Штрих-код цветной революции: агрессивная киберфизическая среда современного политического конфликта

УДК 32.019.51; 323.2

Николай ЛЕВЧУК, доктор политических наук

Николай ЛЕВЧУК. Штрих-код цветной революции: агрессивная киберфизическая среда современного политического конфликта. В статье раскрываются техносоциальные основы современного политического пространства, дается представление о киберфизических системах. Сетевой порядок взаимодействия между такими системами и их субъектами олицетворяет новое качество среды безопасности и формирование инновационной среды политического конфликта, одним из типичных примеров которого является цветная революция.
Ключевые слова: цветная революция, киберфизическая система, блокчейн, интернет вещей, информационно-коммуникационные технологии.

Nikolai LEVCHUK. Color revolution bar-code: Aggressive cyberphysical environment of modern political conflict. The article explores the technosocial foundations of modern political landscape and suggests an idea of cyberphysical systems. The network order of interaction between such systems and their subjects represents a new quality of the security environment and marks the formation of an innovative environment of political conflict, one of the typical examples of which is a color revolution.
Keywords: color revolution, cyberphysical system, blockchain, Internet of Things, information and communication technologies.

В современных условиях средой возникновения и развития политического конфликта выступает информационная сфера, в которой находят воплощение как общественные противоречия, так и борьба за ресурсы, а также любые конфликтные отношения между ее субъектами *[1]*. Типовым условием его возникновения в Республике Беларусь является дестабилизация извне социально-политической обстановки, а под информационной сферой подразумевается область деятельности людей, связанная с созданием, преобразо-

ОБ АВТОРЕ

ЛЕВЧУК Николай Николаевич.

Родился в 1973 году в г. Бресте. Окончил Минское суворовское военное училище (1990), факультет журналистики Белорусского государственного университета (1995).

В 1996–2008 годах работал корреспондентом, начальником отдела идеологической работы печатного органа Министерства обороны «Во славу Родины». С 2009 года – начальник отдела зарубежной военной информации информационного агентства Вооруженных Сил Республики Беларусь «Ваяр». С 2012 по 2015 год – научный сотрудник, с 2015-го – начальник научно-исследовательского отдела (проблем военной безопасности) научно-исследовательского управления (военно-гуманитарных исследований) Научно-исследовательского института Вооруженных Сил Республики Беларусь. Полковник.

Доктор политических наук (2022).

Автор двух монографий, 20 научных и более 200 публицистических статей.

Сфера научных интересов: теория национальной безопасности, теория коммуникации, геополитика, конфликтология, инноватика.

ванием и потреблением информации. Данная сфера под воздействием непрерывного процесса цифровой трансформации проявляет себя как киберфизическая среда взаимодействия политических субъектов.

Цифровой суверенитет

В глобальном контексте цифровые технологии используются в виде санкционного инструментария геополитического противоборства, как, например, в случае с решением ЕС об отключении нескольких белорусских банков от платформы передачи финансовых сообщений SWIFT, ограничении доступа к высоким технологиям. В современных условиях цифровые блокчейн-системы форматируют взаимодействие международных экономических блоков, а технологические платформы предопределяют границы политических союзов. В широком обиходе противоборствующих сторон на разных уровнях политического конфликта находится применение киберсаботажа, а новый железный занавес, выстраиваемый коллективным Западом в ходе объявленной им тотальной санкционной войны, имеет цифровые очертания.

Когнитивная среда политического конфликта обеспечивается существованием глобальной информационной инфраструктуры, имеющей сетевой характер и играющей стратегическую роль в нарастании потенциала конфликтности между геополитическими центрами силы. Но киберфизический характер взаимодействия в ней в большей степени выявляет эволюция современных промышленных систем. В данном контексте вызовы четвертой промышленной революции вторгаются в область политических трансформаций и реализуются в применении сетевого инструментария геополитического противоборства, апеллируя к необходимости укрепления цифрового суверенитета страны.

Поступательное созревание технологических условий четвертой промышленной революции обусловливает интеграцию в информационную сферу киберфизических систем (КФС) *[2]*, образуемых в процессе цифровизации. Формат и основные направления развития таких систем задают инновационные промышленные практики, реализуемые в цифровой концепции «Индустрия 4.0» (рис.) *[3]* и умной фабрике как ее

Индустрия 4.0: пример киберфизической системы
Источник: http://ar2016.rostec.ru/digital-current/.

