия избирает Совет

² “The Prague Proposals: The Chairman Statement on Cyber Security of Communication Networks in a Globally Digitalized World,” Prague 5G Security Conference, Prague, May 3, 2019, по состоянию на 12 марта 2020, https://www.vlada.cz/assets/media-centrum/aktualne/PRG_proposals_SP_1.pdf.

³ Ragnar E. Löfstedt, *Risk Management in Post-Trust Societies*, Earthscan Risk in Society series (London: Earthscan, 2008).

⁴ “The Real Cost to Rip and Replace of Chinese Equipment in Telecom Networks,” *Strand Consult*, 2019, p. 12, по состоянию на 1 февраля 2020, <https://strandconsult.dk/the-real-cost-to-rip-and-replace-chinese-equipment-from-telecom-networks>.

⁵ Tai Ming Cheung, “The Rise of China as a Cybersecurity Industrial Power: Balancing National Security, Geopolitical, and Development Priorities,” *Journal of Cyber Policy* 3, no. 3 (2018): 306-326, 311, <https://doi.org/10.1080/23738871.2018.1556720>.

⁶ Elsa Kania, “Much Ado about Huawei (part 1),” *The Strategist* (Australian Strategic Policy Institute), March 27, 2018, по состоянию на 9 марта 2020, <https://www.aspi.org.au/much-ado-huawei-part-1>.

⁷ “Huawei’s Position Paper on Cyber Security” (Huawei, November 2019), 61, по состоянию на 12 марта 2020, <https://www-file.huawei.com/-/media/corp/facts/pdf/2019/huaweis-position-paper-on-cyber-security.pdf?la=en>.

директоров и Наблюдательный совет, которые, в свою очередь, выбирают Правление.⁸

Хотя это отчасти верно, представительство компании умалчивает о важных деталях своих связей с КПК. Главное – 99% её акций принадлежат не основателю или сотрудникам, а профсоюзному комитету Huawei Investment & Holding. Профком Huawei Investment & Holding в конечном счёте подотчётен Всекитайской федерации профсоюзов, глава которой – член Политбюро ЦК Коммунистической партии Китая (КПК).⁹ Следует также учитывать роль КПК в компании, о чём свидетельствует то, что её нынешний начальник отдела контроля и этики – партийный секретарь.

Китайские государственные банки тоже относятся к Huawei, как к государственной компании. Так, главный финансист Huawei – Китайский банк развития, который контролируется китайским правительством и является крупнейшим в мире кредитором.¹⁰ Профиль рисков 2018 г. показывает, что Huawei получил миллиарды долларов финансирования и от нескольких государственных банков Китая.¹¹ Арест в 2018 г. главного бухгалтера Huawei, имевшего несколько разных паспортов, включая паспорт «общественного лица», который обычно выдают государственным чиновникам, вызывает сомнения в утверждениях о независимости.¹²

Недоверие усиливает и китайская практика кибершпионажа. Критики утверждают, что в Китае не различают военно-политический шпионаж, который ведёт каждая страна, и массовую, экономически мотивированную кражу интеллектуальной собственности у бизнес-конкурентов. Хуже того, КПК делится краденными результатами с китайскими компаниями, что даёт им экономические преимущества, дополняющие щедрые государственные субсидии.¹³ Успех Huawei объясняет именно государственная поддержка, поскольку она позволила Huawei быстро развиваться, устранив конкурентов.

⁸ “Who Runs Huawei: Ownership and Governance,” *Huawei*, по состоянию на 24 марта 2020, <https://www.huawei.com/minisite/who-runs-huawei/en>.

⁹ Christopher Balding and Donald C. Clarke, “Who Owns Huawei?” *SSRN Journal*, April 17, 2019, <https://doi.org/10.2139/ssrn.3372669>.

¹⁰ Bob Seely, Peter Varnish, and John Hemmings, “Defending Our Data: Huawei, 5G and the Five Eyes,” *Henry Jackson Society*, Asia Studies Centre, May 16, 2019, p. 26, по состоянию на 1 февраля 2020, <https://henryjacksonsociety.org/publications/defendingourdata>.

¹¹ RWR Advisory Group, “A Transactional Risk Profile of Huawei,” February 13, 2018, p. 20, по состоянию на 17 марта 2020, <https://www.rwradvisory.com/wp-content/uploads/2019/03/RWR-Huawei-Risk-Report-2-13-18.pdf>.

¹² Michael Mui, “How Meng Wanzhou’s ‘P’ Passport Works,” *The Star*, January 23, 2019, <https://www.thestar.com/vancouver/2019/01/23/how-meng-wanzhou-p-passport-works.html>.

¹³ Su-Mei Ooi and Gwen D’Arcangelis, “Framing China: Discourses of Othering in US News and Political Rhetoric,” *Global Media and China* 2, no. 3-4 (2017): 269-283, 275, <https://doi.org/10.1177/2059436418756096>.

Беспокойство вызывает и возможность Китая принуждать компании к сотрудничеству с разведслужбами. В Законе о разведке 2017 г. есть статьи, которые могут давать китайскими разведслужбами доступ к ИКТ Huawei или право принуждать компанию к сотрудничеству.¹⁴ В частности, основания для контроля приведены в Статье 7. Китай уверяет, что Статья 7 неправильно понята и не угрожает безопасности.¹⁵ В ответ Huawei попросил китайскую юридическую фирму подтвердить это,¹⁶ но критики отмечают, что правовая оценка не устраняет беспокойство.¹⁷ В данный момент есть основания считать, что неисполнение Huawei Статьи 7 испортило бы её отношения с КПК.

Чтобы укрепить доверие к компании, глава Huawei в 2019 г. предложил подписать «соглашение об отказе от шпионажа» с Великобританией, Германией и Индией,¹⁸ но это предложение не вызвало доверия других стран, потому что Huawei не ведёт себя, как частная компания. Например, Huawei утверждает, что избегает публичности по моральным соображениям. Сили, Варниш и Хеммингс¹⁹ подозревают, что реальной причиной может быть «юридическое требование сообщать структуру компании, данные аудита и финансовые отчеты, касающиеся движения денежных средств, капитала и балансов, общественности, акционерам и таким органам, как Комиссия по ценным бумагам и фондовому рынку США». Кроме того, Сили и др.²⁰ отмечают, что «отсутствие соглашений о сотрудничестве в области безопасности или подобных договоров, в частности, решений о достаточности мер защиты данных» свидетельствует о рисках китайских технологических компаний в данной ситуации.

Всё больше стран запрещают технику Huawei в своих сетях из-за риска, вызванного тесными связями Huawei с КПК и боязнью шпионажа. В настоящее время Huawei запрещён, в частности, в США, Великобритании, Японии, Тайване, Австралии, Новой Зеландии, Швеции, Чехии, Дании, Эстонии, Гернси, Джерси, Латвии, Польше и Румынии. Развивающиеся страны обращают меньше внимания на угрозы безопасности. В большинстве случаев

¹⁴ People's Republic of China, National Intelligence Law of the People's Republic, June 27, 2017.

¹⁵ Bonnie Girard, "The Real Danger of China's National Intelligence Law," *The Diplomat*, February 23, 2019, по состоянию на 2 мая 2020, <https://thediplomat.com/2019/02/the-real-danger-of-chinas-national-intelligence-law>.

¹⁶ Seely, Varnish, and Hemmings, "Defending Our Data: Huawei, 5G."

¹⁷ Samantha Hoffman and Elsa Kania, "Huawei and the Ambiguity of China's Intelligence and Counter-Espionage Laws," *The Strategist* (Australian Strategic Policy Institute), September 13, 2018, по состоянию на 17 марта 2020, www.aspistrategist.org.au/huawei-and-the-ambiguity-of-chinas-intelligence-and-counter-espionage-laws.

¹⁸ "Huawei Answers on Cybersecurity," *Huawei*, October 21, 2019, по состоянию на 26 февраля 2020, <https://www.huawei.eu/story/huawei-answers-cybersecurity>.

¹⁹ Seely, Varnish, and Hemmings, "Defending Our Data: Huawei, 5G."

²⁰ Seely, Varnish, and Hemmings, "Defending Our Data: Huawei, 5G."

причина заключается в одновременном предоставлении займов и других форм помощи китайскими государственными организациями,²¹ что помогает развивающимся странам преодолеть препятствия для получения технологий.

Пробел: Меры кибердоверия

В отсутствие общепринятых правил страны применяют меры доверия, основанные на нормах контроля обычных вооружений, для укрепления доверия в киберпространстве. Пока что международно признанных обязательных норм приемлемого поведения в этой сфере нет. Международное сообщество согласилось, что существующие международные законы, включая Хартию Организации Объединённых Наций (ООН), действуют и в киберпространстве.²² Однако нет единства в том, как применять и выполнять эти законы по отношению к конкретным кибероперациям. Одна из причин состоит в том, что существующие законы не рассчитаны на кибердеятельность. Ещё одна причина – отсутствие консенсуса между странами в терминах и определениях, необходимых для выработки приемлемых правил. Часто это объясняется недоверием или отсутствием доброй воли для компромисса со странами-оппонентами из-за нежелания рисковать, доверившись деятелям с иными ценностями.²³

Меры доверия призваны уменьшить риск или его восприятие, укрепляя доверие и улучшая отношения между странами-участницами. Цель мер кибердоверия – установить стабильные международные отношения и общее понимание приемлемых норм поведения государств в киберпространстве.²⁴ Они охватывают обмен информацией и сотрудничество стран в борьбе с незаконными кибератаками разных видов.²⁵ Опираясь на классический контроль вооружений, международные игроки могут оформить меры кибердоверия в виде двусторонних и многосторонних договоров.²⁶

²¹ Cheung, “The Rise of China as a Cybersecurity Industrial Power,” 323.

²² UN General Assembly, “Developments in the Field of information and Telecommunication in the Context of International Security,” Resolution 70/237 Adopted by the General Assembly on December 23, 2015, по состоянию на 18 марта 2020 (United Nations, 2015), <https://undocs.org/en/A/RES/70/237>.

²³ Michael Siegrist, George Cvetkovich, and Claudia Roth, “Salient Value Similarity, Social Trust, and Risk/Benefit Perception,” *Risk Analysis: An International Journal* 20, no. 3 (2000): 353-362, <https://doi.org/10.1111/0272-4332.203034>.

²⁴ Katharina Ziolkowski, ed., *Peacetime Regime for State Activities in Cyberspace: International Law, International Relations and Diplomacy* (Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2013).

²⁵ Geun Hye Kim, Kyung Bok Lee, and Jong In Lim, “CBMs for Cyberspace beyond the Traditional Environment: Focusing on Features for CBMs for Cyberspace in Northeast Asia,” *The Korean Journal of Defense Analysis* 27, no. 1 (2015): 87-106.

²⁶ Arnold Kraesten, “Cyber Confidence-Building Measures. Ten Stumbling Blocks Which Complicate the Development and Implementation of Worldwide Politically Acceptable

Они усиливают общее чувство безопасности стран, демонстрируя добрые намерения всех участников.²⁷ Меры кибердоверия также могут помочь обмену методами и практикой работы, а также взаимным ожиданиям поведения. Поскольку нормы отражают стандарты поведения, ожидаемые от стран в киберпространстве, меры и нормы кибердоверия часто дополняют друг друга.²⁸

Меры кибердоверия разработаны для взаимодействия государственных учреждений, поэтому сейчас они не применимы к отношениям государственных и негосударственных субъектов. Большинство экспертов согласны, что меры кибердоверия также должны учитывать многосторонний характер киберпространства, куда входят и частные корпорации.²⁹ Однако разработкой мер кибердоверия и кибернорм в основном занимаются традиционные межгосударственные международные и региональные организации, такие, как ООН или Организация по безопасности и сотрудничеству в Европе (ОБСЕ).³⁰ Это имеет смысл для мер доверия, где государства – единственные носители военной и ядерной мощи, но бесполезно в киберпространстве. Здесь власть по умолчанию принадлежит не только государствам, но и технологическим компаниям, которые разрабатывают и эксплуатируют большую часть критической инфраструктуры, включая сети 5G.

Предложение: Расширение мер кибердоверия на негосударственные субъекты

В статье Хитченса и Галлахера сравнивается прогресс работы Группы правительственных экспертов ООН и ОБСЕ по разработке норм и мер кибердоверия в апреле 2019 г. Два момента там представляют ценность для нашей статьи. Во-первых, авторы подчёркивают важность отношений между государственными и негосударственными субъектами, прежде всего – в обмене

Cyber Confidence-building Measures,” MSc in Cyber Security, with assistance of Sergej Boeke (The Hague, 2016).

²⁷ Erica D. Borghard and Shawn W. Lonergan, “Confidence Building Measures for the Cyber Domain,” *Strategic Studies Quarterly* 12, no. 3 (Fall 2018), по состоянию на 26 декабря 2019, <https://www.hsdl.org/?view&did=815333>.

²⁸ Patryk Pawlak, “Confidence-Building Measures in Cyberspace: Current Debates and Trends,” in *International Cyber Norms: Legal, Policy & Industry Perspectives*, ed. Anna-Maria Osula and Henry Rõigas (Tallinn: NATO CCD COE Publication, (2016), 129-153, https://ccdcoe.org/uploads/2018/10/InternationalCyberNorms_Ch7.pdf.

²⁹ Jason Healey, John C. Mallery, Klara J. Tothova, and Nathaniel V. Youd, “Confidence-Building Measures in Cyberspace: A Multistakeholder Approach for Stability and Security,” Report (Atlantic Council, November 5, 2014), по состоянию на 30 декабря 2019, <https://atlanticcouncil.org/in-depth-research-reports/report/confidence-building-measures-in-cyberspace-a-multistakeholder-approach-for-stability-and-security>.

³⁰ Borghard and Lonergan, “Confidence Building Measures for the Cyber Domain.”

информацией и оценке риска.³¹ Во-вторых, они рекомендуют расширить круг участников за счёт «компаний, владеющих или использующих ключевые компоненты инфраструктуры ИКТ ... вместе с некоторыми провайдерами услуг кибербезопасности частного сектора»,³² в унисон с недавними заявлениями ОБСЕ и Группы правительственных экспертов ООН. В разработке и применении мер кибердоверия должны участвовать и государственные, и негосударственные субъекты, включая частные компании.

В качестве причин нынешнего неучастия ИКТ-сектора в разработке мер кибердоверия приводится «непонимание правительствами киберсферы, ручное регулирование и попытки национальных служб безопасности скомпрометировать инструменты и сети частного сектора в своих интересах».³³ Согласно традиции классических мер кибердоверия, Хитченс и Галлахер призывают развивать сотрудничество для лучшей интеграции частных компаний. Но наша статья предлагает иное толкование описанной в цитате картины. Именно непонимание киберсферы правительствами даёт компаниям возможность скомпрометировать попытки государства регулировать киберпространство. Поэтому страны должны быть заинтересованы в том, чтобы провайдеры ИКТ были не просто участниками процесса мер кибердоверия – они должны стать равноправными субъектами.

В Центре передового опыта совместной защиты от киберугроз НАТО (Cooperative Cyber Defence Centre of Excellence, CCD COE) различают две группы мер кибердоверия. Одна модель основана на спросе, где нормы приемлемого поведения в киберпространстве подстёгивают разработку параллельных мер кибердоверия, что ведёт к росту кибервозможностей. Другая модель основана на предложении – новые кибервозможности, часто разработанные и внедрённые негосударственными субъектами, подстёгивают разработку «конкретных совместных мер доверия для всех сторон».³⁴ Эти меры кибердоверия ведут к появлению новых норм использования странами новых возможностей.

Павляк планировал использовать негосударственные субъекты для улучшения межгосударственных отношений, но для нашей статьи важно отличие между разными моделями мер кибердоверия. В статье утверждается, что с развитием прорывных технологий в киберпространстве, таких, как 5G, возникает необходимость разработки мер кибердоверия, чтобы снизить риски участников. Как видно из нынешних дебатов о включении или не-включении Huawei в сети 5G ряда стран, эти прорывные технологии, не совсем ещё разработанные и даже понятые, уже стали реальностью.

³¹ Theresa Hitchens and Nancy W. Gallagher, “Building Confidence in the Cybersphere: A Path to Multilateral Progress,” *Journal of Cyber Policy* 4, no. 1 (2019): 4-21, <https://doi.org/10.1080/23738871.2019.1599032>.

³² Hitchens and Gallagher, “Building Confidence in the Cybersphere.”

³³ Hitchens and Gallagher, “Building Confidence in the Cybersphere.”

³⁴ Pawlak, “Confidence-Building Measures in Cyberspace.”

Согласно Пражским предложениям 2019 г., оценка риска должна охватывать потенциальные угрозы технического и нетехнического характера, исходящие от поставщика. Нужно учитывать такие моменты, как правовое поле страны происхождения, форма правления, сотрудничество в области безопасности.³⁵ Хартия доверия (Charter of Trust, CoT) – консорциум технологических компаний, выступающий за обязательные правила и стандарты – предлагает интересный подход для укрепления доверия между поставщиками ИКТ. Он основан на управлении цепочками поставок и содержит очень важное для этой статьи заявление: «Партнёры по CoT также считают, что никакие незадокументированные функции или возможности удаленного подключения не должны входить в первоначальные настройки устройства, хотя сегодня это еще не является общим правилом».³⁶ Он признаёт, что не только компании, но и правительства могут оказаться в ситуации, когда присутствующие ИКТ риски требуют создания правил идентификации и управления доступом.³⁷

Появилась тенденция привлекать к регулированию киберпространства зарубежных участников, но включение негосударственных субъектов пока что ограничивается советом и обратной связью. Идея сделать частный сектор партнёром государства при соблюдении мер кибердоверия означает новый подход, о котором совсем недавно упоминалось в отчете Глобальной комиссии по стабильности киберпространства (Global Commission on the Stability of Cyberspace, GCSC), в виде норм киберпространства для государственных и негосударственных субъектов.³⁸

Как указано в предыдущем разделе, развитию бизнеса Huawei с рядом стран мешает глубокое недоверие. Позиция Huawei по кибербезопасности показывает, что компания ясно осознаёт это, поскольку целая глава там посвящена «независимости бизнеса». Компания даже заявила о готовности подписать соглашение «об отказе от шпионажа» и скорее закрыться, чем посягнуть на конфиденциальность и безопасность клиентов.³⁹ Но эта декларация вряд ли убедит критиков, поскольку это – рекламное заявление, не способное серьезно укрепить доверие, что сделать очень трудно, когда оно

³⁵ “The Prague Proposals: The Chairman Statement on Cyber Security.”

³⁶ “Charter of Trust Partners Decide on Further Measures for More Cybersecurity,” *Charter of Trust*, February 14, 2020, по состоянию на 27 марта 2020, <https://www.charteroftrust.com/news/charter-of-trust-partners-decide-on-further-measures-for-more-cybersecurity>.

³⁷ “Our 10 Principles: Cybersecurity Concerns Us All,” *Charter of Trust*, по состоянию на 27 марта 2020, <https://www.charteroftrust.com/about>.

³⁸ Global Commission on the Stability of Cyberspace, *Advancing Cyberstability*, Final Report (Global Commission on the Stability of Cyberspace, November 2019), по состоянию на 1 января 2020, <https://cyberstability.org/report/>.

³⁹ “Huawei’s Position Paper on Cyber Security.”

утрачено.⁴⁰ Тут срабатывает упомянутая ранее модель, основанная на предложении. Поскольку новые технологии, предлагаемые Huawei, считаются рискованными, стороны, в частности, заинтересованные страны, должны выработать меры кибердоверия, чтобы устранить риск.

Теперь рассмотрим Центр оценки кибербезопасности (Cyber Security Evaluation Center, HCSEC) Huawei, где тестируют оборудование Huawei и выявляют риски в программном и аппаратном обеспечении, в качестве фундамента для более сложных мер. HCSEC был создан в 2010 г. и укомплектован Huawei, а британский Национальный центр кибербезопасности (National Cyber Security Centre, NCSC) выступал прямым партнёром компании. Наблюдательный совет HCSEC возглавляет глава NCSC, а в его состав входят руководитель Huawei, ряд представителей британского правительства и эксперты частного сектора. Наблюдательный совет с 2014 г. выпускает годовые отчёты, включая аудит, чтобы показать свою независимость от штаб-квартиры Huawei.⁴¹ Цель HCSEC – «показать рост технических возможностей Huawei» и программного обеспечения, но другая его цель – «и далее предоставлять гарантии британскому правительству, обеспечивая открытость, прозрачность и реагирование на вопросы безопасности, возникающие у правительства и британских клиентов»,⁴² что соответствует концепции мер кибердоверия. Но анализ технических возможностей сам по себе не устраняет корень проблемы.

В случае Huawei Центр должен решить вопросы реального владения, независимости от влияния КПК и Закона о разведке 2017 г. Эти вопросы связаны со страной происхождения Huawei, что тоже соответствует оценкам риска, изложенным в Пражских предложениях. Хотя HCSEC сообщал об отсутствии свидетельств причастности китайского государства к выявленным техническим недостаткам, это не убедило критиков. Если кто-то считает, что Huawei сотрудничает с КПК и китайскими разведслужбами, отсутствие оборудованного технического «чёрного хода» не будет достаточным доказательством. Учитывая быстрое развитие технологий, кодекс со временем может быть изменен. Непрозрачные отношения между Huawei и китайскими разведслужбами являются серьёзным препятствием для налаживания доверия.

⁴⁰ Paul Slovic, "Perceived Risk, Trust, and Democracy," *Risk Analysis: An International Journal* 13, no. 6 (1993): 675-682, <https://doi.org/10.1111/j.1539-6924.1993.tb01329.x>.

⁴¹ Huawei Cyber Security Evaluation Centre Oversight Board, "Huawei Cyber Security Evaluation Centre (HCSEC) Oversight Board Annual Report 2020: A Report to the National Security Advisor of the United Kingdom," Part I: Summary, September 2020, по состоянию на 2 ноября 2020, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/923309/Huawei_Cyber_Security_Evaluation_Centre__HCSEC__Oversight_Board-_annual_report_2020.pdf.

⁴² Huawei Cyber Security Evaluation Centre Oversight Board, "Huawei Cyber Security Evaluation Centre (HCSEC) Oversight Board Annual Report 2020," Part II: Section I.

Политические рекомендации

В статье признаётся, что Huawei, вероятно, не согласится на меры кибердоверия, несмотря на все заявления о стремлении к прозрачности. Но суть статьи не в этом. Она предлагает скорректировать и применить модель, основанную на предложении, как главную меру при выборе страной провайдеров ИКТ. Меры кибердоверия должны укрепить доверие между странами и компаниями ИКТ и способствовать безопасности в киберпространстве, устанавливая нормы прозрачности.

Рекомендация №1: Во-первых, страны должны создать собственные независимые службы корпоративных мер кибердоверия, укомплектованные и руководимые правительственными экспертами в области ИКТ. Задачей этих органов будет проверка потенциальных поставщиков основных ИКТ для страны и оценка связанных с ними рисков. Далее они должны выработать адекватные корпоративные меры кибердоверия для устранения рисков, выявленных в каждой компании. ИКТ-компания, заинтересованная в ведении бизнеса со страной, должна соблюдать меры доверия, чтобы стать поставщиком. Дополнительная выгода корпоративных мер кибердоверия заключается в том, что результаты анализа можно делиться с другими странами, что уменьшит избыточность для ИКТ-компаний. Страны, не способные создать собственную службу, могут брать отчёты о корпоративных мерах кибердоверия других стран за основу для своих контрактов по ИКТ. Или же несколько стран могут объединить ресурсы и создать службы корпоративных мер кибердоверия на региональном уровне. При этом они должны синхронизировать свои будущие стандарты прозрачности и выработать общие условия ведения бизнеса с частными компаниями.

В случае Huawei служба корпоративных мер кибердоверия могла бы выявлять описанные выше риски и разрабатывать меры для их устранения. Один из возможных подходов – условие, чтобы Huawei внедрил меры прозрачности аналогично его европейским конкурентам, Ericsson и Nokia. Как указано в недавнем докладе Strand, эти конкуренты превосходят Huawei по финансовой и технической прозрачности,⁴³ включая прозрачность использования стороннего кода, что является ещё одной проблемой безопасности базовой программной платформы Huawei, которую чертовски трудно проверить.⁴⁴ Ещё одной корпоративной мерой кибердоверия могла бы быть концепция создания национального подразделения Huawei, как целиком отдельного субъекта хозяйствования, которым совместно владеют Huawei и отечественная частная или государственная компания, с серверами внутри страны.

⁴³ “The Real Cost to Rip and Replace of Chinese Equipment in Telecom Networks.”

⁴⁴ Jiwon Seo and Monica S. Lam, “InvisiType: Object-Oriented Security Policies” (Stanford University, Computer Systems Laboratory, 2010), p. 1, по состоянию на 7 декабря 2020, <https://suif.stanford.edu/papers/ndss10.pdf>.

Рекомендация №2: Странам надо предложить это новое расширенное определение мер кибердоверия международным и региональным организациям для признания негосударственных субъектов активными партнерами стран, на которые распространяются меры кибердоверия. Международная организация, например, ООН, может не воспринимать негосударственные субъекты как равных партнёров национальных государств, но такие региональные организации, как ОБСЕ и Организация Американских Государств, должны быть более благосклонны к негосударственным субъектам, поскольку многие механизмы доверия создавались на региональном уровне.

Если такие организации начнут соглашаться с этим расширенным определением мер кибердоверия, это добавит концепции легитимности, мотивируя частные компании приспособляться к корпоративным мерам кибердоверия и готовиться, прежде чем предлагать странам вести с ними бизнес. По мере приближения 4-й промышленной революции будет расти зависимость от частного сектора при развитии ИИ, наблюдения, биотехнологий и квантовых исчислений. Эти новые технологии создадут новые вызовы и риски, которые еще предстоит определить и осмыслить. Поскольку многие из этих технологий имеют двойное (военное и гражданское) применение, тем более важно укреплять доверие между странами и частными компаниями, разрабатывающими эти технологии.

Примечание

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

Об авторе

Маттиас Клаус – аналитик в области международной безопасности и рисков. Был командиром отделения, взвода и инструктором Бундесвера, затем поступил на обучение по магистерской программе в области международной безопасности, совместно организованной Центром им. Джорджа Маршалла и Университетом Бундесвера в Мюнхене.
Электронная почта: mk2124@cam.ac.uk



Руослахти, Кобёрн, Трент, & Тиканмяки,
Connections QJ 20, № 2 (2021): 33-46

<https://doi.org/10.11610/Connections.rus.20.2.04>

Рецензированная статья

Пробелы в кибернавыках – системный обзор научной литературы

*Гарри Руослахти*¹, *Джанель Кобёрн*¹, *Амир Трент*¹,
Илкка Тиканмяки^{1,2}

¹ *Программа безопасности и учёта рисков, Университет прикладных наук Лауреа, Эспоо, Финляндия, <http://www.laurea.fi/en>*

² *Кафедра военной службы, Университет национальной обороны, Хельсинки, Финляндия, <https://maanpuolustuskorkeakoulu.fi/en>*

Аннотация: Этот обзор литературы является частью исследования роли электронных навыков и обучения им в современном обществе, а именно роли кибернавыков. В статье показано, как научная литература рассматривает кибернавыки и определяет электронные навыки, которые можно считать необходимыми для деятельности нынешнего общества. Во вступлении поясняется общее значение кибернавыков в нашем современном обществе. Далее описан метод анализа и кратко изложены ответы на вопросы наших исследований. Наконец, в заключении на основе результатов исследований рассматриваются достижимость, последствия, сильные и слабые стороны, а также возможные этические проблемы.

Ключевые слова: общество, кибербезопасность, киберобучение, электронное обучение, кибернавыки.

Вступление

Применение компьютеров и других цифровых технологий – повседневная реальность больше чем для половины населения планеты, особенно в современной Европе. Из примерно 7,8 млрд. обитателей планеты на март

2020 г.¹ примерно 59% пользуются Интернетом, и в 2019 г. 49% этих пользователей имели дома компьютеры.²

Глядя на эти цифры, логично предположить, что комплекс электронных навыков стал необходимым условием жизни в обществе. Поэтому цель этого обзора литературы – понять связь кибернавыков с электронными навыками и выявить пробелы и кибернавыки, способные заполнить эти пробелы, по данным научной литературы.

Проект ЕСНО³ (Европейская сеть центров кибербезопасности и хабов компетенции для инноваций и работы, European Network of Cybersecurity Centres and Competence Hub for Innovation and Operations), начатый в 2019 г., направлен на упреждающее повышение кибербезопасности в Европейском Союзе благодаря сетевому подходу и действенному сотрудничеству разных секторов. Исследование расширяет собранный в рамках проекта массив знаний, показывая, как обучение кибернавыкам рассматривается в научной литературе, как они соотносятся с более широкими электронными навыками и как такое обучение может помочь выработать практические меры по определению и обучению специальным кибернавыкам в рамках более общих электронных навыков. Планируя это исследование, мы рассматривали электронные навыки как навыки, необходимые для работы в нынешнем цифровом мире, т.е. физической работы с компьютерами и цифровыми устройствами и эффективного использования программ, приложений и цифровой информации.

Система кибернавыков, выработанная в рамках проекта ЕСНО, определяет подход к описанию требований к кибернавыкам для разработки учебных программ, чтобы вооружить специалистов по кибербезопасности необходимыми знаниями для решения выявленных отраслевых, общих и межотраслевых проблем кибербезопасности.⁴ Кроме того, определение конкретных навыков кибербезопасности и соответствующих программ обучения персонала всех уровней может восполнить недостаток знаний, ограничивающий реагирование на атаки. Как отмечено в исследовании ЕСНО, киберпрограммы и кибернавыки помогут системе здравоохранения и другим

¹ Joseph Chamie, "World Population 2020: Overview," *Yale Global Online*, February 11, 2020, по состоянию на 12 апреля 2020, <https://yaleglobal.yale.edu/content/world-population-2020-overview>.

² Statista, "Share of Households with a Computer at Home Worldwide from 2005 to 2019," March 2, 2020, по состоянию на 11 апреля 2020, <https://www.statista.com/statistics/748551/worldwide-households-with-computer>.

³ European Commission, "European network of Cybersecurity centres and competence Hub for innovation and Operations (ECHO)," Grant Agreement Number: 830943 – ECHO – H2020-SU-ICT-2018-2020/H2020-SU-ICT-2018-2 (2019).

⁴ European Commission, "European network of Cybersecurity centres and competence Hub for innovation and Operations (ECHO)," Deliverable 2.2 ECHO Multi-sector Assessment Framework, November 13, 2019, p. 121.

секторам сделать важный шаг к совершенно новому уровню кибербезопасности.⁵

Согласно Чейми,⁶ современное общество развилось в технологический мир благодаря появлению Интернета. Интернет изменил все аспекты жизни общества, от ведения бизнеса (превратив традиционные компании в цифровые) до средств обучения (например, при помощи платформ электронного обучения) и взаимодействия между людьми (в соцсетях). С развитием инструментов информационно-коммуникационных технологий (ИКТ), например, ручных мобильных устройств, обеспечивающих постоянный и мгновенный доступ в Интернет, люди больше, чем когда-либо, связаны с ИКТ. ИКТ – неотъемлемый элемент нашей повседневной жизни. Кроме многочисленных выгод использования Интернета и других ИК технологий, к сожалению, есть и угрозы, например, от хакеров, которые пытаются воспользоваться уязвимостью этих ИКТ в преступных целях. Чтобы понять важность развития кибернавыков, в этом обзоре литературы основное внимание уделено киберобучению и развитию кибернавыков в соответствующих статьях. Цель данного исследования – расширить имеющиеся знания об обучении ИКТ. Для упорядочения, в данном исследовании ставились такие вопросы:

Вопрос 1: Как научная литература описывает пробелы в кибернавыках?

Вопрос 2: Какие меры предлагаются в научной литературе для восполнения этих пробелов?

Методы

Главный метод данного исследования – системный обзор литературы. Это качественное исследование, и главная задача этого системного обзора современной литературы – выявить пробелы в знаниях о кибернавыках современного общества с целью прояснения выработки электронных навыков для дальнейших исследований.⁷

Построение качественного исследования

Согласно Китченхэму,⁸ системный обзор литературы – кропотливый процесс, который может помочь представить свидетельства последствий неких событий, описанных в исследовании, которые не могут передать традиционные несистемные обзоры литературы. Системные обзоры литературы могут быть шире обычных. Для выполнения обзора литературы проводился

⁵ European Commission, “European network of Cybersecurity centres and competence Hub for innovation and Operations (ECHO),” Deliverable 2.2 ECHO Multi-sector Assessment Framework, November 13, 2019, p. 64.

⁶ Chamie, “World Population 2020.”

⁷ Barbara Kitchenham, “Procedures for Performing Systematic Reviews,” Joint Technical Report TR/SE-0401 (Keele, UK: Keele University, 2004): 1-26, <https://www.inf.ufsc.br/~aldo.vw/kitchenham.pdf>.

⁸ Kitchenham, “Procedures for Performing Systematic Reviews.”

научный поиск, чтобы найти ответы на вопросы исследования. Исследование проходило в четыре этапа: поиск, критерии отбора, анализ табличных данных, и написание выводов и заключения.

Поиск

Поиск статей выполнялся в марте 2020 г. Поиск производился по научным базам данных ProQuest Central и EBSCO Host. В качестве параметров поиска при логическом поиске по ключевым словам использовали словосочетания «обучение кибербезопасности» и «обучение электронным навыкам». Период для поиска охватывал литературу, вышедшую за 10 лет, в 2010-2020 гг.

Поиск в базе данных ProQuest Central выдал всего 67 рецензированных статей, а в базе данных EBSCO Host – ещё две рецензированных статьи. Окончательная выборка отбиралась для анализа, применяя критерии включения к 67 статьям из первоначального поиска по ключевым словам. К оригинальным 69 документам применялись следующие критерии включения: название или аннотация включали темы, связанные с кибер- (электронными) навыками обучения работников и кибер- (электронными) навыками обучения студентов. Применение критериев включения дало окончательную выборку в составе 21 рецензированной статьи (Таблица 1), которые были внимательно прочитаны для анализа.

Таблица 1. Этапы поиска и полученное число научных статей.

Этапы поиска	Статей в выборке
Результаты первоначального поиска в ProQuest Central и EBSCO Host	69
После применения критериев включения	21

Анализ окончательной выборки проводился путём переноса релевантных фрагментов информации в таблицу данных на основе вопросов исследования. В следующем разделе рассмотрены выводы из выборки, включавшей 21 статью.

Выводы

Внимание к кибернавыкам

Результаты показывают, что кибербезопасность представляет существенную проблему в современном обществе. С развитием новых технологий и сетевых возможностей для критической инфраструктуры и повседневной деятельности киберустройства становятся уязвимыми для кибератак, от кражи личных данных до кибершантажа, и эти атаки могут существенно влиять на финансовые, экономические и социальные системы. Большое число статей, не соответствующих критериям включения, указывает на то, что многие авторы рассматривают кибербезопасность в основном с позиций технологии или рисков.

Статьи, включённые в окончательную выборку, показывают, что большинство людей, имеющих доступ к ИКТ-устройствам, подвергаются риску. Это люди, которые слабо знакомы с кибербезопасностью или не применяют надлежащие меры кибербезопасности. Проблемы кибербезопасности различаются в зависимости от возраста. Молодёжь более подвержена кибератакам, по ряду причин: неприменение мер безопасности, излишнее доверие к защите своих персональных устройств, незнание новых технологий соцсетей, активные покупки в интернете. Разглашение личной информации в соцсетях или на сайтах, к которым имеют доступ третьи лица, тоже повышает риск для кибербезопасности.

В целом стоит отметить, что электронные навыки упоминаются намного реже, чем кибернавыки. Навыки кибербезопасности на рабочем месте и в профессиональной деятельности – главная тема обсуждения. 17 из 21 рецензированной статьи касаются навыков кибербезопасности, обучения кибербезопасности и безопасности информации (сетей). Поиск термина «электронные навыки» дал всего один результат, три другие статьи были найдены по ключевому слову «электронное обучение». Исходя из этого, один из первых выводов обзора литературы состоит в том, что научные публикации намного чаще касаются нынешних угроз кибербезопасности, недостаточности киберподготовки и квалификации для противодействия современным киберугрозам и новых методов обучения противодействию угрозам кибербезопасности.

Анализ содержания 21 статьи первоисточников об электронных и кибернавыках позволил выявить четыре крупные тематические категории.

1. Общая кибербезопасность: 8 статей касаются необходимости и практики обучения кибербезопасности, информированности и грамотности.
2. Обучение кибербезопасности: в 7 статьях речь идёт о необходимости киберобразования в числе учебных программ, рекомендуются методы обучения кибербезопасности и показаны отличия между киберобразованием и киберобучением. Среди подкатегорий обучения кибербезопасности появились кибер-полигоны и упражнения. В этих статьях описаны такие полигоны и упражнения, как механизмы обучения и то, как они работают.
3. Электронное обучение: 5 статей дают определение электронного обучения, описывают препятствия для электронного обучения, необходимость навыков ИКТ для завершения электронного обучения и эффективные и конкретные практические подходы к успешному электронному обучению.
4. Электронные навыки: только в одной статье из первоначальной выборки речь идёт о необходимости повышать навыки ИКТ в ЕС, почему эти электронные навыки нужны в повседневной работе и личной жизни, и как это влияет на экономику ЕС и всего мира.

В 8 из 21 статей упоминаются навыки, нужные для профессиональной работы или повседневной жизни, либо навыки кибербезопасности, необходимые для предотвращения успешных действий хакеров. В одной статье о специализированных электронных навыках предложены категории, в зависимости от уровня электронных навыков, нужных в повседневной работе. По Сингху,⁹ это функциональные категории навыков ИКТ-практиков, ИКТ-пользователей и электронного бизнеса.

Общая кибербезопасность

В Таблице 2 ниже приводится обзор восьми статей об обучении общей кибербезопасности и их темы.

Таблица 2. Статьи об общей кибербезопасности.

Статья	Тема
Ricci et al. (2019) ¹⁰	Результаты исследования среди взрослых и обучение кибербезопасности
Clifton (2018) ¹¹	Повышение информированности о кибербезопасности в хосписах
Ghafir et al. (2018) ¹²	Угрозы безопасности для критической инфраструктуры: человеческий фактор
Russell and Jackson (2018) ¹³	Действия в темноте: основы принятия киберрешений
Zăgan et al. (2018) ¹⁴	Морские реалии концепции кибербезопасности

⁹ Sumanjeet Singh, "Developing e-Skills for Competitiveness, Growth and Employment in the 21st Century: The European Perspective," *International Journal of Development Issues* (Emerald Group Publishing) 11, no. 1 (2012): 37-59, <https://ideas.repec.org/a/eme/ijdipp/v11y2012i1p37-59.html>.

¹⁰ Joseph Ricci, Frank Breitinger, and Ibrahim Baggili, "Survey Results on Adults and Cybersecurity Education," *Education and Information Technologies* 24 (2019): 231–249, <https://doi.org/10.1007/s10639-018-9765-8>.

¹¹ Tim Clifton, "P-236: Increasing Cyber Security Awareness in the Hospice Environment," *BMJ Supportive & Palliative Care* 8, no. 2 (2018): A94, <https://dx.doi.org/10.1136/bmjspcare-2018-hospiceabs.261>.

¹² Ibrahim Ghafir et al., "Security Threats to Critical Infrastructure: The Human Factor," *The Journal of Supercomputing* 74 (2018): 4986-5002, <https://doi.org/10.1007/s11227-018-2337-2>.

¹³ Scott Russell and Craig Jackson, "Operating in the Dark: Cyber Decision-Making from First Principles," *Journal of Information Warfare* 17, no.1 (2018): 1-15, https://cacr.iu.edu/files/documents/Operating_in_the_dark.pdf.

¹⁴ Remus Zăgan, Gabriel Raicu, Radu Hanzu-Pazara, and Stănică Enache, "Realities in Maritime Domain Regarding Cyber Security Concept," *Advanced Engineering Forum* 27 (April 2018): 221-228, <https://doi.org/10.4028/www.scientific.net/AEF.27.221>.

Nikolova (2017) ¹⁵	Лучшие практики развития потенциала кибербезопасности в государственном секторе Болгарии
Choi and Lee (2015) ¹⁶	Исследование развития программ информирования о безопасности на основе системы контроля доступа RFID для предотвращения утечек внутренней информации
Rahim et al. (2015) ¹⁷	Системное исследование подходов к оценке знаний о кибербезопасности

Согласно Рахиму и др.,¹⁸ взрослые могут вести себя неосмотрительно в интернете, например, открывая личную почту в Wi-Fi сетях общего доступа, переходя по незнакомым ссылкам или используя один и тот же пароль для разных электронных счетов. Кроме того, пожилые люди обычно не так хорошо разбираются в кибербезопасности, как молодёжь, и более доверчивы, что можно использовать для фишинга и манипуляций, используя их незащищённость.

Обучение кибербезопасности

В Таблице 3 ниже перечислены 7 документов, попавших в окончательную выборку, и их отношение к обучению кибербезопасности.

Результаты показывают, что кибербезопасность в большинстве случаев подрывают человеческие ошибки и слабые знания и навыки кибербезопасности. Поскольку кибербезопасность становится насущной проблемой в современном обществе, затрагивая бизнес, личную жизнь и критическую инфраструктуру, растёт потребность в квалифицированном, обученном кибербезопасности персонале для защиты этих систем.

¹⁵ Irena Nikolova, “Best Practice for Cybersecurity Capacity Building in Bulgaria’s Public Sector,” *Information & Security: An International Journal* 38 (2017): 79-92, <https://doi.org/10.11610/isij.3806>.

¹⁶ Kyong-Ho Choi and Donghwi Lee, “A Study on Strengthening Security Awareness Programs based on an RFID Access Control System for Inside Information Leakage Prevention,” *Multimedia Tools and Applications* 74, no. 20 (2015): 8927–8937, <https://doi.org/10.1007/s11042-013-1727-y>.

¹⁷ Noor Hayani Abd Rahim et al., “A Systematic Review of Approaches to Assessing Cybersecurity Awareness,” *Kybernetes* 44, no. 4 (2015): 606-622, <https://doi.org/10.1108/K-12-2014-0283>.

¹⁸ Rahim et al., “A Systematic Review of Approaches.”

Таблица 3. Статьи, касающиеся обучения кибербезопасности.

Статья	Тема
Yamin et al. (2020) ¹⁹	Киберполигоны и испытательные стенды безопасности: сценарии, функции, инструменты и архитектура
Aaltola and Taitto (2019) ²⁰	Использование экспериментальных и организационных теорий обучения для улучшения показателей человека при киберобучении
Beuran et al. (2019) ²¹	Обеспечение обучения кибербезопасности путём интеграции систем организации обучения: система организации киберобучения
Raineri and Fudge (2019) ²²	Изучение достаточности знаний студентов по кибербезопасности в рамках программ предпринимательства ведущих университетов
Chapman et al. (2017) ²³	Можно ли симитировать атаку на сеть в моделируемой среде для обучения сетевой безопасности?
Adams and Makramalla (2015) ²⁴	Навыки обучения кибербезопасности: хакероцентричный игровой подход
Lester (2010) ²⁵	Практическое применение программ безопасности при обучении разработке программного обеспечения

¹⁹ Muhammad Mudassar Yamin, Basel Katt, and Vasileios Gkioulos, "Cyber Ranges and Security Testbeds: Scenarios, Functions, Tools and Architecture," *Computers and Security* 88 (January 2020), 101636, <https://doi.org/10.1016/j.cose.2019.101636>.

²⁰ Kirsi Aaltola and Petteri Taitto, "Utilising Experiential and Organizational Learning Theories to Improve Human Performance in Cyber Training," *Information & Security: An International Journal* 43, no. 2 (2019): 123-133. <https://doi.org/10.11610/isij.4311>.

²¹ Razvan Beuran et al., "Supporting Cybersecurity Education and Training via LMS Integration: CyLMS," *Education and Information Technologies* 24 (2019): 3619-3643, <https://doi.org/10.1007/s10639-019-09942-y>.

²² Ellen M. Raineri and Tamara Fudge, "Exploring the Sufficiency of Undergraduate Students' Cybersecurity Knowledge Within Top Universities' Entrepreneurship Programs," *Journal of Higher Education Theory and Practice* 19, no. 4 (2019): 73-92, <https://doi.org/10.33423/jhetp.v19i4.2203>.

²³ Samuel Chapman et al., "Can a Network Attack Be Simulated in an Emulated Environment for Network Security Training?" *Journal of Sensor and Actuator Networks* 6, no. 16 (2017), <https://doi.org/10.3390/jsan6030016>.

²⁴ Mackenzie Adams and Maged Makramalla, "Cybersecurity Skills Training: An Attacker-Centric Gamified Approach," *Technology Innovation Management Review* 5, no. 1 (January 2015): 5-14, <http://doi.org/10.22215/timreview/861>.

²⁵ Cynthia Y. Lester, "A Practical Application of Software Security in an Undergraduate Software Engineering Course," *International Journal of Computer Science Issues* 7, no. 3 (May 2010): 1-9.

Топхэм с коллегами²⁶ утверждает, что организации, готовящиеся к адекватному отражению угроз, способных нарушить их безопасность и деятельность, должны защищать все критические элементы своей инфраструктуры. Фундамент начинается с пользователей, которые, как показывают результаты, часто оказываются слабым звеном из-за необученности понятию киберугроз и отсутствия опыта снижения возможных киберугроз. Манипуляции и фишинг – самые распространённые атаки, с которыми обычно сталкиваются конечные пользователи. Без специального обучения кибербезопасности эти пользователи с трудом отличают обычный запрос от кибератаки. В результате они могут неумышленно подставить сеть своей компании под удар злоумышленников. Результатом является рекомендация вкладываться в программы информирования о кибербезопасности и киберобучения для противодействия киберугрозам. Гафир и др.²⁷ видят задачу внедрения обучения кибербезопасности в организациях в том, как правильно организовать обучение, которое реально научит персонал (неспециалистов в ИКТ) применять меры безопасности и развивать свои кибернавыки. Задача специалистов в ИКТ – повышать свою квалификацию для анализа и противодействия постоянно меняющимся киберугрозам.