технологическом ядре. В более широкой трактовке КФС – это умные сети электроснабжения, умные дома, умные города. В операционном отношении КФС составляют датчики, оборудование и информационные системы, охватывающие как отдельные объекты, так и комплексы объектов. КФС как сетевая система может включать интернет вещей, индустриальный интернет, умные энергетические сети, системы больших данных, системы облачных и туманных вычислений, системы дополненной реальности.

На уровне функционирования человеко-машинных систем КФС становятся объектами воздействия в войнах нового поколения, которые синтезируют определенный спектр вызовов и угроз, комплексно влияющих на среду безопасности *[4]*. Через информационное пространство фактически происходит вмешательство во внутренние дела государства, преднамеренная дискредитация его конституционных основ, побуждение к гражданскому неповиновению *[5]*. А это и есть политический конфликт, в крайнем проявлении представляющий собой войну, которая в современных условиях сопровождается увеличением объема передаваемой информации, ростом требований к системам разведки и управления, сокращением циклов управления войсковыми формированиями *[6]*. При этом сами по себе средства ведения и обеспечения вооруженной борьбы являются сложными автоматизированными устройствами, связанными между собой по сетецентрическому принципу, которые тоже могут быть идентифицированы как КФС.

В новой и новейшей истории накоплен немалый опыт деструктивного воздействия на КФС, в первую очередь осуществляемого в виде кибератак различного уровня исполнения. Один из самых масштабных актов кибersаботажа новейшей истории пережила Венесуэла, где в марте 2019 года почти вся территория (22 из 23 штатов) была обесточена из-за неполадок на крупнейшей в стране гидроэлектростанции «Гури». Из-за сбоя приостановили свою работу аэропорты и метро, выключились светофоры и уличное освещение, перестала работать телефонная связь *[7]*. По некоторым данным, эта атака была осуществлена силами киберкомандования вооруженных сил США.

Вещи интернета вещей

В грубом приближении киберфизическая система – это усложненный интернет вещей, сам по себе рассматриваемый в качестве КФС. Его возникновение, реализующее возможность телекоммуникационной связи между физическими объектами, находящимися в непосредственном пользовании человека, за последние десятилетия существенно расширило перечень объектов для возможных кибератак.

В Республике Беларусь мониторинг и противодействие подобным инцидентам осуществляются на системной основе. По данным Национального центра реагирования на компьютерные инциденты, в начале 2021 года в стране была зарегистрирована целевая атака на транспортно-логистическую сферу для получения информации и/или нарушения функционирования инфраструктуры при помощи трояна Emotet *[8]*. И это лишь один из примеров. Центром регулярно фиксируются попытки несанкционированного доступа к информационным системам государственных органов и организаций, внедрения в информационную инфраструктуру вредоносного программного обеспечения.

Так, 19 и 20 июля 2021 года в национальном сегменте интернета были зафиксированы очередные рассылки фишинговых писем. Показателен перечень объектов атаки: дипломатические и консульские представительства, органы местного управления, предприятия военно-промышленного комплекса, сфера реализации государственных закупок; предприятия – производители и поставщики техники и оборудования для лесного и сельского хозяйства, учреждения здравоохранения, компании транспортно-логистического профиля, производители технологического оборудования и систем промышленной автоматизации.

В настоящее время увеличивается количество правонарушений и преступлений с использованием информационно-коммуникационных технологий. Усложняются процессы и технологии, что требует все более

высокой квалификации работников. Пока не складывается общего понимания необходимости особой защиты критически важных объектов информатизации (КВОИ), и поэтому не вполне срабатывают соответствующие нормативные и организационные меры. Сохраняется высокая зависимость Республики Беларусь от импорта информационных технологий, средств информатизации и защиты информации, продолжается использование несертифицированных импортных программно-технических средств *[5]*.