Адамс и Макрамалла²⁸ отмечают, что главное препятствие, мешающее персоналу научиться применению мер безопасности и выработать навыки кибербезопасности, возникает из-за преподавания в рамках программ обучения кибербезопасности. Большинство этих программ учат безопасности традиционно, информация бывает сложно усвоить и применить на практике. Дополнение теоретических знаний сотрудников общего профиля экспериментами и интерактивным обучением (игры, задачи, сценарии) может дать более практичную подготовку с фокусом на реальные угрозы (например, на киберполигонах). Программы обучения кибербезопасности, реализуемые собственными ИКТ-специалистами организаций, могут действительно оптимизировать развитие навыков кибербезопасности и понимание угроз у сотрудников для умелой защиты себя и своей организации от атак.

По мнению Топхэма и др.,²⁹ практическое обучение при помощи упражнений в сети и интерактивных киберлабораторий может помочь развить соответствующие кибернавыки студентам, изучающим кибербезопасность в ВУЗах. В результате они будут затребованы компаниями при приёме на работу в качестве компьютерно грамотных сотрудников и даже будущих кибер-специалистов, способных справиться с нынешними и будущими киберугрозами с развитием ИК технологий.

²⁶ Luke Topham et al., “Cyber Security Teaching and Learning Laboratories: A Survey,” *Information & Security: An International Journal* 35, no.1 (2016.): 51-80, <https://doi.org/10.11610/isij.3503>.

²⁷ Ghafir et al., “Security Threats to Critical Infrastructure.”

²⁸ Adams and Makramalla, “Cybersecurity Skills Training.”

²⁹ Topham et al., “Cyber Security Teaching and Learning Laboratories.”

Электронное обучение

В Таблице 4 ниже представлен обзор пяти документов, касающихся электронного обучения. Электронное обучение считается ценным активом для инвестирования организаций с целью достижения оптимальных деловых и личных результатов во всей своей деятельности, зависящей от ИКТ. Оно предусматривает разработку программ электронного обучения, развивающих электронные навыки и дающих образование, нужное для эффективного использования современных ИКТ-устройств, сетей и систем.

Таблица 4. Статьи, касающиеся электронного обучения.

Статья	Тема
Iqbal (2016) ³⁰	Разработка и появление педагогической онлайн-лаборатории информационной безопасности как целостного артефакта
Topham et al. (2016) ³¹	Обучение кибербезопасности и учебные лаборатории: исследование
Hagen et al. (2011) ³²	Долгосрочные результаты электронного обучения информационной безопасности для обучения в организации
Annansingh and Bright (2010) ³³	Изучение препятствий для эффективного электронного обучения: Пример DNPA
Anonymous (2010) ³⁴	Электронное обучение в Администрации национального парка Дартмур: Как свести к минимуму процент отсева и невосприятие будущих программ обучения

³⁰ Sarfraz Iqbal, "Design and Emergence of a Pedagogical Online InfoSec Laboratory as an Ensemble Artefact," *Journal of Information Systems Education* 27, no. 1 (2016.): 17-35, <https://aisel.aisnet.org/jise/vol27/iss1/2>.

³¹ Topham et al., "Cyber Security Teaching and Learning Laboratories."

³² Janne Hagen, Eirik Albrechtsen, and Stig Ole Johnsen, "The Long-term Effects of Information Security e-Learning on Organizational Learning," *Information Management & Computer Security* 19, no. 3 (2011): 140-154, <https://doi.org/10.1108/09685221111153537>.

³³ Fenio Annansingh and Ali Bright, "Exploring Barriers to Effective e-Learning: Case Study of DNPA," *Interactive Technology and Smart Education* 7, no. 1 (2010): 55-65, <https://doi.org/10.1108/17415651011031653>.

³⁴ Anonymous, "E-learning at Dartmoor National Park Authority: How to Minimize Dropout Rates and Resistance to Future Training Programs," *Development and Learning in Organizations* 24, no. 6 (2010): 20-22, <https://doi.org/10.1108/14777281011084720>.

Один из самых популярных методов электронного обучения, которые упоминают Аннансингх и Брайт³⁵ – сетевое электронное обучение, при котором ресурсы распределяются на сетевых платформах и доступны на любом компьютере, подключённом к Интернету. Выгоды сетевого электронного обучения включают дистанционность, возможность работать на курсах в любом месте и в любое время, возможность интерактивного обучения, например, при помощи практичных приложений с ситуативными примерами, в отличие от обучения учителем посредством лекций для понимания безопасности, и возможность повторения предыдущих курсов для закрепления понимания. Наконец, знания, полученные при сетевом электронном обучении, запоминаются лучше, чем при традиционном обучении.

При всех преимуществах электронного обучения, проблемой является то, что электронное обучение требует серьёзных навыков ИКТ. Сотрудники с ограниченными навыками ИКТ могут не усвоить информацию так, как те, кто имеет опыт и навыки ИКТ. Среди препятствий отмечаются недостаток времени для электронного обучения, сопротивление изменению привычного обучения (обучение с учителем по сравнению с онлайн-обучением) и поддержание дисциплины при обучении на длительных курсах электронного обучения. Все эти причины могут привести к отсеву с увеличением продолжительности курсов. Негативный опыт курсов электронного обучения тоже может помешать успеху.

Для успешного проведения курсов электронного обучения Аннансингх и Брайт³⁶ рекомендуют учитывать возможности слушателя электронных курсов. Успех программ электронного обучения, с одной стороны, зависит от того, как проводится курс, а с другой – от слушателя. Слабость слушателя может помешать участию сотрудника или успеху электронного обучения. Результаты показывают, что стимулирование (например, продвижение по службе или повышение зарплаты) может сильнее побудить сотрудников заниматься электронным обучением.

Электронные навыки

Как видно из Таблицы 5 ниже, в окончательную выборку попала лишь одна статья, в которой рассмотрен термин «электронные навыки».

Таблица 5. Статьи, касающиеся электронных навыков.

Статья	Тема
Singh (2012) ³⁷	Развитие электронных навыков для конкуренции, роста и работы в XXI веке

³⁵ Annansingh and Bright, “Exploring Barriers to Effective e-Learning.”

³⁶ Annansingh and Bright, “Exploring Barriers to Effective e-Learning.”

³⁷ Singh, “Developing e-Skills for Competitiveness.”

Согласно Синху,³⁸ мир становится всё более ИКТ-ориентированным, и развитие общих навыков ИКТ (электронных навыков) просто необходимо. В связи с широким влиянием ИКТ на общественную и личную жизнь, электронные навыки в современном обществе важны. Инвестирование в ИКТ / электронные навыки может дать множество преимуществ, кибернавыки дают знания и возможности для защиты от киберугроз.

Заключение

В научной литературе в основном обсуждают текущие вопросы кибербезопасности: киберугрозы, киберобучение и квалификацию. Предлагается путём исследований определить, какие электронные навыки, кроме необходимых навыков кибербезопасности, нужны для успеха в современном обществе. Исследование позволило выделить четыре главные категории электронных навыков. Как видно из Таблицы 6, эти категории помогают понять роли кибер- и электронных навыков в современном обществе. Становится очевидным, что пользователи, будь то обычные граждане, работники или ИКТ/киберспециалисты, потенциально являются слабым звеном в кибервопросах. Поэтому нужны кибернавыки для защиты людей, организаций и общества от деструктивных киберинцидентов и злонамеренных кибератак.

Программы обучения кибербезопасности для всех аудиторий с разными электронными навыками и киберзнаниями могут помочь выработать культуру кибербезопасности с надлежащим поведением и установкой на защиту в Интернете. Такую платформу информирования о безопасности могут дополнять методы обучения, чётко проясняющие вопросы кибербезопасности и киберугроз для лучшего понимания кибератак. Применяя эти контрмеры кибербезопасности, люди будут легче воспринимать информацию о кибербезопасности и охотнее принимать меры безопасности в Интернете, что будет способствовать безопасному поведению в киберпространстве и окажет положительное влияние на общество.

Если пользователям сложно отличить обычный запрос от возможной кибератаки, это говорит о пробеле в обучении кибербезопасности. Поэтому инвестирование в программы обучения кибербезопасности и киберобучение противодействию киберугрозам должно быть приоритетом организаций.

Поскольку ИКТ стали важным фактором глобальной конкурентоспособности, роста и инноваций в Европе, необходимо инвестировать в обучение электронным навыкам и кибербезопасности для повышения устойчивости общественных, экономических и промышленных систем. Правительства и научные учреждения могли бы помочь различным организациям решить проблему низкой ИКТ-компетентности сотрудников, помогая организации

³⁸ Singh, "Developing e-Skills for Competitiveness."

курсов обучения кибернавыкам и обучению электронным навыкам, что поможет стабильному росту и инновациям европейских экономик благодаря развитию ИКТ.

Таблица 6. Главные выводы.

Категория	Главные выводы
Общая кибербезопасность	<ul style="list-style-type: none">• киберустройства уязвимы для кибератак• люди либо не знают о кибербезопасности, либо не принимают мер кибербезопасности
Обучение кибербезопасности	<ul style="list-style-type: none">• конечные пользователи часто являются самым слабым звеном• рекомендуется инвестировать в программы обучения кибербезопасности и киберобучение• может быть полезным практическое обучение с помощью имитации в сети и интерактивного обучения в киберлабораториях
Электронное обучение	<ul style="list-style-type: none">• электронное обучение – важный актив для инвестирования организаций• выгоды сетевого электронного обучения: удалённый доступ, работа в любом месте/в любое время, возможность интерактивного обучения
Электронные навыки	<ul style="list-style-type: none">• современное общество постепенно становится более технологичным• обучение электронным навыкам стало необходимостью• электронные навыки нужны как бизнесменам, так и обычным пользователям• выгоды развития электронных навыков велики и на личном уровне

Кроме того, чтобы внедрить эффективные программы кибербезопасности и электронных навыков, преподаватели должны устранить причины, мешающие пользователям инвестировать в эти программы. Преподаватели могут адаптировать свои педагогические методы и системы таким образом, чтобы те приносили наибольшую пользу конечным пользователям, одновременно оптимизируя совершенствование их электронных навыков. В результате учащийся получит интересный опыт этих программ и сможет использовать новые навыки для личного совершенствования, внося свой вклад в общество.

Исследование выявило общий недостаток устоявшихся терминов ИТ. Это «электронные навыки», «кибернавыки», «компьютерные навыки», «ИКТ

навыки», и все они могут иметь разные значения у разных авторов. Мы рекомендуем продолжить исследования и дать чёткое определение каждому из этих терминов.

Примечание

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

Благодарность

Данная работа была выполнена при поддержке проекта ЕСНО, финансируемого по программе исследований и инноваций Европейского Союза «Horizon 2020» согласно грантового соглашения № 830943. Финансируемые Европейской Комиссией пилотные проекты, такие, как Европейская сеть центров кибербезопасности и хабов компетенции для инноваций и работы (ЕСНО), дают исследователям возможность проводить эксперименты и собирать эмпирические данные для изучения этих вопросов с разных точек зрения.

Об авторах

Д-р Гарри Руослахти – старший преподаватель программы безопасности и учёта рисков в Университете прикладных наук Лауреа. Возглавляет группу Лауреа в проекте «Европейская сеть центров кибербезопасности и хабов компетенции для инноваций и работы» (ЕСНО) программы «Horizon 2020». Электронная почта: harri.ruoslahti@laurea.fi

Джанель Кобёрн работала экспертом по научным исследованиям и инновациям в Университете прикладных наук Лауреа, где она принимала участие в ряде научно-исследовательских проектов, включая изучение кибернавыков в рамках проекта ЕСНО.

Амир Трент – студент бакалаврата по информационным технологиям для бизнеса в Университете прикладных наук Лауреа.

Илкка Тиканмяки – научный сотрудник программы безопасности и учёта рисков в Университете прикладных наук Лауреа, докторант в области оперативного искусства и тактики Университета национальной обороны Финляндии.



Дезинформация: Политическая реакция для повышения устойчивости граждан

Инез Миямото

Азиатско-Тихоокеанский центр исследований в области безопасности имени Даниэля Иноуйе

Аннотация: Злоумышленники используют фейковые аккаунты в соцсетях и автоматизированные инструменты так называемой компьютерной пропаганды для проведения операций по дезинформации. Хотя технологические компании и исследователи совершенствуют выявление компьютерной пропаганды, они знают, что искоренить социальных ботов и дезинформацию невозможно. Поскольку компьютерная пропаганда продолжает нарастать, правительства должны обратить внимание на разработку политики, снижающей спрос граждан на дезинформацию. Цель этой статьи – исследовать дезинформацию на стыке технологий и устойчивости граждан. Во-первых, будет рассмотрена текущая картина, чтобы понять воздействие дезинформации на общество и его граждан. Во-вторых, будет проанализировано влияние технологий на появление дезинформации. В-третьих, будут рассмотрены методы снижения потребления дезинформации для повышения устойчивости граждан.

Ключевые слова: дезинформация, цифровая грамотность, устойчивость граждан.

Вступление

С развитием соцсетей в Интернете растёт поток нерегулируемого контента. Ушли социально ответственные издатели, редактора и профильные эксперты, которые оценивали информацию в традиционных СМИ.¹ Теперь

¹ Institute for the Study of Diplomacy, *The New Weapon of Choice: Technology and Information Operations Today* (Washington: Institute for the Study of Diplomacy, October 2020), <https://georgetown.app.box.com/s/ivwz4irk3un8blngm3wo0t3uwfc6hpz8>.

граждане сами решают, где правда, а где ложь, и злоумышленники пользуются моментом и открытостью демократий, чтобы влиять на общество посредством дезинформации. Дезинформация определяется как целенаправленное использование ложной информации, создаваемой и распространяемой намеренно, для замешательства или введения в заблуждение, что может содержать смесь правды и лжи или намеренное игнорирование контекста.² Правительства должны обратить внимание на разработку политики, снижающей потребление дезинформации гражданами, потому что контроль потока дезинформации – сложная задача в условиях, когда контент всё больше генерируют машины.

Правительства, общественные организации и технологические компании признают дезинформацию мировой проблемой, но не могут дать ответ на неё. Злоумышленники сеют раздор и недоверие, применяя новые, лучшие инструменты, заставляя граждан, ставших объектом дезинформации, беспокоиться о последствиях дезинформации в Интернете. Кнуутила с коллегами выяснили, что 53% обычных Интернет-пользователей (154 195 респондентов в 142 странах) озабочены дезинформацией в Интернете, больше всего (65%) – в Северной Америке.³ Дезинформация волнует их больше, чем Интернет-мошенничество или запугивание.

В этой статье дезинформация рассматривается на стыке технологий и устойчивости граждан. Во-первых, будет рассмотрена текущая картина, чтобы понять воздействие дезинформации на общество и его граждан. Во-вторых, после рассмотрения воздействия технологий на поступление дезинформации, анализируется потребление дезинформации на предмет устойчивости граждан. Заканчивается статья политическими рекомендациями начать реализацию программы устойчивости граждан.

Компьютерная пропаганда

Злоумышленники используют фейковые аккаунты в соцсетях и автоматизированные инструменты так называемой компьютерной пропаганды для проведения операций по дезинформации. Вули и Ховард (2016) определяют компьютерную пропаганду как «алгоритмы, автоматизацию и надзор человека для намеренного распространения вводящей в заблуждение ин-

² Samantha Bradshaw and Lisa-Maria Neudert, “The Road Ahead: Mapping Civil Society Responses to Disinformation,” Working Paper (Washington: National Endowment for Democracy, January 2021), <https://www.ned.org/mapping-civil-society-responses-to-disinformation-international-forum>.

³ Aleksi Knuutila, Lisa-Maria Neudert, and Philip N. Howard, “Global Fears of Disinformation: Perceived Internet and Social Media Harms in 142 Countries,” COMPROP Data Memo 2020.8, December 15, 2020, <https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/127/2020/12/Global-Fears-of-Disinformation-v.13.pdf>.

формации в соцсетях».⁴ К инструментам компьютерной пропаганды относятся, в частности, боты, клоны, робо-тролли и дипфейковые видео.

Первые, боты — сокращение от роботов — это незапрещённые компьютерные программы, например, для автоматизации задач на веб-сайтах. При операциях дезинформации сетевые боты имитируют людей в соцсети, связываясь и взаимодействуя с людьми и системами. Например, это могут быть сетевые боты — фейковые автоматизированные аккаунты, или киборги — аккаунты, используемые человеком при помощи бота. Злоумышленники также массово используют ботов в соцсетях для создания иллюзии единства при онлайн-пропаганде.⁵

Вторые, «левые» аккаунты или клоны — это фиктивные аккаунты, созданные человеком или группой людей для обмана. Например, человек или группа создаёт множество аккаунтов в соцсети для влияния на подписчиков «лайками» или голосованием в постах. Они также могут исказить или увести в сторону онлайн-дискуссию или поддержать конкретный Интернет-аккаунт. Так, русская разведка использовала левый аккаунт в Твиттере под именем Jenna Abrams с 70 000 подписчиков, чтобы влиять на консервативных избирателей на выборах в США в 2016 г.⁶

Третьи, тролли — реальные люди, которые намеренно провоцируют других в Интернете, размещая подстрекательские или оскорбительные посты. Если их аккаунты автоматизированы при помощи программ, они называются робо-тролли и могут генерировать контент.⁷ Исследователей тревожит использование робо-троллей экстремистами и террористами. Те испытывают программы искусственного интеллекта (ИИ), генерирующие тексты, которые могут использовать робо-тролли.⁸ Генерирующие текст программы (ИИ) могут быть мощным инструментом в руках экстремистов и террористов, потому что они могут быстро плодить пропаганду, которую сейчас люди создают вручную, что занимает много времени.

⁴ Samuel C. Woolley and Philip N. Howard, "Automation, Algorithms, and Politics: Political Communication, Computational Propaganda, and Autonomous Agents – Introduction," *International Journal of Communication* 10 (2016), <https://ijoc.org/index.php/ijoc/article/view/6298>.

⁵ Samuel C. Woolley and Philip N. Howard, "Computational Propaganda Worldwide: Executive Summary," Working Paper No. 2017.11 (Oxford: University of Oxford, 2017), <https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/06/Casestudies-ExecutiveSummary.pdf>.

⁶ Ben Collins and Joseph Cox, "Jenna Abrams, Russia's Clown Troll Princess, Duped the Mainstream Media and the World," *The Daily Beast*, November 3, 2017, <https://www.thedailybeast.com/jenna-abrams-russias-clown-troll-princess-duped-the-mainstream-media-and-the-world>.

⁷ Tom Simonite, "To See the Future of Disinformation, You Build Robo-Trolls: AI-Powered Software Is Getting Better and Could Soon Be Weaponized for Online Disinformation," *Wired*, November 19, 2019, <https://www.wired.com/story/to-see-the-future-of-disinformation-you-build-robo-trolls>.

⁸ Simonite, "To See the Future of Disinformation, You Build Robo-Trolls."

Четвёртые – инструменты на основе ИИ, позволяющие создавать дипфейковые видео: изменённые цифровыми методами видео для введения в заблуждение. По данным Sensity AI (ранее – DeepTrace), количество дипфейковых видео растёт. 96% дипфейковых видео в интернете – это порнография со знаменитостями без их согласия.⁹ Эксперты считают, что число и сложность этих видео будет и дальше расти с появлением новых доступных дипфейковых сервисов и инструментов.¹⁰ Уже сейчас высококачественные дипфейковые видео трудно распознать.¹¹

В ответ на рост компьютерной пропаганды технологические компании начали применять контрмеры при помощи ИИ. В то время как компании научились лучше выявлять и блокировать ботов, разработчики ботов начали использовать более продвинутые технологии, например, созданные ИИ изображения, тексты и видео.¹² Поскольку искусственно генерируемый контент имитирует стиль человека, контент ИИ сложно отличить от сгенерированного человеком.¹³ Новые сетевые боты больше похожи на аккаунты людей, потому что ИИ используют для создания «гибрида действий автомата и человека».¹⁴ Проблему усложняет то, что злоумышленники могут окутать правдивую информацию ложью, из-за чего технологическим компаниям сложно пометить информацию как достоверную или недостоверную.¹⁵ Как следствие, в будущем граждане не смогут определить достоверность информации или подлинность аккаунта.

Тем временем компьютерная пропаганда растёт во всём мире. Брэдшоу и др. отмечают, что государственные и политические деятели в 81 стране используют соцсети для распространения компьютерной пропаганды.¹⁶ Такой рост представляет проблему, поскольку компьютерная

⁹ Henry Ajder, Giorgio Patrini, Francesco Cavalli, and Laurence Cullen, *The State of Deepfakes: Landscape, Threats and Impact* (Amsterdam: Deeptrace, 2019), <https://sensity.ai/reports/>.

¹⁰ Ajder, Patrini, Cavalli, and Cullen, *The State of Deepfakes*.

¹¹ Matt Groh, “DetectDeepFakes: How to Counteract Misinformation Created by AI,” по состоянию на 28 января 2021, www.media.mit.edu/projects/detect-fakes/overview.

¹² Stefano Cresci, “A Decade of Social Bot Detection,” *Communications of the ACM* 63, no. 10 (October 2020): 72-83, <https://doi.org/10.1145/3409116>.

¹³ Renée DiResta, “The Supply of Disinformation Will Soon Be Infinite: Disinformation Campaigns Used to Require a Lot of Human Effort, but Artificial Intelligence Will Take Them to a Whole New Level,” *The Atlantic*, September 20, 2020, <https://www.theatlantic.com/ideas/archive/2020/09/future-propaganda-will-be-computer-generated/616400>.

¹⁴ Cresci, “A Decade of Social Bot Detection.”

¹⁵ Kate Starbird, “Disinformation’s Spread: Bots, Trolls, and All of Us,” *Nature* 571, no. 449 (2019), <https://doi.org/10.1038/d41586-019-02235-x>.

¹⁶ Samantha Bradshaw, Hannah Bailey, and Philip N. Howard, *Industrialized Disinformation: 2020 Global Inventory of Organized Social Media Manipulation* (Oxford: University of Oxford, 2021), <https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/127/2021/01/CyberTroop-Report20-FINALv.3.pdf>.

пропаганда – «мощный инструмент, способный разрушить демократию». ^{17,18} Хотя технологические компании и исследователи продолжают совершенствовать распознавание компьютерной пропаганды, они знают, что искоренить сетевых ботов и дезинформацию невозможно. Нужны усилия всего общества для повышения устойчивости граждан к растущей угрозе, которая разрушает доверие в обществе.

Правительства реагируют на дезинформацию с обеих сторон уравнения поступления и потребления. С точки зрения поступления дезинформации важно ограничить поток дезинформации в информационную экосистему. С точки зрения потребления нужно решить проблему потребления гражданами дезинформации. ¹⁹ Далее в статье рассмотрены обе части уравнения поступления и потребления дезинформации.

Поступление дезинформации

Очевидно, что решение проблемы поступления дезинформации побуждает правительства, технологические компании и гражданское общество к сотрудничеству для выработки ответа всего общества. Политикам сложно противодействовать поступлению дезинформации из-за отсутствия главного органа, ответственного за противодействие операциям дезинформации. Поэтому в стране может не быть скоординированной политики реагирования. Как следствие, при дезинформационной атаке на внутреннюю политику (например, безопасность на выборах, катастрофы, реагирование на пандемию и вакцинация) профильное ведомство может не иметь средств, чтобы отреагировать на атаку. А когда права и обязанности пересекаются, бывает сложно определить, какое ведомство в государстве должно организовать реагирование (внутренняя безопасность, министерство обороны, министерство юстиции, избирательная комиссия и т.д.). Злоумышленники видят зазоры между правительственными ведомствами и используют их для атак.

Подходы к ограничению дезинформации с точки зрения поступления включают законодательство, правительственных контролёров по проверке фактов и информационные войска, но оценивать их эффективность пока ещё слишком рано. ²⁰ Например, в Германии в 2017 г. приняли Закон о

¹⁷ Woolley and Howard, “Computational Propaganda Worldwide.”

¹⁸ Stanford History Education Group (SHEG), “Evaluating Information: The Cornerstone of Civic Online Reasoning,” Working Paper (Stanford: SHEG, 2016), <https://stacks.stanford.edu/file/druid:fv751yt5934/SHEG%20Evaluating%20Information%20Online.pdf>.

¹⁹ Alina Polyakova and Daniel Fried, “Democratic Defense Against Disinformation 2.0,” *Atlantic Council*, June 2019, https://www.atlanticcouncil.org/wp-content/uploads/2019/06/Democratic_Defense_Against_Disinformation_2.0.pdf.

²⁰ Olga Robinson, Alistair Coleman, and Shayan Sardarizadeh, “A Report of Anti-Disinformation Initiatives” (Oxford: University of Oxford, August 2019),

правопорядке в сети, обязывающий компании, которые ведут соцсети, удалять проявления ненависти и другие нарушения в контенте. Недостатком этого закона является то, что он может привести к цензуре и ограничить свободу слова.²¹

Ещё одним подходом с точки зрения поступления является внедрение в Евросоюзе добровольного, самостоятельно применяемого стандарта для технологических компаний, таких как Google, Facebook, Mozilla и Twitter. В 2018 г. они подписали Кодекс ЕС по борьбе с дезинформацией и обязались повысить прозрачность политической рекламы, удалив фейковые аккаунты, и решить проблему злонамеренного использования ботов. Первые выводы о Кодексе неоднозначны. Сохраняется нехватка доверия между компаниями, ведущими соцсети, правительствами и гражданским обществом, в основном из-за того, что технологические компании ограничивают доступ к своим данным.²² В 2020 г. Еврокомиссия дала комплексный ответ на дезинформацию – План действий европейской демократии (European Democracy Action Plan).²³ Одна из его инициатив – сделать Кодекс дополнительным нормативным актом.

Со своей стороны, Эстония, бывшая объектом русской дезинформации с 2007 г., привлекает для этого гражданское общество. Правительство создало добровольные силы безопасности – Лигу защиты Эстонии – под эгидой Министерства обороны. Лига защиты Эстонии помогает киберобороне, а также мониторит Интернет на предмет дезинформации и ведёт контрпропагандистский блог, чтобы бороться с ложными нарративами. Эстония также привлекает группу интернет-активистов «Балтийские эльфы» для реагирования на русских троллей, сообщения о ботах, распространения контрнарративов.²⁴ Кроме того, поскольку в Эстонии проживает немалая русская община, там работает русскоязычный телеканал для противодействия дезинформации.

Тайвань – ещё одна страна, чей подход предусматривает участие всего общества в обуздании потока дезинформации. С 2018 г., когда на Тайване впервые назначили Министра информатизации, страна инициировала не-

<https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2019/08/A-Report-of-Anti-Disinformation-Initiatives>.

²¹ “Germany: Flawed Social Media Law,” *Human Rights Watch*, February 14, 2018, <https://www.hrw.org/news/2018/02/14/germany-flawed-social-media-law>.

²² James Pammet, “EU Code of Practice on Disinformation: Briefing Note for the New European Commission” (Carnegie Endowment for International Peace, March 3, 2020), <https://carnegieendowment.org/2020/03/03/eu-code-of-practice-on-disinformation-briefing-note-for-new-european-commission-pub-81187>.

²³ European Commission, “European Democracy Action Plan,” accessed February 2, 2021, https://ec.europa.eu/info/strategy/priorities-2019-2024/new-push-european-democracy/european-democracy-action-plan_en.

²⁴ Joseph Robbins, “Countering Russian Disinformation” (Center for Strategic & International Studies, September 23, 2020), <https://www.csis.org/blogs/post-soviet-post/countering-russian-disinformation>.

сколько гражданских технических инициатив для укрепления доверия граждан и гражданского общества. Министр информатизации не только придумал прозрачное правительство, но и объединил усилия правительственных групп, технологических компаний и граждан по противодействию дезинформации. Тайвань реализует ряд успешных инициатив, включая Сеть проверки фактов в Интернете, чат-боты для проверки фактов в соцсетях и мемы против нарративов дезинформации.²⁵

Главное преимущество подхода Эстонии и Тайваня – участие граждан в борьбе с дезинформацией. Войну с дезинформацией можно выиграть, только ведя её вместе с гражданами, которые потребляют и распространяют дезинформацию. Если граждане игнорируют дезинформацию, её распространение затухает. В следующем разделе этой статьи мы рассмотрим методы борьбы с потреблением дезинформации.

Потребление дезинформации

Один из путей сократить потребление дезинформации – цифровая грамотность и знания о дезинформации.²⁶ Доказано, что цифровая грамотность может быть эффективной стратегией борьбы с дезинформацией.²⁷ Поскольку общепринятого определения цифровой грамотности нет, в этой статье цифровая грамотность включает медийную, новостную и информационную грамотность и определяется как «способность использовать информационно-коммуникационные технологии для поиска, оценки, создания и передачи информации, требующая когнитивных и технических навыков».²⁸

Часто считают, будто пожилые люди более восприимчивы к дезинформации, чем молодые, из-за того, что им сложно пользоваться цифровыми технологиями. Есть данные, что пожилые люди чаще делятся дезинформацией в соцсетях.²⁹ Но молодые люди, более привычные к технологиям, тоже подвержены дезинформации из-за низкой цифровой грамотности. Группа изучения истории Стэнфордского университета (Stanford History Ed-

²⁵ Rorry Daniels, “Taiwan’s Unlikely Path to Public Trust Provides Lessons for the US,” *Brookings*, September 15, 2020, <https://www.brookings.edu/blog/order-from-chaos/2020/09/15/taiwans-unlikely-path-to-public-trust-provides-lessons-for-the-us>.

²⁶ Polyakova and Fried, “Democratic Defense Against Disinformation 2.0.”

²⁷ Andrew M. Guess et al., “A Digital Media Literacy Intervention Increases Discernment Between Mainstream and False News in the United States and India,” *Proceedings of the National Academy of Sciences* 117, no. 27 (2020): 15536-15545, <https://www.pnas.org/content/pnas/117/27/15536.full.pdf>.

²⁸ American Library Association (ALA), “Literacy for All: Adult Literacy through Libraries,” (Chicago: ALA, 2019), http://www.ala.org/aboutala/sites/ala.org/aboutala/files/content/Literacy%20for%20All_Toolkit_Online.pdf.

²⁹ Andrew Guess, Jonathan Nagler, and Joshua Tucker, “Less Than You Think: Prevalence and Predictors of Fake News Dissemination on Facebook,” *Science Advances* 5, no. 1 (January 2019), <https://doi.org/10.1126/sciadv.aau4586>.

ucation Group) выяснила, что студентам школ, ВУЗов и колледжей трудно оценить достоверность информации в соцсетях. Они ошибочно считают информацию достоверной, исходя из неверных фактов: верхние результаты поиска в поисковике, принадлежность сайта к домену .org или аккаунт в Твиттере с большим числом подписчиков.³⁰ Эти недостатки указывают на необходимость цифровой грамотности общества.

Политики и педагоги переосмысливают основы цифровой грамотности, включая критическое мышление и гражданскую активность в программы обучения. Ранее правительства больше занимались развитием цифровых навыков, необходимых для инициатив «цифровой трансформации», что не всегда включало критическое мышление и гражданскую активность. Однако более новые программы включают устойчивость граждан. Так, в Канаде в 2019 г. предложили совместную инициативу «Цифровой гражданин» (Digital Citizen). Эта инициатива поддерживает гражданскую активность, в частности, разработку учебных материалов, инвестиции в программы исследований и медийную грамотность (гражданскую, новостную и цифровую).³¹ Есть и неправительственные программы. Например, два института Университета Южной Флориды (Флоридский центр кибербезопасности (Florida Center for Cybersecurity) и Флоридский центр методик обучения (Florida Center for Instructional Technology)) объединились с неприбыльным беспартийным аналитическим центром «New America» для развития навыков киберграждан у школьников. Они планируют создать Рабочую группу по кибергражданству (Cyber Citizenship Working Group) для взаимодействия с деятелями гражданского общества и Портал кибергражданства (Cyber Citizenship Portal), где будут представлены образовательные материалы для общественности.³²

Пока ещё рано оценивать эффективность программ обучения цифровой грамотности и информированности. Более того, цифровая грамотность граждан – лишь первый шаг к новым знаниям и навыкам, таким, как алгоритмическая грамотность и информационная грамотность (об ИИ).³³ Чтобы подготовиться к новым вызовам, политикам нужно стратегическое предвидение, дабы лучше подготовить граждан к дезинформационным атакам

³⁰ Stanford History Education Group, “Evaluating Information: The Cornerstone of Civic Online Reasoning.”

³¹ UNESCO, “Digital Citizen Initiative,” *UNESCO Diversity of Cultural Expressions*, по состоянию на 1 февраля 2021, <https://en.unesco.org/creativity/policy-monitoring-platform/digital-citizen-initiative>.

³² “Cyber Florida, Florida Center for Instructional Technology and New America Launch New Partnership to Improve ‘Cyber Citizenship’ Skills for K-12 Students,” *New America* (International Security), December 16, 2020, www.newamerica.org/international-security/press-releases/cyber-florida-fcit-new-america-partnership-to-improve-cyber-citizenship.

³³ Ramesh Srinivasan, “This Is How Digital Literacy Can Transform Education,” *World Economic Forum*, March 3, 2020, <https://www.weforum.org/agenda/2020/03/why-is-digital-literacy-important>.

нового поколения. Подводя итоги, начальной точкой повышения устойчивости граждан являются следующие политические рекомендации:

Политическая рекомендация №1: Повышать цифровую грамотность всех граждан

Правительства должны разработать программу цифровой грамотности для обучения цифровой грамотности всех граждан, выработав её стандарт или принципы. Существует много систем, используемых в качестве основы создания программы цифровой грамотности. В их числе – Глобальные основы цифровой грамотности (Digital Literacy Global Framework) Организации Объединённых Наций по вопросам образования, науки и культуры (ЮНЕСКО), Основы цифровой грамотности граждан (Digital Competence Framework for Citizens) Европейского Союза и Основы цифрового интеллекта (DQ) д-ра Ю Хьон Пак.

Заложив основы, правительство должно разработать программу обучения цифровой грамотности, соответствующую потребностям граждан на разных этапах жизни (первичный, вторичный и третичный уровень). Разработав программы обучения для разных уровней, педагоги и учителя смогут быстро адаптировать материал к своей учебной программе. Методы обеспечения доступности контента для взрослых включают организацию массовых открытых онлайн-курсов и создание онлайн-видео для самообучения на протяжении всей жизни. Навыки цифровой грамотности не только повысят устойчивость граждан к дезинформации, но и подготовят их к неминуемой цифровой трансформации, то есть переустройству общества в результате внедрения цифровых технологий.

Политическая рекомендация №2: Включать цифровую безопасность в ежегодные кампании информирования о кибербезопасности

Осведомленность граждан начинается с кампаний информирования общественности. Многие правительства уже используют ежегодный месяц или неделю кибербезопасности для повышения безопасности в Интернете и пропаганды мер безопасности. Поскольку главный элемент кибербезопасности – это понимание онлайн-угроз для безопасности граждан, информирование о дезинформации необходимо. В частности, нужно рассказывать о сетевых ботах и об оценке источников информации в интернете. Кампания информирования даёт ещё одну возможность привлечь внимание граждан к дезинформации.

Политическая рекомендация №3: Усилить гражданское общество, укрепляя доверие и информируя об использовании компьютерной пропаганды государством и политиками

Укрепление доверия и обмен информацией повышает устойчивость граждан. Граждане не поймут масштаб и силу компьютерной пропаганды против их страны, если они не вооружены информацией. Им нужно знать, кто

совершил дезинформационную атаку, какую, где, когда и как, и как они могут противостоять дезинформации. Поскольку политическая компьютерная пропаганда может быть организована государством, правительства не всегда могут рассказать все детали атаки по соображениям секретности. Для достижения доверия правительству надо найти способ откровенно сообщить об атаке, в то же время придерживаясь требований безопасности. Информацию также следует доносить простым языком, избегая технических терминов и канцляризмов.

Правительства также могут поощрять партнёрство государства с частным сектором для обмена информацией и сотрудничества при решении задач технической компьютерной пропаганды и устойчивости граждан. Поскольку технологические компании владеют данными, необходимыми правительству, общественным организациям и учёным для выработки мер противодействия, партнёрство позволяет вырабатывать инновационные решения путём привлечения граждан и укреплять доверие благодаря обмену информацией и открытому диалогу. Сейчас правительства, технологические компании и гражданское общество больше, чем когда-либо, должны сотрудничать для укрепления доверия и устойчивости граждан.

Примечание

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

Об авторе

Инез Миямото – профессор кибербезопасности в Азиатско-Тихоокеанском центре исследований в области безопасности имени Даниэля Иноуйе. Электронная почта: miyamotoi@dkiapcss.net



Соцсети – Язык ненависти – Преступления на почве ненависти

Лукаш Вилим

Министерство внутренних дел Чешской Республики,

<https://www.mvcr.cz/mvcren/>

Аннотация: В статье рассмотрена проблема языка ненависти в социальных сетях с точки зрения системы безопасности Чехии и ее инструментов, предназначенных для обеспечения внутренней безопасности, а также необходимые изменения в законодательстве, которые позволят правоохранительным органам эффективно решить эту проблему. При нынешнем подходе к киберпространству социальные сети становятся инструментом постоянного распространения основанных на ненависти идеологий, а этого нельзя допустить.

Ключевые слова: соцсети, система безопасности, язык ненависти, преступная деятельность, экстремизм, терроризм, недопущение.

Вступление

В настоящее время в социальных сетях нередко наблюдаются проявления ненависти, дезинформации, элементы экстремизма и терроризма. Мы уже видим, как политические и религиозные экстремистские группировки используют соцсети для распространения своей идеологии, вовлечения новых членов, демонстрации силы, шокируют общество съёмками войны как чего-то обычного и неизбежного. Общество и само может противодействовать такому использованию социальных сетей и его негативным последствиям. Для этого есть много путей. Прежде всего могут реагировать пользователи соцсетей, указав на неприемлемое поведение своим друзьям и заявив, что они не желают иметь ничего общего с подобными постами. Они могут осудить такое поведение или удалить эти профили из друзей. Можно назвать такой подход наивным, но мы исходим из того, что у нас – демократическое общество, основанное на коллективном договоре граждан, что

предполагает некую моральную ответственность перед окружающими. Другой путь – сообщить о проблемном профиле администратору соцсети, который оценит, настолько ли высок уровень насилия или ненависти в посте, что требуется вмешательство в виде блокировки или удаления аккаунта. В крайних случаях можно решиться на правовые меры, а именно сообщить о неприемлемом комментарии, профиле или группе правоохранительным органам, которые обязаны оценить, подпадает ли действие под определение преступления и нужны ли шаги, предусмотренные Уголовно-процессуальным кодексом.

Перед тем, как рассмотреть репрессивные меры, следует обратить внимание на инструменты, имеющиеся у демократического государства и системы безопасности Чехии для успешной борьбы с этим явлением в реальном мире и в киберпространстве.

Инструменты системы безопасности Чешской Республики для борьбы с языком ненависти в Интернете

Демократическое государство руководствуется Конституцией и Хартией основных прав и свобод, которые гарантируют свободу выражения. Нужны адекватные инструменты, защищающие эти права и в то же время не допускающие нежелательных проявлений и нарушений закона при их использовании. Вопрос языка ненависти или преднамеренного распространения дезинформации можно рассматривать с разных позиций: с точки зрения внутренней безопасности государства, этического воспитания общества, профессионализма СМИ или сил безопасности государства.

Верхушку системы безопасности составляют правительство, исполнительные ведомства и Палата депутатов Чешской Республики. Постоянным рабочим органом правительства Чехии по вопросам безопасности является Государственный совет безопасности (*Bezpečnostní rada státu – BRS*), предусмотренный конституционным законом №110/1998 «О безопасности Чешской Республики». Это один из стратегических инструментов противодействия новым угрозам в киберпространстве в виде нежелательного контента. Согласно закону,¹ в BRS имеется шесть постоянных рабочих органов, обязанных подавать стратегические документы и материалы о безопасности государства (т.е. о новых угрозах безопасности). Безопасность киберпространства оценивают на трёх базовых уровнях: киберзащита, кибербезопасность и киберпреступность. В организационном плане кибербезопасность опирается на эффективные скоординированные действия вооружённых сил, соответствующего органа кибербезопасности (Национальное управление кибернетической и информационной безопасности; *Národní úřad pro kybernetickou a informační bezpečnost – NÚKIB*), сил безопасности (особенно чешской полиции) и разведслужб, а также частного сектора. В связи с таким

¹ Правительство Чешской Республики, www.vlada.cz/assets/ppov/brs/Statut-BRS-rijen-2018.pdf.

возможным разделением вопроса к решению проблемы языка ненависти в киберпространстве привлекаются три комитета BRS: Комитет внутренней безопасности (в сфере ведения Министерства внутренних дел), Комитет кибербезопасности (в сфере ведения Национального управления кибернетической и информационной безопасности), и Комитет по разведывательной деятельности, подчинённый премьер-министру. Пока что все меры по рассмотрению человеконенавистнического содержания или дезинформации в киберпространстве поручают в первую очередь Комитету внутренней безопасности, что процедурно соответствует Закону о полномочиях.²

О существовании и угрозе языка ненависти в Интернете сообщалось ещё в 1997 г. в Докладе о ходе расследования государственными органами преступлений по мотивам расизма и ксенофобии (“Zpráva o postupu státních orgánů při postihu trestných činů motivovaných rasismem a xenofobií”), а затем, с их обострением – в каждом новом годовом докладе Министерства внутренних дел об экстремизме и терроризме. Из содержания докладов можно заключить, что Интернет и, соответственно, социальные сети становятся не только местом распространения человеконенавистнических идей или экстремистских идеологий, но и средой языка ненависти и прямых выпадов против людей из-за их цвета кожи, религии или просто другого мнения. Поэтому больше внимания уделяется мониторингу событий в Интернете, связанных с экстремизмом и терроризмом, о чём можно прочитать в соответствующих годовых докладах полиции, разведслужб и учёных.

Вопрос преступлений на почве ненависти и языка ненависти рассмотрен в документе, подготовленном профессором Мирославом Марешем (Miroslav Mareš) в 2011 г. в рамках анализа под названием «Проблематика преступлений на почве ненависти» (“*Problematika Hate Crime*”). В анализе упоминается обязанность

принимать меры против всех форм выражения, в том числе в средствах массовой информации и в Интернете, которые могут быть обоснованно истолкованы как приводящие к подстрекательству, распространению или поддержке дискриминации в отношении лесбиянок, геев, бисексуалов и трансгендеров, а также других форм дискриминации. Такие проявления должны запрещаться и публично осуждаться, когда они имеют место. При всех мерах должны уважаться основные права на свободу выражения согласно Статье 10 Конвенции и судебной практике Европейского суда (Комитет министров, Совет Европы, 2010).³

² Act No. 2/1969 Coll., “On the Establishment of Ministries and Other Central Bodies of the State Administration of the Czech Republic, Which Designates Individual Central Bodies and Regulates Their Competence,” Public administration portal, Ministry of Interior, <https://portal.gov.cz/app/zakony/zakonPar.jsppage=0&idBiblio=31338&fulltext=&nr=2~2F1969&part=&name=&rpp=15#local-content>.

³ “Problematika Hate Crimes,” страница Министерства внутренних дел Чешской Республики, 20 июля 2020, www.mvcr.cz/clanek/problematika-hate-crimes.aspx.

Именно в этом заключается решение проблемы языка ненависти в Интернете, в том числе в социальных сетях, на международном уровне.

Так называемый «Аудит национальной безопасности» (“*Audit národní bezpečnosti*”), в нескольких главах рассматривающий проявления человеконенавистнического содержания в Интернете, можно уверенно считать важным материалом Министерства внутренних дел по данному вопросу. Вопрос борьбы с распространением человеконенавистнического и радикального контента в Интернете и соцсетях рассматривается в главе о террористических угрозах, об экстремистских угрозах, как справа (например, ненависть к определённым меньшинствам), так и слева (классовая ненависть, ненависть к идейным оппонентам и ненависть к государственной власти и всей демократической системе), угрозах кампаний дезинформации с распространением ненависти по отношению к определённым группам населения, а также органам государственной власти, и угрозах достижению военных, политических или экономических целей внешней политики Чехии. Кибертерроризм тоже назван в аудите реальной угрозой безопасности, при которой государство обязано, в частности, защищать себя от действий в киберпространстве в виде подстрекательства к ненависти или создания и распространения пропаганды. Киберсреду для терроризма следует понимать как средство или инструмент реализации политических, религиозных или иных амбиций агрессора.⁴ Аудит национальной безопасности, как важный документ стратегии безопасности, был утверждён постановлением Правительства №1125 14 декабря 2016 г. и прошёл оценку Комитета внутренней безопасности и, затем, Государственного совета безопасности. Постановление Правительства предписывало министру внутренних дел составить План действий по Аудиту национальной безопасности и представить его Правительству до 30 апреля 2017 г. План действий был утверждён Постановлением Правительства №407 от 22 мая 2017 г. В то же время руководителям конкретных мероприятий Плана действий было предписано обеспечить их выполнение. Так, министр внутренних дел должен ежегодно, до 30 апреля, представлять оценку выполнения Плана действий Государственному совету безопасности.⁵ Государственный совет безопасности принял к сведению оценку выполнения Плана действий Аудита национальной безопасности в 2019 г. Постановлением от 8 июня 2020 г. в материале содержались выводы о ходе выполнения задач, поставленных перед конкретными руководителями, включая проблему языка ненависти.⁶

⁴ “*Audit národní bezpečnosti – Bezpečnostní aspekty migrace – Aktuální informace o migraci*,” Министерство внутренних дел Чешской Республики, 21 июля 2020, <https://www.mvcr.cz/migrace/clanek/audit-narodni-bezpecnosti-bezpecnostni-aspekty-migrace.aspx>.

⁵ Постановление Правительства Чешской Республики от 14 декабря 2016 г. № 1125.

⁶ “*Bezpečnostní rada státu se zabývala otázkami spojenými s řešením situace v souvislosti s výskytem onemocnění covid-19*,” Правительство Чешской Республики,

Как указано выше, Государственный совет безопасности или его комитеты могут непосредственно заняться проблемой языка ненависти. Помимо Комитета внутренней безопасности (*Výbor pro vnitřní bezpečnost – VVB*) – главного органа, ответственного за эту проблему – другие комитеты тоже могут рассмотреть это явление в пределах своих полномочий.