Вместе с тем постоянно пополняемый список киберинцидентов и нарастающая активность противоборства в киберпространстве свидетельствуют о том, что в Республике Беларусь были приняты своевременные меры по созданию Государственного реестра КВОИ и в целом выстраивается эффективная система кибербезопасности. Накопленный мировой опыт позволяет идентифицировать основные сферы типологизации таких объектов: атомная энергетика, электроэнергетика, управление природными ресурсами (включая водоочистку и сточные воды), транспорт, пищевая промышленность, здравоохранение, телекоммуникации, финансовая и банковская системы, органы государственной власти, объекты массового скопления людей в первую очередь подвержены кибератакам. Принятая в марте 2019 года Концепция информационной безопасности Республики Беларусь *[9]* позволяет решать эту проблему на новом методологическом уровне.

Очевидно, что особой средой формирования современного политического конфликта является киберпространство. Методология нейтрализации рисков такого конфликта связана с локализацией КФС и последующей реализацией системы защиты КВОИ, а в более широком смысле общегосударственной стратегии противодействия дестабилизации. Ряд вышеописанных инцидентов и целенаправленных атак свидетельствует о том, что обеспечение кибербезопасности требует системного подхода, а также регулярной отработки деструктивных сценариев в ходе специальных учений по кибербезопасности. Одним из наиболее масштабных сценариев такого типа является цветная революция.

Разрозненный майдан

Лидером в теоретико-прикладных вопросах подготовки и реализации цветных революций являются США. В частности, 21 января 2003 года президент Дж. Буш подписал директиву о создании Управления глобальных коммуникаций для борьбы с антиамериканскими настроениями в мире. Весной 2005 года в Госдепартаменте США было создано новое специальное Управление трансформацией политических режимов для ведения информационного противоборства по осуществлению «демократических» переворотов в других странах в рамках так называемых бархатных революций. Инфраструктура информационных стратегических наступательных операций США по свержению неугодных режимов включает масштабную разветвленную сеть организаций, начиная от фонда Форда с годовым бюджетом более

500 млн долларов до «скромных» жертвователей масштаба фонда Дж.-М. Каплана, располагающего 10–15 млн долларов *[8]*.

Эволюция киберфизических систем позволила деструктивным силам в Республике Беларусь опробовать инновационную системную стратегию цветной революции. Она была основана на технологии «разрозненного майдана», когда «народные» выступления были организованы не только на одной из крупных площадей столицы, но и во всех областных и крупных районных центрах. Перед началом акций протеста проводилось целенаправленное информационное воздействие на население с использованием социальных сетей, мессенджеров и телеграм-каналов. Расшатывание обстановки накануне выборов, координация действий деструктивных сил в ходе массовых беспорядков осуществлялась объединенным оппозиционным штабом посредством социальный сетей и различных мессенджеров.

Одним из координирующих хабов был получивший скандальную известность деструктивный телеграм-канал с польской «пропиской». Накануне выборов там были размещены практические рекомендации (памятка протестующим) по силовому захвату власти в стране. В памятке содержался порядок действий при подготовке к участию в уличных беспорядках (одежда, экипировка и амуниция, телефоны правозащитных организаций); порядок действий при использовании личного автотранспорта в ходе беспорядков; порядок действий при использовании правоохранительными органами специальных средств; порядок передачи команд (сигналов) в ходе столкновений при отсутствии или неустойчивой работе интернета.

Особое внимание данным каналом отводилось обучению тактике действий протестующих при противостоянии с правоохранительными органами – «боевые» построения и перестроения; рассредоточение, отступление, быстрое перемещение и сбор во вновь назначенной точке, возведение и удержание баррикад, порядок применения самодельных взрывных устройств (средств поражения), вывод из строя специальной техники правоохранительных органов, занятие и перекрытие основных транспортных артерий и создание транспортного коллапса. Эти и другие протестные действия предполагают сетевую координацию, которая на уровне современных технических средств осуществима даже при полной блокировке доступа к интернету в локализованных местах городского пространства.

В итоге, как отмечает доктор политических наук Е.Г. Пономарева, уже на подготовительной стадии белорусских протестов были апробированы основные технологии дестабилизации: массовые протестные акции с применением сцепок и провоцированием сотрудников ОМОН, пикеты солидарности различных уровней, флешмобы, челленджи (жанр интернет-роликов, в которых блогер выполняет задание на видеокамеру) *[10]*.