Язык ненависти также может быть элементом кампаний дезинформации в СМИ, известных как *фейковые новости*⁷ – лживые новости в соцсетях, к которым часто прибегают экстремисты для продвижения своих идей. Общество давно требует дать политическую оценку этому явлению. Оно также может требовать от компетентных органов власти комментариев по той или иной кампании дезинформации. При рассмотрении этой угрозы безопасности важно понимать, что органы государственной власти не имеют монополии на правду и не могут решать, что правдиво, а что нет, в новостях. Прежде чем объявить новость фальшивой, ей нужно проанализировать и определить, какая информация в конкретной «фейковой новости» должна считаться ложной. Для этого в демократическом обществе есть независимые СМИ, которые проверяют новости, критикуют и затем комментируют их. Органы власти могут комментировать новость, только если они обладают достаточной проверенной информацией, и она относится к их компетенции. Затем граждане формируют своё мнение и решают, верить новости или нет.

Проявление ненависти в рамках лживых новостей или комментариев в соцсетях также может быть элементом политической кампании государства по влиянию на граждан страны, государственную политику или отвлечению внимания от реальных проблем. Нынешней тенденцией является сочетание многочисленных угроз целостности и единству государства, получившее название гибридной угрозы. Этот термин часто используют, но определить его содержание нелегко:

Определения гибридных угроз различны и зависят от изменчивого характера этих угроз. В целом, [гибридная угроза] – это набор различных принудительных и подрывных мер, стандартных и нестандартных методов (в частности, дипломатических, военных, экономических и технических), которые различные государственные и негосударственные органы могут скоординировано применять для достижения конкретных целей без официального объявления войны. Обычно их цель – использовать уязвимые места жертвы и создать запутанные ситуации для срыва процесса принятия решений. *Массированные кампании дезинформации и*

8 июня 2020, <https://www.vlada.cz/cz/media-centrum/aktualne/bezpecnostni-rada-statu-se-zabyvala-otazkami-spojenyimi-s-resenim-situace-v-souvislosti-s-vyskytem-onemocneni-covid-19-181915/>.

⁷ Фейковые новости – это *лживые новости*. Этим термином называют тревожные «утки», ложь и дезинформацию, распространяемую в Интернете, в печатных СМИ и по телевидению. Люди часто сталкиваются с ними, например, в соцсетях или в электронной почте. Источник: *nav-ches*, 23 июля 2020, www.vodafone.cz/uzitecne-odkazy/slovník-pojmu/fake-news/.

использование соцсетей для пропаганды или радикализации, привлечения и прямого контроля сторонников могут быть инструментами этих гибридных угроз.⁸

Для противодействия гибридным угрозам в Министерстве внутренних дел создан так называемый Центр терроризма и гибридных угроз (*Centrum pro terorizmus a hybridní hrozby – СТНН*), задача которого – «устранение гибридных угроз для безопасности Чешской Республики, находящихся в сфере ведения Министерства внутренних дел, таких, как терроризм, нападение на незащищённые объекты, безопасность миграции, экстремизм, массовые мероприятия, нарушения общественного порядка и различная преступная деятельность, или же аспекты безопасности кампаний дезинформации, затрагивающих внутреннюю безопасность государства. Центр был создан, исходя из рекомендаций Аудита национальной безопасности, утверждённых правительством».⁹ СТНН создан решением министра внутренних дел Милана Хованеца 1 января 2017 г. на основе Аудита национальной безопасности и согласно Стратегии безопасности Чешской Республики 2015 г.¹⁰

Государственный совет безопасности тоже отреагировал, создав экспертную рабочую группу по гибридным угрозам. В группу вошли представители Государственного совета безопасности, чешских разведслужб, Управления национальной безопасности, чешской полиции, Национального банка Чехии, Государственного управления ядерной безопасности и Уполномоченного Правительства по кибербезопасности. Экспертная рабочая группа была создана постановлением Государственного совета безопасности № 9 от 8 марта 2017 г. Все её члены обязаны сотрудничать, обмениваясь информацией о гибридных угрозах.¹¹

Как указано выше, у государства имеется множество инструментов для борьбы с языком ненависти, в том числе и на высшем правительственном уровне. Члены Правительства или Государственного совета безопасности решают, считать ли язык ненависти достаточно серьёзной проблемой, чтобы решать её, применяя необходимые контрмеры, или оставлять её решение органам более низкого уровня, например, правоохранительным ор-

⁸ “Hybridní hrozby”, Министерство здравоохранения, 20 июля 2020, www.mzcr.cz/hybridni-hrozby.

⁹ “Úvodní strana – Terorismus a těžké cíle”, Министерство внутренних дел Чешской Республики, 24 июля 2020, <https://www.mvcr.cz/cthh/>.

¹⁰ “Bezpečnostní strategie České republiky”, Правительство Чешской Республики, 2015, 9 октября 2020, <https://www.vlada.cz/assets/ppov/brs/dokumenty/bezpecnostni-strategie-2015.pdf>.

¹¹ “Bezpečnostní rada státu schválila ustavení odborné pracovní skupiny pro hybridní hrozby,” Правительство Чешской Республики, 8 марта 2017 www.vlada.cz/cz/media-centrum/aktualne/bezpecnostni-rada-statu-schvalila-ustaveni-odborne-pracovni-skupiny-pro-hybridni-hrozby-154226/.

ганам, занимающимся киберпреступностью. С другой стороны, стоит отметить, что нижние эшелоны обязаны предлагать решения и подавать предложения по устранению новых угроз безопасности. Таким образом, задача руководителя по внутренней безопасности – отслеживать и оценивать информацию от своих подразделений и выработать стратегию противодействия. Также важно понимать, что решение проблемы языка ненависти организованных экстремистских группировок, например, является обязанностью Министерства внутренних дел и других сил безопасности, которые тоже могут подавать комитетам Государственного совета безопасности концептуальные и стратегические документы.

Существующее законодательство о языке ненависти в соцсетях

Мы не найдём определения языка ненависти в правовой системе Чехии:

Под ним обычно понимают оскорбительную речь, которая подстрекает, поощряет или распространяет ненависть к определённой группе людей или человеку и часто провоцируется предрассудками и стереотипами. Причиной ненависти может быть, например, цвет кожи, гражданство, национальность, пол, сексуальная ориентация или идентификация, религия, вера, мировоззрение, возраст, инвалидность человека и т.д. Язык ненависти можно отнести к более широкой категории насилия по мотивам ненависти, что включает не только словесные, но и физические оскорбления из-за ненависти к некоторым уязвимым группам населения.¹²

Язык ненависти в Интернете в первую очередь может рассматриваться как правонарушение в рамках одного из законов о правонарушениях:

Это может быть правонарушение против гражданского сожительства, совершаемое путем причинения вреда другому лицу из-за его принадлежности к национальному меньшинству, этнического происхождения, расы, цвета кожи, пола, сексуальной ориентации, языка, веры, религии, возраста, инвалидности, политических или иных убеждений, членства или деятельности в политических партиях или политических движениях, профсоюзах или иных объединениях, социального происхождения, имущественного положения, здоровья или семейного положения.¹³ За это нарушение может быть наложен штраф в размере до 20 000 чешских крон.¹⁴

Если человеконенавистническое поведение в соцсетях превышает некий порог, его должны оценить правоохранительные органы. Далее они оценивают наличие признаков состава преступления. Какие преступления име-

¹² A. Šabatová, “Nenávistné projevy na internetu a rozhodování českých soudů,” No. 47/2019/DIS/PŽ, No.: KVOP-2720/2020 (Výzkum veřejného ochránce práv, 2020).

¹³ Положения Ст. 7, часть 3.б) Закона о некоторых правонарушениях.

¹⁴ Согласно Ст. 7, часть 4.б) Закона о некоторых правонарушениях.

ются в виду, можно понять из исследования Омбудсмена 2020 г. под названием «Проявления ненависти в Интернете» (“Nenávistné projevy na internetu”). В этом документе преступления на почве ненависти профессионально описаны, как так называемая триклинная система, и

если мотив предубеждения является элементом основной фактической стороны некоторых уголовных преступлений, лицо, совершившее эти преступления, наказывается лишением свободы на срок до трех лет. Кроме того, для отдельных преступлений мотив предубеждения является условием применения более высокой обязательной меры наказания, так называемой фактологической базы для квалификации. Тогда мотив ненависти также включается в Уголовный кодекс в качестве так называемого общего отягчающего обстоятельства, которое применяется, если фактическая сторона конкретного преступления не содержит специального отягчающего обстоятельства (квалифицируемая фактическая сторона). Общее отягчающее обстоятельство принимается во внимание при определении наказания, которое затем назначается в рамках основного обязательного наказания.¹⁵

Главное внимание в связи с языком ненависти, проявлениями ненависти и преступлениями уделяется наиболее частым преступлениям; такие действия основаны на анализе Омбудсмена с 2016 г., который, благодаря его опыту, весьма информативен и пригоден для органов, занимающихся уголовным производством, работающих с окончательными решениями судов. Исследовалась избранная группа наиболее частых преступлений. Это не исчерпывающий список всех преступлений, которые могут быть связаны с языком ненависти в Интернете.

Заключительная часть анализа касается преступлений и вынесенных наказаний. Наиболее частыми (см. Рис. 1) были факты подстрекательства к ненависти к группе людей или подавлению их прав и свобод (Статья 356 Уголовного кодекса) – почти половина рассмотренных судебных решений. Примерно пятую часть составляли случаи оскорбления нации, расы, этнических и других групп (Ст. 355); далее шли насилие против группы граждан или отдельных лиц (Ст. 352) и выражение симпатии к движению, направленному на подавление прав и свобод человека (Ст. 404). Согласно анализу Омбудсмена, другие факты отмечались реже.

Ниже перечислены преступления, связанные с языком ненависти в Интернете, согласно Закону 40/2009, Уголовному кодексу (действующему законодательству), и наиболее частые преступления по анализу Омбудсмена на основе судебных решений, вынесенных с 2016 г. по июнь 2019 г. Всего отмечено 47 случаев проявления языка ненависти в Интернете. Через доступную компьютерную сеть против группы людей (граждан) или отдельных

¹⁵ Ombudsman, “Nenávistné projevy na internetu a rozhodování českých soudů: Výzkum veřejného ochránce práv 2020,” July 25, 2020, https://www.ochrance.cz/fileadmin/user_upload/ESO/47-2019-DIS-PZ-Vyzkumna_zprava.pdf.

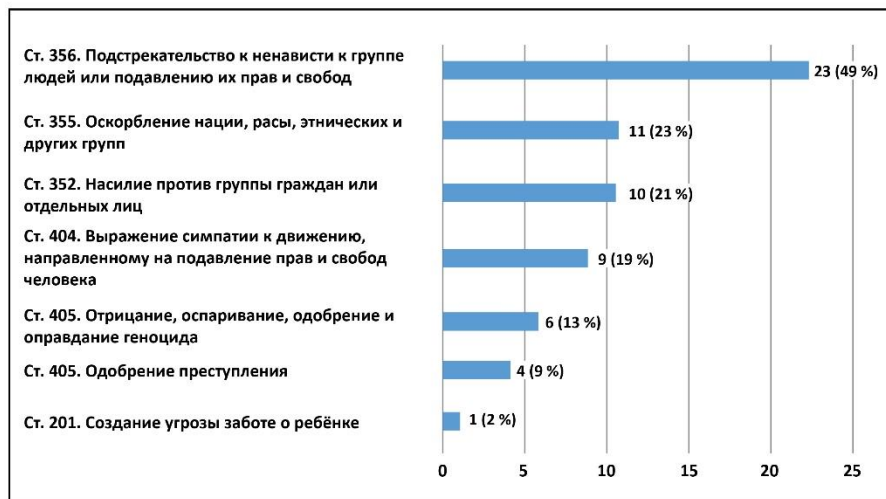


Рис. 1: Статьи Уголовного кодекса, применимые к преступлениям на почве ненависти ¹⁶

лиц из-за их фактической или предполагаемой расы, этнической принадлежности, гражданства, политических убеждений, религии или реального либо предполагаемого атеизма совершались следующие преступления:

Ст. 352. Насилие против группы граждан или отдельного лица

- Угроза группе граждан смертью, увечьем или крупным ущербом.

Ст. 355. Оскорбление нации, расы, этнической или другой группы

- Публичное оскорбление нации, её языка, расы, этнической или другой группы.

Ст. 356. Подстрекательство к ненависти к группе людей или подавлению их прав и свобод

- Публичное подстрекательство к ненависти к нации, расе, этнической группе, религии, классу либо другой группе людей или ограничению прав и свобод их членов.

Ст. 365. Одобрение преступления

- Публичное одобрение преступления или публичная похвала преступнику;
- Вознаграждение или компенсация наказания нарушителю или приближённому к нему лицу;

¹⁶ Šabatová, A. Nenávistné projevy na internetu a rozhodování českých soudů, Výzkum veřejného ochránce práv 2020, No.: 47/2019/DIS/PŽ, No.: KVOP-2720/2020, p. 23.

- Организация сбора для такого вознаграждения или компенсации.

Ст. 403. Основание, поддержка и поощрение движения, направленного на подавление прав и свобод человека

- Характер данного преступления заключается в создании, поддержке или поощрении движения, явно направленного на подавление прав и свобод человека или провозглашающего расовую, этническую, национальную, религиозную или классовую неприязнь или неприязнь к иной группе лиц.

Хотя указанная выше фактическая сторона преступления не часто упоминается в индивидуальной статистике, она принадлежит к числу важнейших, поскольку она связана с распространением экстремистских идеологий, тесно связанных с языком ненависти как в реальном, так и в виртуальном мире.

Ст. 404. Выражение симпатии к движению, направленному на подавление прав и свобод человека

- *Публичное* выражение симпатии к движению, упомянутому в Ст. 403.

Ст. 405. Отрицание, оспаривание, одобрение и оправдание геноцида

- *Публичное* отрицание, оспаривание, одобрение или оправдание нацистского, коммунистического или другого геноцида либо нацистских, коммунистических или других преступлений против человечности, либо военных преступлений, либо преступлений против мира.

Вышеупомянутое уголовное законодательство охватывает большую часть преступных деяний в киберпространстве, касающихся преступлений на почве ненависти и проявлений ненависти отдельными лицами или группами лиц. Демонстрация намерения правонарушителя поддержать или продвигать уже не существующее движение может представлять проблему. Это касается движений, которые в прошлом поддерживали или продвигали радикальные идеи, направленные на подавление прав и свобод человека.

Суть проблемы заключается в том, что согласно ст.ст. 403 и 404, невозможно преследовать за действия в поддержку или поощрение движения, которое уже не существует:

Допустим, что должны быть соблюдены признаки уголовных преступлений согласно ст.ст. 403 и 404. В этом случае наличие такого конкретного движения должно быть подтверждено оценкой представленных доказательств, а действия обвиняемого должны так или иначе объективно отражать касающиеся его правонарушения.¹⁷

¹⁷ "Povinnost prokázat existenci hnutí směřujícího k potlačení práv a svobod člověka – část I," *Právní prostor*, February 4, 2020, www.pravniprostor.cz/clanky/trestni

Это касается и продажи календарей и чашек с изображением нацистской символики, как символов не существующего в настоящее время движения. Согласно поправкам к уголовному законодательству и опыту, значительный процент деяний, в которых преступник пропагандирует нацистские, коммунистические или другие преступления против человечности, военные преступления или преступления против мира, может преследоваться по ст. 405, где закон включает не действующие в данный момент соображения.

В случае языка ненависти в Интернете правоохранительные органы должны собрать качественные доказательства и проанализировать их, потому что доказательства могут сопровождаться символикой экстремистских движений, направленных на подавление прав и свобод человека.

Нынешние правила установлены постановлением Верховного суда Чешской Республики от 12 июня 2019 г. № 8 Tdo 314 /2019-43. В случае символа, используемого движением, направленным на подавление прав и свобод человека, постановление Верховного суда в первую очередь ссылается на уже упомянутые выводы Уголовной палаты Верховного суда Чешской Республики Trjn 302/2005. Далее там сказано: «Если прокурор не выполняет свою обязанность доказать наличие такого движения уже в подготовительном производстве, то имеются не все юридические признаки состава преступления».¹⁸ Это касается обязанностей не только прокурора, но и органа полиции, возбудившего уголовное дело. Уголовное производство должно начинаться, когда орган полиции убежден, что в его распоряжении имеется достаточно доказательств наличия всех признаков состава преступления.

По мнению Верховного суда, ясно, что для соблюдения критериев уголовных преступлений согласно ст.ст. 403 и 404 Уголовного кодекса *существование такого конкретного движения должно быть доказано представленными доказательствами и объективным поведением обвиняемого в вышеупомянутых уголовных преступлениях*. Правоохранительные органы, участвующие в уголовном производстве, должны следовать мнению Верховного суда, то есть ссылки на другое решение Верховного суда в другом деле, в котором было установлено существование движения, не достаточно для доказательства его существования в данный момент. Существование конкретного экстремистского движения, левого или правого, должно быть доказано прямыми доказательствами, исходящими от правонарушителя, в отношении которого должно быть доказано, что он знал о сути пропагандируемого движения, по крайней мере в общих чертах. Это включает понимание того, что движение явно направлено на подавление прав и свобод человека или распространение и поддержку расовой, этнической, национальной, религиозной или классовой ненависти либо ненависти к конкретной группе людей; желание поддержать или поощрить это

pravo/povinnost-prokazat-existenci-hnuti-smerujiciho-k-potlaceni-prav-a-svobod-cloveka.

¹⁸ Постановление Верховного суда от 12 июня 2019, № 8 Tdo 314/2019-43.

движение своими действиями; или понимание, что действия поддерживали или продвигали такое движение.

И наоборот, нельзя исключать, что общеупотребительный символ будет использоваться не по назначению в экстремистских целях и, следовательно, его нормальное использование усложнится. Примером служит обычный символ ОК (этот жест используют, например, ныряльщики, чтобы подтвердить, что всё в порядке); в прошлом так бывало из-за кампаний дезинформации, вследствие чего некоторые СМИ сочли этот жест расистским. Этот символ даже включила в список расистских символов американская неприбыльная организация «Антидиффамационная лига» (Anti-Defamation League, ADL). Это произошло в 2017 г. из-за «утки»¹⁹ на веб-сайте 4chan.²⁰ Этот простой жест рукой, при котором большой и указательный пальцы сведены вместе, а остальные пальцы вытянуты, используют в Британии с начала XVII века, и обычно он означает понимание, согласие, одобрение или благополучие. Он приобрёл якобы расистскую окраску из-за ложного сообщения, впервые появившегося на портале 4chan и в других социальных сетях, и поэтому новое, иное значение стали ассоциировать с неонацистской культурой. Всё это произошло из-за выдумки участников сайта 4chan, которые шутки ради продвигали этот жест как символ ненависти и утверждали, что он передаёт буквы «wp», что означает «власть белых» (white power) (см. Рис. 2). К сожалению, в случае жеста «okay» афера была настолько успешной, что этот символ стал популярной тактикой троллинга для правых экстремистов, которые часто публиковали фото в соцсетях с таким символом. В 2019 г. австралийский неонацист Брентон Тарронт (Brenton Tarrant) использовал этот символ в суде, как искреннее выражение превосходства белых, после ареста за расстрел 50 человек в Крайстчёрче, Новая Зеландия.

При оценке этих новых символов важен контекст их использования – кто их использует, в связи с чем, и, коротко, возможен ли здесь субъективный аспект. Уголовное производство вряд ли будет начато, если этот символ использует ныряльщик. Мы можем пофантазировать и допустить, что производство начнётся, если символ использует ныряльщик – явный правый экстремист, или правый экстремист с лицензией ныряльщика. В тех случаях, когда речь идет о наказании за эти символы, необходимо воздерживаться от каких-либо спекуляций и фантазий, действовать разумно и не пытаться приплести уголовную ответственность там, где ее нет. В случае чрезмерного использования экстремистской символики в соцсетях нужно потребовать от их участников соблюдения определенной интернет- культуры и этичного поведения. Требование может исходить как от групп в социальных сетях,

¹⁹ Английское слово hoax («утка») означает лживые новости, мистификацию, выдумку, обман, переполох, вымысел, розыгрыш. “Co je to hoax?” HO@X, <https://www.hoax.cz/hoax/co-je-to-hoax>.

²⁰ 4chan – американский сайт с рисунками, запущенный 1 октября 2003 г. и изначально ориентированный на обсуждение манги и аниме.



Рис. 2: Жест «Okay», © 2020 ADL.²¹

так и напрямую от провайдера, который имеет право блокировать и затем удалять аккаунты экстремистской и радикальной направленности.

Отношение чешских судов к языку ненависти в Интернете

Из уже рассмотренных дел видно, что суды в Чехии обращают внимание на язык ненависти. Конечно, этому предшествует соответствующая работа правоохранительных органов. Борьба с языком ненависти и проявлениями экстремизма в Интернете сейчас является приоритетом.

Примером может служить дело Вацлава Клешила (Václav Kleštil), которому Высший суд Праги оставил в силе трехлетний условный приговор за одобрение в Фейсбуке теракта в мечетях в Крайстчёрче, Новая Зеландия. Суд счёл его виновным в поддержке и поощрении терроризма (Статья 312e Уголовного кодекса). Таким образом, апелляционный суд отклонил апелляцию Клешила, считавшего приговор слишком строгим. Прокурор в данном случае вообще требовал пятилетнего заключения, а это значит, что сами правоохранительные органы видят в таких преступлениях высокий риск для общества, и, следовательно, в общих интересах сурово наказывать за этот вид преступлений. Клешила судили и приговорили за комментарии в соцсети Фейсбук, где он в середине марта 2019 г. написал под статьёй в *Hospodářské noviny* о нападении, в результате которого в Новой Зеландии был убит 51 человек: «Хоть у кого-то нашлись яйца, чтобы показать, как нужно

²¹ Anti-Defamation League (ADL), “Okay Hand Gesture,” n.d., по состоянию на 21 марта 2021, <https://www.adl.org/education/references/hate-symbols/okay-hand-gesture>.

поступать с мусульманами. Хорошая работа». Статья была размещена в открытом доступе на странице газеты в Фейсбуке. При этом он совершил преступление, наказуемое до 15 лет заключения. Однако до сих пор суды первой инстанции наказывали такие действия условными сроками. Апелляционный суд согласился с этим подходом. По мнению апелляционного суда, подобных преступлений становится всё больше. «Не может быть сомнения в опасности такого поведения», сказал председатель сената Зденек Совак (Zdeněk Sovák). Тем не менее он счёл, что человек до сих пор жил честно и сожалеет о своём комментарии, поэтому приговор станет достаточным предупреждением для него. В то же время судья обратил внимание на растущее мнение, что установленное наказание от 5 до 15 лет за одобрение терроризма в печати, кино, радио, на телевидении или в общедоступных компьютерных сетях не распространяется на подобные словесные комментарии.²²

Из приведенного примера ясно, что государственный обвинитель видит общественный интерес в судебном преследовании такого языка ненависти в Интернете. Любой участник публичного виртуального общения должен понимать, что он сообщает свои взгляды не друзьям за столиком в ресторане, а всему миру; предполагаемая анонимность — лишь заблуждение, устраняющее барьеры для неэтичного поведения.