Уровень координации протестов свидетельствует о нарастании «социальной тесноты» сетевого взаимодействия *[11]*. И здесь необходимо уточнение понятия КФС, преодоления бытующего стереотипа ее сугубо промышленной интерпретации, связанной с внедрением вычислительных ресурсов в физические сущности любого типа. Такая модель не самодостаточна без человеческого разума как ее априорного сущностного признака, а, значит, к физическим и программным компонентам КФС добавляются мыслительные и поведенческие алгоритмы, формализуемые на уровне новейших технологий, в том числе в виде искусственного интеллекта. Цифровая эволюция информационной сферы привела к формированию киберфизической среды массовой коммуникации, предполагающей, кроме прочего, ее артикуляцию в формате политического конфликта – типичное деструктивное поведение человека в нем рассматривается почти исключительно в симбиозе с техносферой.

Функционирование человеко-машинных систем, имея созидательный потенциал технологического обновления, в виде «шлакового» выброса социально-политического процесса реализуется на уровне применения дестабилизационных технологий. Онтологический разлом политического конфликта здесь пролегает по линии противоборства сети *[12]*, бросающей вызов государственной иерархии, которая парадоксально использует ее же механизмы для ответного противодействия.

В процессе цифровой трансформации «глобальный социум», содержащий в своем «чреве» заряды многих и многих политических конфликтов различного калибра, проявляет себя в функциональной среде нового качества, обусловленного киберфизическим симбиозом.

Статья поступила в редакцию 04.07.2022 г.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Бурдье, П. О символической власти / П. Бурдье // Социология социального пространства / пер. с франц.; отв. ред. перевода Н.А. Шматко. – М., СПб, 2007. – С. 87–96.
2. Казарин, О.В. Классификация угроз безопасности для киберфизических систем / О.В. Казарин // Комплексная защита информации: материалы XXIV науч.-практ. конф., Витебск, 21–23 мая 2019 г. / Витебский государственный технологический университет. – Витебск, 2019. – С. 59–63.
3. Современные концепции развития цифровой экономики [Электронный ресурс] // Ростех. – Режим доступа: http://ar2016.rostec.ru/digital-current/. – Дата доступа: 29.10.2019.
4. Слипченко, В.И. Войны шестого поколения: оружие и военное искусство будущего / В.И. Слипченко. – М.: Вече, 2002. – 384 с.
5. Арчаков, В. Концепция информационной безопасности Республики Беларусь – взгляд в будущее / В. Арчаков, О. Макаров, А. Баньковский // Беларуская думка. – 2019. – № 3. – С. 24–31.
6. Смирнов, И. Противоборство в киберпространстве по взглядам военно-политического руководства ведущих зарубежных государств / И. Смирнов, Г. Алексеев // Зарубежное военное обозрение. – 2017. – № 6. – С. 8–14.
7. Тумар, В. Киберпространство как среда военных действий: подходы в контексте Концепции информационной безопасности Республики Беларусь / В. Тумар, Н. Левчук // Беларуская думка. – 2020. – № 1. – С. 58–63.
8. Целевая атака на транспортно-логистическую сферу [Электронный ресурс] // Национальный центр реагирования на компьютерные инциденты. – Режим доступа: https://cert.by/?p=1919. – Дата доступа: 29.12.2021.
9. Концепция информационной безопасности Республики Беларусь [Электронный ресурс] // Национальный правовой Интернет-портал Республики Беларусь. – Режим доступа: https://pravo.by/document/?guid=3871&p0=P219s0001&ysclid=latpjfmm6273654025. – Дата доступа: 18.04.2019.
10. Пономарева, Е. Протестное движение в Беларуси: эволюция, технологии, символы / Е. Пономарева // Обозреватель – Observer. – 2021. – № 2. – С. 5–28.
11. Слука, А.Г. Ідэалогія беларускай дзяржаўнасці (метадалогія фарміравання) / А.Г. Слука. – Мінск: РІВШ, 2007. – 334 с.
12. Антанович, Н.А. Сетевые транснациональные структуры как субъекты международной безопасности / Н.А. Антанович // Международная безопасность и НАТО в 2015 г.: сб. материалов междунар. семинара, Минск, 8 дек. 2015 г. / под ред. А.А. Розанова, А.В. Русаковича. – Минск, 2016. – С. 9–15.