Дело Вацлава Клестила – вовсе не исключение. Уголовные суды выносили условные приговоры и в других похожих случаях. Приговор Леошу Махалеку (Leoš Machálek) Пражский городской суд вынес 11 июня 2020 г.; Махалеку прокомментировал видео расстрела мусульман в мечетях, в частности, назвав стрелка «чемпионом». Махалеку защищался в суде, утверждая, что он думал, будто на видео показано нападение союзных сил на радикальных исламистов. Махалеку разместил свой пост на сервере *drsnysvet.cz* утром 17 марта, через два дня после нападения в Новой Зеландии. Он отреагировал на статью под названием «Так нападавший выкосил новозеландскую мечеть». Конкретно он написал: «Разве плохо, если бы и я присоединился? Что эта мусульманская сволочь делает с Европой? Вот с ними и обращаются как с баранами. Они не соблюдают законы страны, принявшей их. Для меня он чемпион».²³

8 июля 2020 г. Иржи Кантор (Jiří Kantor) тоже получил самый строгий возможный условный приговор. Кантор поделился статьей о расстреле на своей странице в Фейсбуке и прокомментировал её: «Что я могу сказать – хорошая работа». В данном случае важна личность преступника. Как выяснило следствие, он с большой вероятностью тяготел к правому экстремизму, поскольку у него на теле были, в частности, готические татуировки

²² “Odvolací soud potvrdil další podmínku za schvalování vraždy 51 lidí na Facebooku. Václav Klestil dostal tři roky,” *Romea.cz*, August 19, 2020, по состоянию на 30 августа 2020, <http://www.romea.cz/cz/zpravodajstvi/domaci/odvolaci-soud-potvrdil-dalsi-podminku-za-schvalovani-vrazdy-51-lidi-na-facebooku.vaclav-klestil-dostal-tri-roky>.

²³ “Odvolací soud potvrdil další podmínku za schvalování vraždy 51 lidí na Facebooku.”

“АСАВ” и “All cops are bastards” («Все копы – ублюдки»). Мы говорим об этом лишь для иллюстрации дела, потому что Кантор защищался, в частности, утверждая, что после прочтения этой статьи он подумал: хорошо, что новозеландская полиция так быстро арестовала его, и поэтому написал комментарий о хорошей работе. Он имел в виду работу полиции и даже не думал хвалить стрелка. Однако татуировки на теле развенчали его утверждения.²⁴

Рената Пеликанова (Renata Pelikánová) тоже получила два года условно за язык ненависти в Фейсбуке. Она написала о стрелке в мечети так: «Талант. Побольше бы нам таких, как он, когда правительства ничего не делают с мусульманскими свиньями, только пасуют перед ними». Как сообщают, в своём посте она добавила, что благодарна ему за храбрость. Пеликанова ответила на пост на сервере Hoj.cz, который, по словам истца, на Фейсбуке читают больше 160 000 человек. По его мнению, тем самым она совершила преступление поддержки и поощрения терроризма, за что предусмотрено до 15 лет заключения. Прокурор Билый (Bílý) признал, что женщина ранее не была судима и вела обычную добропорядочную жизнь; но так как нужно было вынести приговор, он предлагал реальный срок.²⁵

Упомянутые выше случаи красноречиво говорят о нынешнем статусе соцсетей, где люди бездумно, часто неуместно комментируют новости. Кто-то делает это без какой-либо идеологии. В других можно предположить экстремистские наклонности. Указания на принадлежность человека, ведущего себя неподобающе, к экстремистской группе могут быть отягчающим обстоятельством, но уголовное преследование как таковое не может основываться на этих признаках. В этих случаях должен быть четко указан субъективный аспект преступления. Это касается не только его обязательного признака, но и, по возможности, мотива (причины) и цели (намерения) правонарушителя. Для тех преступлений экстремистской направленности, где дополнительный признак не требуется, этот признак следует считать отягчающим обстоятельством. Но с точки зрения уголовного права нам также нужно понимать, что уголовная ответственность не может строиться лишь на домыслах и искусственном анализе или построениях. Демонстрация мотивов и намерений правонарушителя должна основываться на доказанных и веских уликах.

²⁴ “Za schvalování útoku v Christchurchi dostal Kantor pětiletou podmínku. Hrozilo mu až 15 let,” *iROZHLAS – spolehlivé a rychlé zprávy*, July 8, 2020, по состоянию на 30 августа 2020, www.irozhlas.cz/zpravy-domov/christchurch-mesita-schvalovani-facebook-kantor_2007081017_pj.

²⁵ “Za schvalování útoku na mešity dostala žena podmínku. Žalobce pro ni žádá vězení,” *Aktuálně.cz*, June 1, 2020, по состоянию на 30 августа 2020, <https://zpravy.aktualne.cz/domaci/za-schvalovani-terorismu-dostala-zena-podminku/r~012fa30aa3e211eaa7deac1f6b220ee8/>.

В условиях нынешней пандемии COVID 19 можно ожидать дальнейшего роста киберпреступности. Статистики за 2020 год ещё нет, но взгляд на статистику предыдущих лет указывает на быстрый рост киберпреступности в Интернете (см. Рис. 3).²⁶

В ближайшие годы можно ожидать дальнейшего распространения дезинформации и языка ненависти и другими политическими лагерями, не всегда как столкновение ультралевых и ультраправых. Социальные сети становятся ареной для политических кампаний и гибридной деятельности иностранных государств, цель которых – повлиять на общественное мнение по тому или иному политическому вопросу. Одним из примеров этого стал политический спор о демонтаже памятника маршалу Коневу в Праге-6 в 2020 г. Спор о демонтаже обернулся политическим противостоянием касательно отношений с путинской Россией, что можно считать негативом для чешского общества. Однако врата истории вновь раскрылись и общество поняло, что оно всё ещё не примирилось с прошлым, и потребовало убрать памятник из-за критики бывшего Советского Союза и его политики. Этой ситуацией во время обсуждения сноса монумента воспользовалась Россия. Этот случай использовали, чтобы активизировать русскую пропаганду на чешской земле. Россия использует каждую возможность для дезинформации, даже такое мелкое событие, как демонтаж памятника, стало идеаль-



Рис. 3: Киберпреступность в Чехии, 2011-2019. © 2020 Policie ČR²⁷

²⁶ “Kyberkriminalita.”

²⁷ “Kyberkriminalita,” Policie České republiky, по состоянию на 17 сентября 2020, <https://www.policie.cz/clanek/kyberkriminalita.aspx>.

ным поводом. Дело вызвало такой международный резонанс, что даже министр иностранных дел России Сергей Лавров призвал чешских дипломатов обсудить эту тему, в которой Россия увидела грубое нарушение Договора о дружбе 1993 г. Министерство иностранных дел Чехии заявило, что перенос статуи Конева с площади в Праге-6 не нарушает никаких чешско-российских договоров. 3 апреля 2020 г. статую наконец убрали. Это прекрасно иллюстрирует, как Россия может использовать незначительное событие в своих интересах и раздуть международный скандал.

Заключение

Если критически посмотреть на статистику чешской полиции (Рис. 3), мы увидим, что киберпреступность растёт очень быстро, и эта тенденция сохранится в будущем. Это может быть связано с тем, что «виртуальный мир» стал частью нашей жизни, где мы проводим свободное время, обучаемся и даже пытаемся отдохнуть; это ещё одно место нашего самовыражения. Поэтому важно понимать, что в киберпространстве может протекать много социально бесполезной деятельности. Обществу уже ясно, что в киберпространстве может происходить множество преступлений. Действующее законодательство Чехии достаточно для противодействия языку ненависти в Интернете. Для борьбы с этим явлением нужно использовать имеющееся законодательство и качественный анализ. Она всегда будет зависеть от качества работы правоохранительных органов. Упор следует делать на оперативную работу и расследование, что составляет досудебную работу полиции. Основой успеха в судебном заседании являются подтверждённые, чётко установленные доказательства.

Сквозь призму правоохранительной деятельности киберпространство видится как новая сфера, в которой совершаются разные преступления – от малозначительных, типа мошенничества и кражи банковских данных, до самых серьёзных, таких, как терроризм или посягательство на критическую информационную инфраструктуру государства. Нынешнего законодательства может быть достаточно для преследования за язык ненависти и другие серьёзные преступления в Интернете, но необходимо продолжать разработку новых стратегий и работу над новыми международными соглашениями, которые обеспечат защиту принципов демократии в виртуальном мире. Краеугольным камнем тут может быть Конвенция о киберпреступности,²⁸ известная также как Будапештская Конвенция о киберпреступности – первый международный договор, нацеленный на гармонизацию национального законодательства о борьбе с киберпреступностью. Чехия ратифицировала эту конвенцию в 2013 г. 68 стран уже подписали, 65 из них ратифицировали её; среди них, в частности – США, Канада и большинство стран

²⁸ 104/2013 Sb. m. s Sdělení Ministerstva zahraničních věcí o sjednání Úmluvy o počítačové kriminalitě.

участниц Европейского Союза, включая Чехию. Нужно продолжать эту работу и построить сильное общество, которое продолжит реализовывать идею демократии, оставленную нам в наследство первым президентом Чехословацкой Республики Томашем Гарригом Масариком.

Будущее предполагает воспитание молодого поколения, которое необходимо знакомить с плюсами и минусами виртуального мира. Как и в дорожном движении, где запрещено переходить улицу на красный свет, в киберпространстве тоже нужно соблюдать основы этики и порядочности, а поскольку не все люди следуют общественным условностям и правилам, о соблюдении этих основ также должно позаботиться правосудие и правоохранительная система.

Примечание

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

Благодарность

Статья написана при поддержке Министерства внутренних дел Чешской Республики, проект № VI20192022117, «Выявление радикализации в контексте защиты населения и незащищённых объектов от насилия».

Об авторе

Вилим Лукаш – см. резюме на стр. 20 этого издания, <https://doi.org/10.11610/Connections.rus.20.2.02>



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](https://doi.org/10.14505//jarle.v11.4(50).26).

² Victoria V. Tsytko 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 Markopoulou, Vagelis Papakonstantinou, 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/fcapt.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. Cherniavskiy 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 употребляемое 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 узвимостей 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-чёрт, 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/indec.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, скептический 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 Канаде³² 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.

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: tavolzhanский8020@sci-univ.com

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



Дальнейшее развитие квантовых вычислений и их важность для НАТО

*Руперт Брэндмайер,¹ Йорн-Александр Хайе,²
Клеменс Войвод²*

¹ *Школа менеджмента Кутаисского международного университета,
<https://www.kiu.edu.ge>*

² *Аналитический центр JAM Systems Cyber Security Europe, <http://jamsys.eu>*

Аннотация: Первые квантовые компьютеры становятся реальностью и учёные, работающие в разных областях, мечтают воспользоваться их огромным вычислительным потенциалом. В то же время высокая производительность квантовых компьютеров несёт серьёзные риски для кибербезопасности. Можно ожидать гонки вооружений между сторонами: теми, кто защищается, пытаясь гарантировать сохранность и надёжность хранимой и передаваемой информации, и их противниками. Авторы этой статьи попытались описать ход разработки квантовых компьютеров, спрогнозировать следующие шаги и проанализировать возможное влияние будущих квантовых систем на кибербезопасность и военные операции. Сначала мы рассмотрим принципиальные отличия квантовых вычислений от классических и обнаружим, что аналогий между ними немного. Мир квантовых компьютеров уже чрезвычайно разнообразен, и мы поясняем, что и квантовые симуляторы, и универсальные квантовые компьютеры используют q-биты, но работают они совершенно по-разному. Раз уж эксперты в области безопасности изучают новые тенденции квантовых вычислений, мы рассмотрим новейшие технологии и гонку за «квантовое превосходство». Наконец, мы даём детальный анализ конкретных рисков квантовых компьютеров для традиционных систем шифрования и приходим к выводу, что такие асимметричные алгоритмы, как протокол RSA, весьма уязвимы. Угрозы квантовых вычислений для криптографии очевидны, как и проблемность защиты хранимых и передаваемых

данных в военном секторе. Но мы изучаем спектр возможностей квантовых технологий и видим, что взлом асимметричных алгоритмов шифрования – лишь одна грань; другие функции, например, квантовый алгоритм Гровера, могут революционизировать логистику вооружённых сил. Спутниковое квантовое распределение ключей – еще одна перспективная концепция, способная изменить связь между военными подразделениями. Для НАТО квантовые вычисления имеют две стороны: альянсу нужно использовать достижения и быть готовым противодействовать киберугрозам. Мы подсказываем НАТО, что нужно сделать, чтобы подготовиться к квантовой эре.

Ключевые слова: квантовые вычисления, квантовая кибербезопасность, квантовое превосходство, криптография, теория сложности вычислений, квантовая устойчивость, квантовое распределение ключей, НАТО.

Вступление

В нашу эпоху «классических вычислений» обеспечение кибербезопасности представляет собой огромную проблему. После кибератаки 2007 г. на Эстонию НАТО в 2008 г. впервые утвердила Политику киберзащиты и создала Управление киберзащиты в Брюсселе.¹ Стратегическая концепция НАТО 2010 г. признаёт важность гибридных угроз, включая кибератаки, ибо комплексные риски не ограничиваются географическими рамками.

В частности, тревожные масштабы приобретают киберугрозы в финансовом секторе. Cyber Security Ventures и IBM сообщают, что атаки на новичков в этой отрасли ради выкупа происходят каждые 14 секунд. В 2016 г. кибератак на финансовый сектор было на 64% больше, чем на другие сектора.² Взлом, то есть перехват или вмешательство в связь между двумя сторонами, представляет особый риск для финансового и других секторов. Поэтому компаниям и ведомствам рекомендуют защищать все точки доступа, реализуя ряд мер безопасности.³

С развитием технологий защиты успешные кибератаки на корпоративные, правительственные, военные сети требуют всё больше ресурсов более крупных правительственных или преступных организаций. Анализ источников кибератак показывает, что в то время, как нападения на финансовые

¹ Häly Laasme, “The Role of Estonia in Developing NATO’s Cyber Strategy,” Cicero Foundation Great Debate Paper No. 12/08 (The Cicero Foundation, December 2012), https://www.cicerofoundation.org/wp-content/uploads/Laasme_-_Estonia_NATO_Cyber_-_Strategy.pdf.

² Emma Olsson, “Report: FIs Warned to Prepare for Quantum Threats,” *bobsguide*, December 6, 2019, <https://www.bobsguide.com/guide/news/2019/Dec/6/report-fis-warned-to-prepare-for-quantum-threats>.

³ Olsson, “Report: FIs Warned to Prepare for Quantum Threats.”

учреждения по-прежнему в основном совершает небольшая группа мошенников, пытающихся вымогать деньги, разработка правительственных или военных целей ведётся в основном на государственном уровне.⁴

Даже передовой инфраструктуры цифровой защиты скоро может быть недостаточно, поскольку появление квантовых компьютеров изменит качество кибератак. По мнению ряда экономических «тяжеловесов», включая Microsoft и JPMorgan, коммерческий квантовый компьютер появится на рынке к 2030 г., возможно, уже в 2024 г.⁵ Мировой рынок квантовых вычислений к 2024 г. может превысить 10 млрд. долларов.⁶

Впрочем, многие эксперты оспаривают такие прогнозы. Исходя из необходимости множества технических разработок, они считают, что пройдут десятилетия, пока будут созданы квантовые компьютеры, способные «расколоть» нынешние системы шифрования, и не исключают, что такие попытки могут быть безуспешными. Поэтому эти эксперты убеждены, что квантовые компьютеры, представляющие угрозу для существующих методов криптографии, появятся не раньше 2030 г.⁷ Тем не менее администраторы баз конфиденциальных данных, требующих длительной защиты, например, секретных правительственных документов или старых корневых сертификатов, должны искать альтернативы асимметричным алгоритмам.⁸

Учитывая переворот в системах шифрования из-за квантовых вычислений и важность криптографии для военных операций, НАТО уже сейчас нужно начинать готовить эти системы к квантовым кибератакам. Но криптография – не единственная область, которую революционизируют квантовые технологии; другие сектора, например, дальняя связь, тоже крайне важны для НАТО. В этой статье мы пристальней рассмотрим возможные сценарии.

Далее статья построена таким образом: в разделе II а мы рассмотрим, что отличает квантовый компьютер от классического. В разделе II б рассматриваются разные типы квантовых компьютеров. В разделе II с рассмотрены аспекты технологии квантовых вычислений, а в разделе II d описан термин

⁴ J.R. Wilson, “Military Cyber Security: Threats and Solutions. U.S. Government and Military Are Taking a Lead Role in Protecting Sensitive Computers from Cyber Attack, and Solutions Finally Are on the Horizon,” *Military & Aerospace Electronics*, December 18, 2019, <https://www.militaryaerospace.com/trusted-computing/article/14073852/military-cyber-security-tactical-network>.

⁵ Olsson, “Report: FIs Warned to Prepare for Quantum Threats.”

⁶ Walid Rjaibi, Sridhar Muppidi, and Mary O’Brien, “Wielding a Double-edged Sword: Preparing Cybersecurity Now for a Quantum World” (IBM Corporation, July 2018), <https://www.ibm.com/downloads/cas/5VGKQ63M>.

⁷ Arthur Herman and Idalia Friedson, “Quantum Computing: How to Address the National Security Risk” (Washington, D.C.: Hudson Institute, 2018), <https://s3.amazonaws.com/media.hudson.org/files/publications/Quantum18FINAL4.pdf>.

⁸ John Preuß Mattsson and Erik Thormarker, “What Next in the World of Post-Quantum Cryptography?” *Ericsson Blog*, March 4, 2020, <https://www.ericsson.com/en/blog/2020/3/post-quantum-cryptography-symmetric-asymmetric-algorithms>.

«квантовое превосходство». В разделе III анализируются сложности прогнозирования будущих квантовых вычислений. Раздел IV содержит обзор возможностей квантовых компьютеров по решению задач. В разделе V рассмотрено влияние квантовых вычислений на кибербезопасность в целом. В разделе VI показано, как квантовые возможности связаны с военной сферой, а результаты наших исследований обобщены в разделе VII.

II. Наука и технология квантовых вычислений

а. Классический и квантовый компьютер

Сначала посмотрим на отличия «классических» и «квантовых» компьютеров. В классических компьютерах «биты», принимающие значения 0 или 1 («бинарная система»), представлены электрическими сигналами, а данные обрабатываются в виде линейного потока битов. В квантовых компьютерах классический бит заменён «квантовым битом», или «q-битом», причём q-бит соответствует частице, например, фотону или электрону, а не электрическому сигналу. Квантовые вычисления интересны тем, что небольшое количество q-битов позволяет хранить и обрабатывать огромный объём данных.

Подобно биту, q-бит при измерении тоже может находиться в одном из двух состояний, например, спин вверх или вниз (в квантовой механике спин частицы – характерная форма момента вращения). Так в чём же главное отличие между классическими и квантовыми вычислениями? В классическом компьютере информация обрабатывается линейно, а в квантовом компьютере – экспоненциально. Физическое объяснение этого отличия заключается в том, что микроскопические объекты могут находиться в состоянии «суперпозиции» (до наблюдения спиновое состояние электрона может быть «вверх», «вниз», или их суперпозиция), а коллективным состоянием комбинированной системы из нескольких микроскопических объектов может быть суперпозиция отдельных состояний этих объектов («запутанность»).

«Запутанность» и «суперпозиция» возможны лишь для квантовых, но не классических состояний. В квантовом компьютере ансамбль запутанных q-битов готовят так, что когерентная система находится в суперпозиции всех комбинаторных конфигураций q-битов до измерения. Запутанность делает возможным программирование многокубитных логических вентилях.⁹ Время когерентности определяется как время квантовых состояний, которые могут быть использованы в технологических целях.¹⁰

⁹ David Cardinal, “How to Make Sense of Google’s Quantum Supremacy Claim,” *ExtremeTech*, October 29, 2019, <https://www.extremetech.com/extreme/300987-google-quantum-supremacy-paper-tldr-edition>.

¹⁰ Stuart A. Wolf et al., “Overview of the Status of Quantum Science and Technology and Recommendations for the DoD” (Alexandria, Virginia: Institute for Defense Analyses, June 2019), <https://www.jstor.org/stable/resrep22809>.

Рассмотрим «знания» наблюдателя о квантовой механической системе. Есть принципиальное отличие между моментами «до измерения» и «после измерения», потому что квантовая механика – статистическая теория. В зависимости от количества запутанных q -битов, число возможных результатов наблюдения, соответствующих возможным результатам расчётов, может быть огромным. Для «расчёта», т.е. измерения, выбирают лишь одну случайную конфигурацию состояний запутанных q -битов из множества возможных результатов измерений.

Случайность результата одного наблюдения поясняется вероятностным характером квантовой механики. Квантовая неопределённость означает, что нераспределённый q -бит может принимать любое значение, позволенное суперпозицией состояний.¹¹ Без манипуляций результаты измерений спина вверх и вниз одинаково вероятны, но каждый результат связан с индивидуальной амплитудой вероятности. Квантовые вычисления соответствуют такой манипуляции q -битов, что шанс увидеть желаемый результат, скажем, спин вверх, растёт.¹² Задача состоит в том, чтобы организовать q -бит так, чтобы вероятность правильного и неправильного ответа была максимальной и минимальной, соответственно. Эксперимент нужно повторять до достижения выборки достаточного размера, гарантирующей статистическую значимость среднего результата.

Из-за запутанности q -битов процесс измерений при квантовых вычислениях может «создать» информационный контент, растущий экспоненциально с числом q -битов. Этап выбора q -битной конфигурации, при которой используется волновая природа квантовых механических состояний, можно интерпретировать как реализацию процессора, выполняющего столько операций, сколько одновременно может быть q -битных конфигураций. Эта характеристика предполагает высокую эффективность квантовых компьютеров при решении специфичных «квантово-адаптированных» математических задач.

Таким образом, квантовые процессоры в целом не «быстрее» классических процессоров при решении любых вычислительных задач, в частности, потому, что они выполняют больше тактовых циклов в единицу времени – так же определяется скорость классических процессоров. Квантовые процессоры могут превосходить классические процессоры, только если вычислительную задачу можно задать в форме, позволяющей использовать свойства квантовой механической волны q -бита. Представим, что система запутанных q -битов может быть организована так, чтобы выборочно улучшать решение математической задачи и отменять все q -битные конфигурации, соответствующие неправильным ответам, через помехи в деструктивной

¹¹ George Johnson, *A Shortcut Through Time: The Path to the Quantum Computer* (New York: Alfred A. Knopf, 2003).

¹² Eric Jodoin, “Straddling the Next Frontier; Part 1: Quantum Computing Primer,” White Paper (Bethesda, Maryland: SANS Institute, 2014), <https://www.sans.org/reading-room/whitepapers/securitytrends/paper/35390>.

фазе. В этом случае квантовый процессор может дать результат гораздо быстрее, чем классический, потому что требуемое количество квантовых операций («измерений») намного меньше числа классических операций с плавающей запятой.¹³

b. Два типа квантовых компьютеров

В предыдущем разделе мы в общем говорили о «квантовом компьютере», однако нам следует уточнить используемую здесь терминологию. В этом разделе мы даём определения (насколько возможно) разных видов квантовых вычислений. Говоря о программировании многокубитных логических вентилях в предыдущем разделе, мы по умолчанию описывали характеристику «универсального квантового компьютера». Но для двух главных классов квантовых компьютеров – «квантового симулятора» и «универсального квантового компьютера» – характерны и многие другие свойства.

Первый тип квантового компьютера – это квантовый симулятор, или квантовый эмулятор. Квантовые симуляторы можно в какой-то мере рассматривать как аналоговые системы, предназначенные для исследования специфических квантовых явлений, которые трудно исследовать экспериментально и слишком сложно – путём симуляции на классическом суперкомпьютере. Квантовые симуляторы используют квантово-механические свойства суперпозиции и запутанности. Они выполнены в виде разных физических систем, например, как симуляторы на связанных ионах или ультрахолодных атомах.

Квантовый отжиг можно описать как аналоговую версию квантовых вычислений,¹⁴ хотя квантовые отжигатели можно динамически конфигурировать («программировать»), используя программное обеспечение.¹⁵ Эти квантовые процессоры используют q -биты минимальной запутанности, но обеспечивают достаточное время когерентности для выполнения расчётов.

Квантовые отжигатели можно описать как квантовые симуляторы, использующие сверхпроводящие q -биты для определения основных состояний гамильтонианов спиновых систем адиабатным изменением внешнего магнитного поля с начального до конечного значения. Гамильтониан – это математический оператор, определяющий энергетические уровни квантовой механической системы. Термин «адиабатный» означает, что внешнее поле применяют так, что собственные функции системы (квантованные стационарные состояния системы) медленно меняются, а числа заполнения

¹³ Herman and Friedson, “Quantum Computing: How to Address the National Security Risk.”

¹⁴ Arnab Das and Bikas K. Chakrabarti, “Quantum Annealing and Analog Quantum Computation,” *Reviews of Modern Physics* 80, no. 3 (2008): 1061-1081, <https://doi.org/10.1103/RevModPhys.80.1061>.

¹⁵ Jack Krupansky, “What Is a Universal Quantum Computer?” *medium.com*, September 1, 2018, <https://jackkrupansky.medium.com/what-is-a-universal-quantum-computer-db183fd1f15a>.

состояний остаются неизменными. Могут быть разработаны разные профили адиабатного изменения для адиабатной трансформации начального гамильтониана в конечный. Основное состояние этого конечного гамильтониана соответствует решению задачи.¹⁶ При этом подходе используется квантово-механический туннельный переход через потенциальные барьеры для исследования топологии энергетической поверхности.¹⁷

Квантовые отжигатели специально созданы для поиска глобального минимума функции при многих локальных минимумах, что соответствует решению задач комбинаторной оптимизации, наподобие задачи о коммивояжёре, т.е. задач с пространством дискретного поиска. Режим подсчёта квантовых отжигателей основан на квантовых флуктуациях, а не на манипуляции (контролируемой, неслучайной запутанности) q -битов.

Первый коммерческий квантовый отжигатель в 2011 г. запустила компания D-Wave Systems. В 2015 г. сообщалось об ускорении в 108 раз на наборе сложных задач оптимизации в системе D-Wave 2X, по сравнению с моделированием отжига и квантовыми методами Монте-Карло.¹⁸ В тысячекубитной системе Advantage Pegasus P16, показанной в 2020 г., использован принцип квантового отжига для расчётов при помощи более 5000 случайно запутанных сверхпроводящих q -битов. Этот тысячекубитный адиабатный квантовый отжигатель можно, например, использовать для поиска наркотиков.¹⁹ Однако вопрос о реальных преимуществах квантовых отжигателей при решении некоторых алгоритмов оптимизации перед классическими компьютерами остаётся открытым.²⁰

Второй тип квантового компьютера – универсальный квантовый компьютер. Правда, однозначного определения такого устройства не существует.²¹ По Крупанскому,²² универсальный квантовый компьютер использует достаточно большое число q -битов для решения нетривиальных, общих задач, что отличает его от специальных и узкофункциональных квантовых компьютеров, предназначенных для решения некоторых чётко опреде-

¹⁶ P. Richerme et al., “Experimental Performance of a Quantum Simulator: Optimizing Adiabatic Evolution and Identifying Many-body Ground States,” *Physical Review A* 88, no. 1 (July 2013): 12334, <https://doi.org/10.1103/PhysRevA.88.012334>.

¹⁷ Wolf et al., “Overview of the Status of Quantum Science and Technology and Recommendations for the DoD.”

¹⁸ Hartmut Neven, “When Can Quantum Annealing Win?” *Google AI Blog*, December 8, 2015, <https://ai.googleblog.com/2015/12/when-can-quantum-annealing-win.html>.

¹⁹ Nicole Hemsoth, “Glaxosmithkline Marks Quantum Progress with D-wave,” *TheNext Platform*, February 24, 2021, www.nextplatform.com/2021/02/24/glaxosmithkline-marks-quantum-progress-with-d-wave.

²⁰ Wolf et al., “Overview of the Status of Quantum Science and Technology and Recommendations for the DoD.”

²¹ Krupansky, “What Is a Universal Quantum Computer?”

²² Krupansky, “What Is a Universal Quantum Computer?”

лѐнных вычислительных задач, т.е. квантовых симуляторов. Иными словами, квантовый компьютер делает универсальным слой цифровой обработки, преобразующий микрокоманды в импульсы для манипуляции q -битами, позволяя им работать как квантовый логический вентиль.²³ Таким образом все операции могут выполняться на одном q -бите или паре q -битов.

Поскольку «цифровой» означает «с дискретным значением», стоит отметить, что также продолжаются попытки квантовых вычислений непрерывных переменных, например, проект оптических вычислений *Xanadu*.²⁴

Согласно Крупанскому,²⁵ универсальные квантовые компьютеры делят на четыре уровня. Квантовый компьютер 1 уровня – это универсальная квантовая машина Тьюринга, неспособная выполнить сложный набор команд. Возможности универсального квантового компьютера возрастают на каждом уровне, достигая 4 уровня, для которого характерны квантовые компьютеры, намного превосходящие по ёмкости и производительности классический компьютер. Создание универсального квантового компьютера 4 уровня зависит от запутанности большого числа q -битов в течение всего времени вычислений, а это крайне сложная задача.

с. Технология квантовых вычислений

Благодаря возможностям квантовых компьютеров интерес науки и промышленности к их созданию огромен, но то же касается и базовых технических требований. Одной из основных проблем при реализации квантового компьютера является непостоянство запутанности. Чтобы квантовый процессор работал, необходимо поддерживать некоторой количество q -битов в суперпозиции состояний достаточно долгое время – время когерентности. Присущая квантовым состояниям нестабильность ведѐт к тенденции быстрого рассеивания тщательно организованной запутанности. Этот процесс называют декогеренцией.

Поскольку декогеренцию q -битов усиливают внешние помехи, квантовый компьютер должен быть изолирован от внешней среды. Лучшие условия для квантовых процессоров – вакуумные контейнеры и сверхнизкие температуры, потому что они повышают стабильность суперпозиции и запутанности q -битов.²⁶

Сейчас разрабатывают разные концепции реализации q -битов: сверхпроводимость, ионная ловушка, квантовая точка, топологическая, спиновая, триггер. Разработка одних только началась, других – уже продвинулась. Квантовые симуляторы со сверхпроводящими q -битами готовы к выходу на

²³ Richard Versluis, “Here’s a Blueprint for a Practical Quantum Computer,” *IEEE Spectrum*, March 24, 2020, <https://spectrum.ieee.org/computing/hardware/heres-a-blueprint-for-a-practical-quantum-computer>.

²⁴ Krupansky, “What Is a Universal Quantum Computer?”

²⁵ Krupansky, “What Is a Universal Quantum Computer?”

²⁶ Herman and Friedson, “Quantum Computing: How to Address the National Security Risk.”

рынок. Однако q-битную систему, которая позволит создать универсальный квантовый компьютер, ещё предстоит изобрести.

d. Квантовое превосходство

Важным термином при описании развития квантовых вычислений является «квантовое превосходство». Хотя квантовый компьютер, способный расшифровать асимметричное шифрование («премиальный квантовый компьютер», quantum prime computer), может оставаться фантастикой, некоторые эксперты верят в близость ещё одного важного шага в квантовых вычислениях: квантовое превосходство.²⁷ Квантовое превосходство будет достигнуто, когда квантовый компьютер сможет решить задачу, пусть искусственную, которую за полиномиальное время не может решить классический компьютер.

В октябре 2019 г. команда в составе группы Google AI Quantum и университетских учёных²⁸ заявила о достижении квантового превосходства случайным программированием 53 физических q-битов квантового процессора Sycamore с применением однокубитных и двухкубитных логических операций (логические вентили).

Из-за нестабильности физических q-битов требуются определённые комбинации физических q-битов для коррекции ошибок в квантовых вычислениях, чтобы получить абстрактный логический q-бит. Код коррекции ошибок в квантовых вычислениях содержит информацию, соответствующую логическому состоянию одного q-бита при запутанном состоянии ансамбля физических q-битов.²⁹ После коррекции ошибок в квантовых вычислениях процессора Sycamore запутанные физические q-биты сводятся к фракции одного логического q-бита.³⁰

Хотя на этапе программирования теоретического квантового процессора все q-биты могут быть коллективно запутаны, в Sycamore запутываются только соседние q-биты. Это ограничение можно в какой-то степени компенсировать взаимозаменяемостью q-битов, что занимает много времени и поэтому вредит когерентности.³¹ Тем не менее, согласно Эруту с коллегами,³²

²⁷ Herman and Friedson, “Quantum Computing: How to Address the National Security Risk.”

²⁸ Frank Arute et al., “Quantum Supremacy Using a Programmable Superconducting Processor,” *Nature* 574, no. 7779 (October 2019): 505-510, <https://doi.org/10.1038/s41586-019-1666-52019>.

²⁹ Giuliano Gadioli La Guardia, ed., *Quantum Error Correction. Symmetric, Asymmetric, Synchronizable, and Convolutional Codes*, Quantum Science and Technology Series (Springer, 2020).

³⁰ Preuß Mattsson and Thormarker, “What Next in the World of Post-Quantum Cryptography?”

³¹ Cardinal, “How to Make Sense of Google’s Quantum Supremacy Claim.”

³² Arute et al., “Quantum Supremacy Using a Programmable Superconducting Processor.”

для решения численных задач, выполняемых процессором Sycamore примерно за 200 секунд, суперкомпьютеру IBM Summit понадобится 10 000 лет. В IBM сразу же опровергли утверждение Эрута и его коллег,³³ заявив, что дооснащение Summit вторичной памятью сократит время моделирования цепей Sycamore до 2,5 дней, что достаточно быстро, чтобы развеять заявление о превосходстве Sycamore.³⁴

Спор о взгляде на квантовое превосходство Sycamore предвосхищает проблемы толкования и оценки достоверности результатов квантовых вычислений, которые возникнут при достижении этапа невозможности проверки этих результатов с помощью обычных суперкомпьютеров.³⁵

Стоит отметить, что обоснованность термина «квантовое превосходство» в последнее время подвергаются сомнению, поскольку он предполагает очень маловероятный сценарий, что квантовые компьютеры в целом смогут превзойти классические компьютеры, в то время как будущие квантовые компьютеры могут быть эффективнее классических компьютеров только при решении специфических задач. Поэтому для описания прогресса в квантовых вычислениях рекомендуются выражения наподобие «квантовое преимущество» и «квантовая практичность».³⁶

III. Прогноз развития квантовых вычислений

Скорость прогресса квантовых вычислений предугадать очень сложно. Одна из причин такой неопределённости заключается во множестве рассматриваемых в настоящее время q-битных технологий. Чтобы решить, какие q-битные архитектуры окажутся успешными в будущем, нужно ответить на множество теоретических и практических вопросов. Ещё одним фактором является вопрос о том, какое влияние окажет наличие квантовых компьютеров раннего поколения на конструкцию последующих поколений. Наконец, непросто понять, в каком масштабе другие грядущие инновации, такие как искусственный интеллект, могут повлиять на эволюцию квантовых компьютеров.³⁷

³³ Arute et al., “Quantum Supremacy Using a Programmable Superconducting Processor.”

³⁴ Edwin Pednault et al., “Leveraging Secondary Storage to Simulate Deep 54-qubit Sycamore Circuits,” *arXiv*, 2019, <https://arxiv.org/abs/1910.09534>.

³⁵ “Google’s Search for Quantum Supremacy,” *ID Quantique*, March 20, 2018, <https://www.idquantique.com/googles-search-for-quantum-supremacy>.

³⁶ Scott Fulton III, “What Happened to Quantum Supremacy? Quantum Computing Needs a New Success Metric,” *ZDNet*, November 2, 2020, <https://www.zdnet.com/article/what-happened-to-quantum-supremacy-quantum-computing-needs-a-new-success-metric>.

³⁷ Herman and Friedson, “Quantum Computing: How to Address the National Security Risk.”

Собственно, взаимное усиление обеих научных дисциплин не исключено, поскольку квантовые вычисления также окажут влияние на искусственный интеллект, выполняя определенные операции намного быстрее классических компьютеров. Этот прогноз стимулировал появление междисциплинарного направления «Квантовый искусственный интеллект» (Quantum Artificial Intelligence, QAI). Машинное обучение является подотраслью искусственного интеллекта, а одна из дисциплин QAI – последующее квантовое машинное обучение.

В 2019 г. Институт оборонных исследований (Institute for Defense Analyses, IDA) выполнил для Министерства обороны США всесторонний анализ возможного влияния квантовых технологий на военно-политические интересы.³⁸ Согласно Вулфу с коллегами,³⁹ в развитии цифровых квантовых вычислений будет три этапа: квантовые вычисления компонентов (component quantum computation, CQC), квантовые вычисления среднего масштаба с шумами (noisy intermediate-scale quantum computing, NISQ), и устойчивые к ошибкам квантовые вычисления (fault-tolerant quantum computing, FTQC). Для сверхпроводящих q-битов и q-битов со связанными ионами достигнут этап NISQ. Альтернативные архитектуры, например, квантовые точки, всё ещё находятся на этапе CQC. Ни одна q-битная технология пока что не приблизилась к FTQC.

Математик Питер Шор в 1994 г. предложил алгоритм квантового компьютера для факторизации целых чисел в полиномиальный срок.⁴⁰ Для реализации алгоритма Шора для факторизации чисел, слишком больших для классических суперкомпьютеров, нужен процессор уровня FTQC с примерно 106 физическими q-битами. По мнению Грумблинг и Горовица,⁴¹ серьёзно ожидать появления такого премиального квантового компьютера в настоящее время не стоит, его реализация может занять не менее 20 лет.

Остаётся увидеть, пройдёт ли проверку реальностью закон Невена, по которому производительность квантовых компьютеров повышается с молниеносной дважды экспоненциальной скоростью по сравнению с классическими компьютерами. Можно сказать, что закон Невена описывает эволюцию числа q-битов в квантовых процессорах, по аналогии с законом Мура, предопределяющим число транзисторов в обычных процессорах.⁴²

³⁸ Wolf et al., “Overview of the Status of Quantum Science and Technology and Recommendations for the DoD.”

³⁹ Wolf et al., “Overview of the Status of Quantum Science and Technology and Recommendations for the DoD.”

⁴⁰ Peter W. Shor, “Algorithms for Quantum Computation: Discrete Logarithms and Factoring,” in *Proceedings of the 35th Annual Symposium on Foundations of Computer Science* (IEEE Comput. Soc. Press, 1994), 124-134.

⁴¹ Emily Grumblin and Mark Horowitz, eds., *Quantum Computing: Progress and Prospects* (Washington, DC: The National Academies Press, 2019).

⁴² Preuß Mattsson and Thormarker, “What Next in the World of Post-Quantum Cryptography?”

IV. Пригодность квантовых компьютеров для решения конкретных задач

Квантовые компьютеры в целом существенно не превзойдут классические компьютеры при решении задач, но преимущество квантовых компьютеров над классическими будет прямо зависеть от характера решаемых задач. Доказано, что квантовые алгоритмы потенциально могут массово превзойти классические алгоритмы при решении небольшой группы задач. Однако для решения многих других задач квантовые компьютеры, похоже, не дадут особых преимуществ.⁴³ Квантовые компьютеры смогут дать фору классическим компьютерам при выяснении глобальных свойств математических систем. Также в этом разделе мы покажем, что повышение эффективности вычислений при помощи квантовых алгоритмов зависит от характера конкретной задачи.

Прежде, чем продолжить, нам нужно дифференцировать задачи поиска и проверки решений. Для задач класса сложности P решения могут быть найдены и проверены за полиномиальное время. Решение задач класса «недетерминированное полиномиальное время» (NP) нельзя найти за полиномиальное время, но можно за полиномиальное время проверить. Задачу называют NP -полной, если никакие алгоритмы полиномиального времени, ни классические, ни квантовые, не обеспечивают известного решения.

Одним из примеров «квантовой задачи» является разложение n -значного числа на простые множители. Решение, очевидно, можно проверить за полиномиальное время. Однако при лучшем известном алгоритме для классических компьютеров количество шагов возрастает экспоненциально с n . Поэтому считают, что задача факторинга относится к классу NP вне P . Квантовый алгоритм Шора определяет задачу факторинга как глобальное свойство числа и решает эту задачу за полиномиальное время (алгоритм масштабируется с n^2).⁴⁴ Следовательно, задача факторинга не является NP -полной.

Но такая производительность алгоритма Шора не означает, что квантовые алгоритмы всегда дадут экспоненциальное ускорение при поиске глобальных свойств математических систем. Хороший пример – задача о коммивояжёре, тоже относящаяся к глобальным свойствам систем. В первом определении задачи о коммивояжёре (travelling salesman problem, TSP), далее – TSP1, цель – найти маршрут, соединяющий все n узлов сети, не превы-

⁴³ Scott Aaronson, “The Limits of Quantum Computers,” *Scientific American* 298, no. 3 (March 2008): 62-69; Chad Orzel, “What Sorts of Problems Are Quantum Computers Good for?” *Forbes*, April 17, 2017, <https://www.forbes.com/sites/chadorzel/2017/04/17/what-sorts-of-problems-are-quantum-computers-good-for>.

⁴⁴ Shor, “Algorithms for Quantum Computation.”

шающий заданной длины L . Если S — число маршрутов, то S растёт экспоненциально с n . При классическом подходе в среднем нужно $S/2$ попыток найти маршрут, соответствующий условию.

Для понимания усилий по проверке решения TSP важно обратить внимание на конкретную постановку задачи: если она сформулирована как в TSP1, то проверка решения, очевидно, может быть выполнена за полиномиальное время. Квантовый алгоритм Гровера может выявить связь примерно в $S^{1/2}$ шагов, что значительно лучше, чем при классическом подходе, но не сводит экспоненциальное масштабирование к полиномиальному масштабированию. Этот результат показывает, что TSP1 — задача того же типа, что и поиск в неупорядоченной базе данных. Хотя TSP1 касается глобальных свойств сети, классический или квантовый алгоритм решения TSP1 за полиномиальное время пока что не найден, следовательно, TSP1 считается NP-полной задачей.

Другой вариант TSP — поиск кратчайшего пути между n узлами (далее — TSP2). Чтобы ответить на вопрос о кратчайшем пути, недостаточно проверить, соответствует ли длина одного из предлагаемых решений условию снижения определенного предела. Нужно также сравнить длины всех возможных путей. Поэтому даже известный квантовый алгоритм не может проверить решение TSP2 за полиномиальное время. TSP2, вероятно, не NP-полная, но принадлежит к более широкому классу PSPACE, что включает задачи, которые может решить классический компьютер с полиномиальной памятью, возможно, требующий экспоненциального масштабирования времени. PSPACE включает классы сложности P и NP.⁴⁵

Так что же отличает TSP1 от задачи факторинга? Алгоритм Шора использует определённые математические свойства составных чисел и их множителей, которые можно применять для реализации конструктивных и деструктивных моделей вмешательства на квантовом компьютере, что и даёт правильный ответ. Неправильные ответы нейтрализуются деструктивным вмешательством. NP-полные задачи типа TSP1, похоже, не позволяют создавать такие механизмы вмешательства.

Обсуждая классы сложности, следует, однако, иметь в виду, что доказательств отсутствия квантовых или даже классических алгоритмов для решения NP-полных задач пока предъявлено не было. Тем не менее имеется явная аналогия в дифференциации классов P и NP с одной стороны и классов NP и NP-полной с другой. Считают, что $P \neq NP$, потому что не известны никакие классические алгоритмы, способные решать определённые задачи, например, факторинга, за полиномиальное время. Аналогично, выходит, что $NP \neq NP$ -полной, потому что ещё не найдены никакие классические или квантовые алгоритмы, позволяющие решать задачи типа TSP1 за полиномиальное время.

⁴⁵ Aaronson, “The Limits of Quantum Computers.”

V. Квантовые вычисления и безопасность

В нашу эру классических вычислений в основном применяют два класса алгоритмов шифрования: симметричные и асимметричные. Одним из распространённых симметричных протоколов является Передовой стандарт шифрования (Advanced Encryption Standard, AES), поддерживающий три размера ключей: 128, 192 и 256 битов. Область применения симметричных алгоритмов – защита больших объёмов данных, например, шифрование баз данных.

При асимметричном шифровании применяют так называемые открытые и закрытые ключи для шифрования и дешифрования данных, соответственно. Автоматически связанные ключи генерируют алгоритмы шифрования с так называемой необратимой функцией. Известный асимметричный подход – протокол Rivest, Shamir, Adleman (RSA), использующий тот факт, что факторизация больших простых чисел Био на классических компьютерах занимает слишком много времени.⁴⁶ Асимметричные методы медленнее симметричных, но не требуют закрытых каналов для обмена ключами, если зашифрованной информацией обмениваются две или более сторон, как это требуется при симметричных алгоритмах.⁴⁷

Квантовые вычисления представляют угрозу в основном для асимметричных систем шифрования, основанных на простых числах, например, квантовый алгоритм Шора⁴⁸ можно использовать для взлома шифрования RSA, в то время как симметричные протоколы не используют факторизацию простых чисел и считаются по-прежнему безопасными. Будущий квантовый компьютер, использующий алгоритм Шора и достаточно мощный, чтобы вскрыть 2048-битную реализацию протокола RSA меньше чем за день, не сможет расшифровать данные, защищённые протоколом AES-128.⁴⁹

В 1996 г. математик Лов Кумар Гровер представил квантовый алгоритм для поиска в неупорядоченных базах данных.⁵⁰ Задача поиска в базах данных соответствует ситуации, когда единственный способ решить задачу – угадывать входной аргумент «чёрного ящика» функции и проверять правильность результата. Метод Гровера существенно уменьшает среднее количество попыток для поиска отдельной позиции в базе данных с S позиций

⁴⁶ Vasileios Mavroeidis, Kamer Vishi, Mateusz D. Zych, and Audun Jøsang, “The Impact of Quantum Computing on Present Cryptography,” *International Journal of Advanced Computer Science and Applications (IJACSA)* 9, no. 3 (2018), <https://arxiv.org/pdf/1804.00200.pdf>.

⁴⁷ Rjaibi, Muppidi, and O’Brien, “Wielding a Double-edged Sword.”

⁴⁸ Shor, “Algorithms for Quantum Computation.”

⁴⁹ Preuß Mattsson and Thormarker, “What Next in the World of Post-Quantum Cryptography?”

⁵⁰ Lov Kumar Grover, A Fast Quantum Mechanical Algorithm for Database Search,” in *STOC’96: Proceedings of the 28th Annual ACM Symposium on the Theory of Computing*, July 1996, 212-219, <https://doi.org/10.1145/237814.237866>; Mavroeidis, Vishi, Zych, and Jøsang, “The Impact of Quantum Computing on Present Cryptography.”

(S соответствует размеру области функции) до $S^{1/2}$, по сравнению с $S/2$ при классических вычислениях.

Но главная сложность расшифровки симметричного стандарта типа AES в том, что размер базы данных S растёт экспоненциально с длиной ключа. Подход Гровера не меняет это свойство масштабирования. Алгоритм Гровера можно применять для декодирования данных, зашифрованных по протоколу AES, поиском ключа, соответствующего небольшому числу пар «сообщение-шифртекст». Например, чтобы расшифровать алгоритм AES-128, нужно последовательно выполнить около 265 обратимых оценок блочного шифра, поскольку ни один эффективный метод параллелизации не представляется реальным, и квантовое вычисление функции считается более долгим, чем классическое.⁵¹

Риск нынешнего широкого применения асимметричного шифрования стимулировал разработку так называемых «квантово-безопасных», или «постквантовых» алгоритмов шифрования. Эти алгоритмы предназначены для защиты данных на классических компьютерах от попыток расшифровки при помощи квантовых компьютеров.⁵²

Правительство США недавно объявило, что используемый в настоящее время для шифрования данных Коммерческий набор алгоритмов национальной безопасности (Commercial National Security Algorithm Suite) после 2024 г. будут заменять квантово-безопасные алгоритмы, а это значит, что переход завершится не ранее 2030 г.⁵³ Поскольку секретность данных должна гарантироваться не менее 50 лет, правительство США, видимо, не ожидает появления квантовых компьютеров, способных расшифровать, например, протокол RSA-3072, в ближайшие десятилетия.⁵⁴

Тем не менее новые квантово-безопасные функции уже активно исследуют. Две системы шифрования с открытым ключом, которые могут заме-

⁵¹ Preuß Mattsson and Thormarker, “What Next in the World of Post-Quantum Cryptography?”

⁵² Preuß Mattsson and Thormarker, “What Next in the World of Post-Quantum Cryptography?”; Thomas Pöppelmann, “Efficient Implementation of Ideal Lattice-Based Cryptography,” Dissertation (Bochum, Germany: Ruhr-University Bochum, Faculty of Electrical Engineering and Information Technology, June 2015), www.seceng.ruhr-uni-bochum.de/media/attachments/files/2019/11/diss_thomas_poeppelmann.pdf; Petros Wallden and Elham Kashefi, “Cyber Security in the Quantum Era,” in *Communications of the ACM* 62, no. 4 (April 2019): 120-128, <https://doi.org/10.1145/3241037>; Anne Broadbent and Christian Schaffner, (2016): “Quantum Cryptography beyond Quantum Key Distribution,” *Designs, Codes and Cryptography* 78 (2016): 351-382, <https://doi.org/10.1007/s10623-015-0157-4>.

⁵³ Jake Tibbetts, “Quantum Computing and Cryptography: Analysis, Risks, and Recommendations for Decisionmakers,” Technical Report LLNL-TR-790870 (Lawrence Livermore National Laboratory, September 20, 2019), <https://cgsr.llnl.gov/content/assets/docs/QuantumComputingandCryptography-20190920.pdf>.

⁵⁴ Mattsson and Thormarker, “What Next in the World of Post-Quantum Cryptography?”

нить протокол RSA – криптография на основе стохастической решётки и идеальной кристаллической решётки. Безопасность этих методов основана на неразрешимости задач вычисления на стохастической и идеальной решётке, соответственно. Схемы на основе решётки дали большое разнообразие инструментов шифрования, в том числе совершенно новых. Среди них – алгоритмы шифрования на основе решётки, считающиеся постквантовыми методами.⁵⁵

Другой метод с применением открытых ключей – обмен ключами на основе суперсингулярной изогенности Диффи-Хеллмана (SIDH). SIDH позволяет создать секретный ключ между двумя ранее не связанными сторонами по незащищенному каналу связи. Применяя, при сжатии, 2688-битные открытые ключи на 128-битном квантовом уровне безопасности, SIDH использует один из наименьших размеров ключей для всех постквантовых алгоритмов.⁵⁶

Много исследований также посвящено альтернативам квантово-безопасной криптографии, разработанным для классических компьютеров. Один из вариантов – квантовое распределение ключей (quantum key distribution, QKD), что может дать путь реализации обмена незаверенными ключами в квантовой сети. QKD обеспечивает теоретически безопасное шифрование информации, т.е. система шифрования не может быть взломана, даже если шпион имеет неограниченные возможности для вычислений.⁵⁷

Для пояснения мы кратко вернёмся к понятиям квантовой неопределённости и суперпозиции состояний, касающимся нераспределённого q-бита. Появление квантовой частицы устраняет суперпозицию и означает, что суперпозиция переходит в одно состояние. Этот факт можно использовать для обеспечения секретности связи, поскольку подслушивание или вмешательство человека требуют измерения частицы и последующего прекращения суперпозиции состояний. Поэтому такие попытки шпионажа или манипуляции можно будет сразу же обнаружить.⁵⁸

Поскольку принцип QKD по своей природе физический, а не математический, квантовые компьютеры не угрожают защите квантовых сетей при помощи QKD. Из-за высокой стоимости QKD можно будет использовать

⁵⁵ Gary Stevens, “Post Quantum Cryptography: Data Security in a Post-Quantum World,” *Security Boulevard*, April 14, 2020, <https://securityboulevard.com/2020/04/post-quantum-cryptography-data-security-in-a-post-quantum-world/>; Pöppelmann, “Efficient Implementation of Ideal Lattice-Based Cryptography.”

⁵⁶ Stevens, “Post Quantum Cryptography: Data Security in a Post-Quantum World.”

⁵⁷ Andrew Lance, John Leiseboer, and Thomas Symul, “What Is Quantum Key Distribution (QKD)?” White Paper (Quintessence Labs, 2020), www.quintessencelabs.com/wp-content/uploads/2020/12/What-is-Quantum-Key-Distribution-QKD-whitepaper.pdf.

⁵⁸ Jodoin, “Straddling the Next Frontier.”

только для краткосрочной защиты самых важных линий. Будущая спутниковая сеть QKD сможет обеспечить безопасный обмен и передачу ключей в мировом масштабе.⁵⁹

Однако применение QKD в других областях криптографии, кроме квантовой сети, маловероятно, потому что понадобится новое оборудование, а затраты будут высокими. Белая книга британского правительства от марта 2020 г.⁶⁰ не рекомендует крупных инвестиций в исследования QKD из-за довольно узкого диапазона применения.⁶¹

В этой статье мы говорили о функциях, разработке и производительности оборудования для квантовых вычислений, но нужно рассмотреть и программное обеспечение, особенно программы, предназначенные для использования на квантовых процессорах. Уже упоминались алгоритмы Шора и Гровера и ясно, что понадобится много лет для применения обеих процедур на универсальных квантовых компьютерах. Однако применение будущих квантовых процессоров на классических компьютерах можно имитировать уже сейчас, имеются и прототипы квантовых устройств для тестового кода. Активно разрабатываются языки квантового программирования. Для ознакомления с прогрессом в этой области мы отсылаем читателя к работе Гархвал с коллегами.⁶²

VI. Военное применение квантовых компьютеров

В статье для «больших дебатов» Фонда Сисего в 2012 г. эстонский эксперт по безопасности Хяли Лаасме рассмотрел возможности и проблемы квантовых вычислений для НАТО.⁶³ Он рекомендовал «НАТО быть готовым к квантовой эре, обсуждение возможных технологических сдвигов и их последствий должно начаться как можно скорее, особенно учитывая медленный прогресс НАТО в кибернетике».

Математические открытия типа алгоритма Шора оказались очень важны для криптографии. Закрытие связи между воинскими частями, а также секретных данных, например, информации о местонахождении ракет, на центральных серверах – очень высокий приоритет для военных операций. Поэтому обеспечение квантовой устойчивости является приоритетом кибернетиков любого национального оборонного ведомства.

⁵⁹ Lance, Leiseboer, and Symul, “What Is Quantum Key Distribution (QKD)?”

⁶⁰ National Cyber Security Center, UK Government, “Quantum Security Technologies,” March 24, 2020, www.ncsc.gov.uk/whitepaper/quantum-security-technologies.

⁶¹ Mattsson and Thormarker, “What Next in the World of Post-Quantum Cryptography?”

⁶² Sunita Garhwal, Maryam Ghorani, and Amir Ahmad, “Quantum Programming Language: A Systematic Review of Research Topic and Top Cited Languages,” *Archives of Computational Methods in Engineering* 28 (2021): 289-310, <https://link.springer.com/article/10.1007/s11831-019-09372-6>.

⁶³ Laasme, “The Role of Estonia in Developing NATO’s Cyber Strategy.”

Технология, которая способна защитить военную связь и уже была опробована в 2018 г., основана на квантовой механике: спутниковое QKD.⁶⁴ Хотя британское правительство видит потенциал QKD для защиты важных линий связи,⁶⁵ эта технология весьма интересна для разведслужб. Идут исследования данного вопроса, в частности, в Китае, с обеих сторон: применение QKD для шифрования собственных данных и поиск путей получения информации при использовании шифрования QKD противником.⁶⁶ Тем не менее исследование IDA показало, что проблемы аутентификации и наличие безопасных неклассических альтернатив помешают прорыву в военном применении QKD в ближайшее время.⁶⁷

Кроме изучения возможностей QKD для закрытой связи и его угроз для разведки, развитие постквантовых методов шифрования касается и вооружённых сил, обеспечивая достаточно безопасные каналы связи и базы данных для ведения военных операций в квантовую эру.

Хотя квантовые алгоритмы вряд ли когда-либо смогут решать NP -полные задачи за полиномиальное время, ускорение решения TSP1 с $S/2$ шагов вычисления, нужных классическим компьютерам, до $S^{1/2}$ шагов при помощи квантового алгоритма Гровера, существенно. Как мог бы повлиять на военные операции будущий универсальный квантовый компьютер, способный решать высокоразмерные NP -полные задачи с масштабированием $S^{1/2}$? Характер TSP1 уже показывает, что метод Гровера может повлиять на военную логистику. Квантовый компьютер может быть способен управлять танками и машинами обеспечения, военными кораблями и самолётами намного эффективней, оптимизируя маршруты между военными базами.

Однако, согласно исследованию IDA, схемы квантовой оптимизации, например, алгоритм Гровера, вряд ли дадут достаточно большое преимущество над классическими эвристическими подходами, чтобы играть важную роль, кроме очень больших проблем оптимизации.⁶⁸ Кроме того, квантовая оптимизация по методу Гровера требует FTQC и большой квантовой памяти, что может появиться ещё не скоро.

Квантовые отжигатели при решении задач комбинаторной оптимизации используют принцип, отличный от алгоритма Гровера, а некоторые системы

⁶⁴ Wallden and Kashefi, "Cyber Security in the Quantum Era;" Sheng-Kai Liao et al., "Satellite-Relayed Intercontinental Quantum Network," *Physical Review Letters* 120, 30501 (January 2018), <https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.120.030501>.

⁶⁵ National Cyber Security Center, UK Government, "Quantum Security Technologies."

⁶⁶ Eleni Diamanti, Hoi-Kwong Lo, Bing Qi, and Zhiliang Yuan, "Practical Challenges in Quantum Key Distribution," *npj Quantum Information* 2, Article number 16025 (2016), <https://doi.org/10.1038/npjqi.2016.25>.

⁶⁷ Wolf et al., "Overview of the Status of Quantum Science and Technology and Recommendations for the DoD."

⁶⁸ Wolf et al., "Overview of the Status of Quantum Science and Technology and Recommendations for the DoD."

уже есть на рынке. Тем не менее квантовое преимущество этих устройств всё ещё сомнительно.⁶⁹

Шахматы по сути имитируют индийское поле боя VI века, и умение играть в стратегические игры типа шахмат остаётся весьма важным для понимания военной тактики. Шахматы или го как игры подобны TSP2; они ставят задачи PSPACE, выходящие за рамки NP. Вопрос производительности квантовых алгоритмов в стратегических играх прямо ведёт к QAI. Собственно, шахматы были главным объектом моделирования искусственного интеллекта с появления этой отрасли. Традиционные шахматные программы используют для поиска и оценки экспертные знания. Шахматная программа AlphaGo Zero реализует идею обучения с обратной связью – подотрасли машинного обучения, которое само является подотраслью искусственного интеллекта.⁷⁰ Не полагаясь на опыт шахматистов, путём обучения с обратной связью в ходе игры, AlphaGo Zero в 2018 г. совершила революцию, превзойдя обычные шахматные программы.

Прогресс исследований «классического» искусственного интеллекта позволяет спросить, может ли QAI, в частности, квантовое машинное обучение, придать новый импульс расчёту стратегических игр. Последние исследования показывают, что реализация решений за полиномиальное время для стратегических игр через квантовые алгоритмы невозможна, но существенное ускорение по сравнению с классическими алгоритмами всё ещё представляется достижимым, аналогично сценарию TSP1.⁷¹

Исследования IDA также показывают, что одна из главных сложностей квантового машинного обучения – необходимость работы с большими массивами учебной информации.⁷² Поэтому необходим существенный прогресс в разработке QRAM (квантовый эквивалент динамической оперативной памяти, DRAM) для реализации алгоритмов QAI, например, для игры в шахматы – способность соперничать с реализациями классического машинного обучения, наподобие AlphaGo Zero.

На схеме ниже в виде иерархической структуры показано, как квантовые вычисления могут влиять на военную сферу. Если выделить четыре слоя, дифференцируемые по росту сложности, три направления (кибербезопасность, логистика цепей поставки, анализ данных) особо интересны для военных. На схеме показано, как разные сектора зависят от таких применений, как машинное обучение с учителем, и как сами применения связаны с глав-

⁶⁹ Wolf et al., “Overview of the Status of Quantum Science and Technology and Recommendations for the DoD.”

⁷⁰ David Silver et al., “A General Reinforcement Learning Algorithm That Masters Chess, Shogi, and Go through Self-play,” *Science* 362, no. 6419 (December 2018): 1140-1144, <https://doi.org/10.1126/science.aar6404>.

⁷¹ Aaronson, “The Limits of Quantum Computers.”

⁷² Wolf et al., “Overview of the Status of Quantum Science and Technology and Recommendations for the DoD.”

ными дисциплинами квантовых вычислений. Разработка лекарств и финансовые оценки – лишь два примера гражданских отраслей, которые изменяют квантовые вычисления.

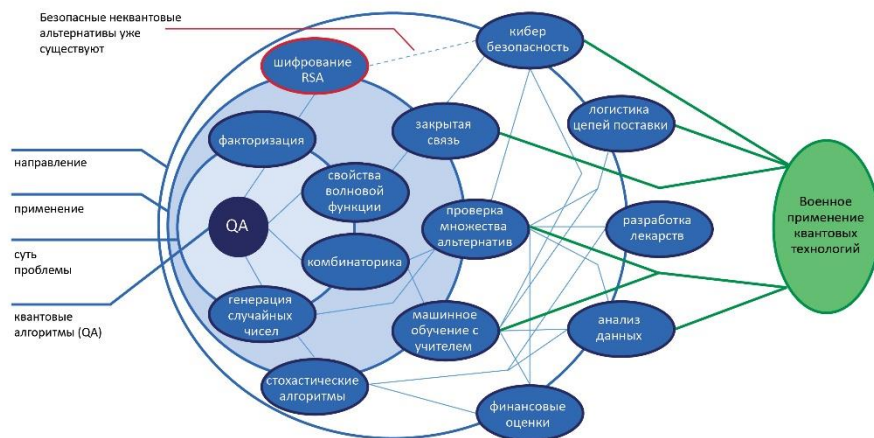


Рис. 1: Потенциальное влияние квантовых вычислений на военную сферу.

Рис. 1 даёт графическое представление о возможном влиянии квантовых вычислений на избранные области военной сферы. Как показано в этом разделе, кибербезопасность и логистика цепей поставок – направления, важные для вооружённых сил, и они же, вероятно, существенно изменятся благодаря развитию квантовых вычислений. Анализ данных – третье направление, интересное для оборонных ведомств, например, в контексте получения информации о военной деятельности противника, что тоже существенно зависит от развития квантовых алгоритмов. Разведывательные спутники собирают огромный объём данных, и квантовые компьютеры, например, в контексте применения QAI, могут помочь с извлечением ценной информации.

VII. Выводы

Во II разделе мы дали общий обзор научно-технической базы разработки квантовых компьютеров в качестве фундамента для обсуждения в последующих разделах. В III разделе коротко описаны будущие варианты квантовых вычислений, в частности, показаны трудности, усложняющие любые прогнозы. Прежде чем обсудить конкретные результаты квантовой эры для военных в VI разделе, мы сделали небольшой экскурс в теорию сложности вычислений (раздел IV), чтобы в целом рассмотреть свойства квантовых алгоритмов. IV раздел касается исключительно будущих универсальных квантовых компьютеров, поскольку они предполагают реализацию кодов, подоб-

ных сформулированным Шором и Гровером. Это логически ведёт к рассмотрению влияния будущих квантовых устройств на кибербезопасность в V разделе.

Эксперты не едины в оценке сроков, когда универсальный квантовый компьютер сможет, например, взломать шифрование RSA-2048 при помощи алгоритма Шора. Эта задача требует поддержания запутанности большего числа q -битов, что представляет огромную техническую проблему. Для создания такого устройства нужен существенный прогресс фундаментальной и прикладной науки, что влечёт значительную неопределённость реальной оценки развития квантовых вычислений. Правительство США не ожидает появления премиального квантового компьютера в ближайшие десятилетия.

Тем не менее ожидаемая способность такого компьютера взламывать ключи шифрования уже сейчас представляет огромный интерес для правительственных ведомств (см. раздел V). Так, квантовые симуляторы производства D-Wave Systems могут решать некоторые задачи оптимизации быстрее классических компьютеров и уже есть на рынке. О важности таких квантовых устройств для НАТО свидетельствует тот факт, что покупателями D-Wave Systems являются Lockheed Martin и Лос-Аламосская национальная лаборатория.

Потенциальная высокая эффективность квантовых симуляторов при решении задач комбинаторной оптимизации делает их привлекательными для применения не только в военной промышленности, но и в тыловом обеспечении войск. Однако пока ещё не ясно, дают ли эти системы реальное квантовое преимущество.⁷³ Поэтому НАТО следует приступить к изучению рисков и возможностей, связанных с квантовыми симуляторами, для своих операций.

Потенциальное влияние квантовых симуляторов на два других направления, показанные на Рис. 1, как важные для военных – кибербезопасность и анализ данных – менее очевидно. Однако эти два направления существенно изменятся, когда универсальные квантовые компьютеры появятся на рынке.

Квантовые компьютеры, способные взламывать традиционные системы шифрования, могут появиться лишь через десятилетия, но НАТО уже сейчас рекомендуется инвестировать в квантовую устойчивость своих компьютеров и сетевой инфраструктуры. Это может включать применение случайных чисел с полной энтропией, генерируемых квантовыми устройствами, для шифрования и применение более длинных ключей для симметричных алгоритмов, наподобие AES. Длинные и полностью рандомизированные симметричные ключи помогают защитить хранимые или восстановленные

⁷³ Wolf et al., “Overview of the Status of Quantum Science and Technology and Recommendations for the DoD.”

ключи, делая их квантово-безопасными. Криптографическая гибкость администраторов ключей предусматривает совместимость с более длинными ключами и квантово-стойкими алгоритмами. Приоритетом должна быть замена протокола RSA, например, квантово-безопасными альтернативами, такими, как криптография на основе кристаллической решётки или SIDH. Также рекомендуется применять защищённые линии связи между узлами управления при помощи QKD и (или) квантово-безопасные алгоритмы. Решения с обменом ключами, например, QKD, тоже нужно исследовать на предмет пригодности для защиты дальней связи.⁷⁴

Применение квантовых компьютеров для обеспечения тактических операций в ближайшее время не выглядит реальным, поскольку стратегические игры наподобие шахмат соответствуют задачам PSPACE, выходящим за рамки NP. Однако впечатляющий результат применения машинного обучения AlphaGo Zero для шахмат показывает, что QAI, как подотрасль квантового машинного обучения, может применяться для моделирования сценариев боя раньше, чем ожидали многие эксперты, хотя необходимость прорывов, в частности, в разработке QRAM по-прежнему является серьезным препятствием для использования QAI.

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.

⁷⁴ “Quantum-Safe Security,” *Quintessence Labs* (Canberra), 2021, <https://www.quintessencelabs.com/quantum-safe-cyber-security>.

Об авторах

Руперт Андреас Брэндмайер изучал экономику (специалист) и археологию (бакалавр) в Университете Людвиг-Максимилиана, Мюнхен. Получил степень доктора за анализ результатов аутсорсинга в информационных технологиях. Профессор Школы менеджмента Кутаисского международного университета.

Электронная почта: rupert.andreas.brandmeier@gmail.com

Йорн-Александр Хайе – партнёр JAM Systems Cyber Security Europe OÜ (Таллинн, Эстония), более 28 лет проработавший директором и генеральным директором международных компаний. Офицер связи Бундесвера (в запасе), служил в стране и за рубежом.

Электронная почта: jheye@jamsys.eu

Клеменс Войвод – научный сотрудник JAM Systems Cyber Security Europe OÜ (Мюнхен). Также сотрудничает с кафедрой химии Мюнхенского Технического университета. Доктор наук в области теоретической химии Мюнхенского Технического университета.

Электронная почта: clemens.woywod@ch.tum.de

Connections: The Quarterly Journal

Правила подачи рукописей


Connections принимает рукописи объёмом от 2000 до 5000 слов, написанные понятным языком для целевой аудитории информированных специалистов-практиков и учёных в области обороны и безопасности. Все рукописи следует подавать в редколлегию *Connections* на электронную почту PFCpublications2@marshallcenter.org или загружать на веб-сайт журнала, <https://connections-qj.org>. В них должно быть указано имя автора, нынешнее место его работы и предварительное название вверху первой страницы, а также, при необходимости, ссылки. Кроме того, авторы должны представить аннотацию и ключевые слова рукописи.

Предпочтительные темы для будущих изданий журнала:

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

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

Инициативные рукописи принимаются в текущем порядке на усмотрение Редколлегии Консорциума ПрМ.



Весенний выпуск Connections 2021 г. посвящен ряду проблем в киберсфере, включая рост киберпреступности, коррупции, распространения языка ненависти, пропаганды и дезинформации. Авторы предлагают перспективные решения – усиление правового режима, в том числе международных норм, применение мер доверия и развитие кибернавыков, а также описывают вызовы для обороны, возникающие в результате развития квантовых вычислений.

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

**Partnership for Peace – Consortium
Managing Editor – LTC Ed Clark
Gernackerstrasse 2
82467 Garmisch-Partenkirchen, Germany
Phone: +49 8821 750 2259
E-Mail: PfPCpublications2@marshallcenter.org**

ISSN 1812-1101

