Научная статья
УДК 004 ; 327
DOI: 10.20323/2658-428X-2024-4-25-58
EDN: TVEBYH

Кибербезопасность в Евразийском регионе в контексте противостояния Запад-Восток

Чжан Цзэмин
Аспирант факультета международных отношений, Школа социальных наук, Университет Цинхуа, КНР, г. Пекин
zzm22@mails.tsinghua.edu.cn, https://orcid.org/0000-0002-6692-544X

Аннотация. После начала полномасштабного политического кризиса в отношениях Запада и Востока ситуация с кибербезопасностью в Евразийском регионе стала критической. Международные конфликты привели к снижению уровня кибербезопасности, частым атакам на критически важную цифровую инфраструктуру и распространению их на соседние страны. Страны с высоким уровнем развития интернета сталкиваются с такими проблемами, как уязвимость сетей, слабые пароли и раскрытие конфиденциальной информации, в то время как страны с более низким уровнем развития сталкиваются с частыми инцидентами безопасности из-за недостаточных инвестиций. Страны Евразийского региона предпринимают различные меры для повышения уровня кибербезопасности, но в краткосрочной перспективе ситуация не внушает благоприятного исхода. В долгосрочной перспективе, в ответ на различные проблемы кибербезопасности, страны Евразийского региона выбрали различные меры по повышению уровня кибербезопасности с учетом собственных реалий, но в краткосрочной перспективе ситуация с кибербезопасностью в Евразийском регионе все еще не оптимистична. Китай и Россия могут усилить сотрудничество в области информационной безопасности в рамках Шанхайской организации сотрудничества, чтобы повысить уровень кибербезопасности в соседних регионах.

Противостояние Запад-Восток будет продолжать оказывать устойчивое влияние на киберситуацию в Евразийском регионе: кибератаки станут неотъемлемой частью военных операций, кибершпионаж и инциденты в сфере кибербезопасности не прекратятся, а ситуация с кибербезопасностью останется очень серьезной. В то же время с развитием технологий искусственного интеллекта постепенно возникают новые проблемы регулирования и риски безопасности, что ставит новые задачи перед некоторыми странами Евразийского региона, которые относительно отстали в развитии цифровой инфраструктуры.

Ключевые слова: интернет; кибербезопасность; Евразия; геополитика; перетекание рисков; Шанхайской организации сотрудничества; шпионаж

Для цитирования: Чжан Цзэмин Кибербезопасность в Евразийском регионе в контексте противостояния Запад-Восток // Социально-политические исследования. 2024. № 4 (25). С. 58-71. http://dx.doi.org/10.20323/2658-428X-2024-4-25-58. https://elibrary.ru/TVEBYH.

Original article

Cybersecurity in the Eurasian region in the context of the West-East confrontation

Zhang Zeming
Graduate student at international relations, School of social sciences, Tsinghua university, PRC, Beijing
zzm22@mails.tsinghua.edu.cn, https://orcid.org/0000-0002-6692-544X

Abstract. After starting a full-scale political crisis in relations between the West and the East, the situation with cybersecurity in the Eurasian region has become critical. International conflicts have led to a decline in cybersecurity, frequent attacks on critical digital infrastructure and their spread to neighboring countries. Countries with high levels of Internet development face challenges such as network vulnerability, weak passwords and disclosure of confidential information, while countries with lower levels of development face frequent security incidents due to insufficient investment. The Eurasian region countries are taking various measures to increase the level of cybersecurity, but in the short term the situation is not optimistic. In the long term, in response to various cybersecurity problems, the countries of the Eurasian region have chosen various measures to increase the level of cybersecurity, taking into account their own realities, but in the short term, the situation with cybersecurity in the Eurasian region is still not optimistic. China and Russia can strengthen information security cooperation under the Shanghai Cooperation Organization in order to increase the level of cybersecurity in neighboring regions.

The West-East confrontation will continue to have a sustainable impact on the cyber situation in the Eurasian region: cyber attacks will be an integral part of military operations, cyber espionage and cybersecurity incidents will not stop, and the cybersecurity situation will remain very serious. At the same time, with the development of artificial intelligence technologies, new regulatory problems and security risks are gradually emerging, which poses new challenges for some countries in the Eurasian region, which are relatively behind in the development of digital infrastructure.

Key words: internet; cybersecurity; Eurasia; geopolitics; risk overflow; Shanghai cooperation organization; espionage

For citation: Zhang Zeming Cybersecurity in the Eurasian region in the context of the West-East confrontation. *Social and political researches*. 2024;4(25): 58-71. (In Russ). http://dx.doi.org/10.20323/2658-428X-2024-4-25-58. https://elibrary.ru/TVEBYH.

Введение

С быстрым развитием интернета и других цифровых технологий внимание международного сообщества к международному ландшафту кибербезопасности продолжает увеличи-

ваться. В последние годы процесс выработки глобальных правил кибербезопасности столкнулся с проблемами, и хотя некоторые страны достигли официальных соглашений по кибербезопасности на двустороннем и многостороннем уровнях, таких как международные договоры и заявления правительств с определенной степенью обязательной силы, в условиях обострения стратегической конкуренции между крупными державами дипломатическая игра вокруг международных правил кибербезопасности на международной арене усилилась, а формирование необязательных норм также сталкивается с неудачами. В результате пессимистичный взгляд на формирование международных правил в области кибербезопасности сохраняется и по сей день, а перспективы формирования глобального консенсуса остаются под вопросом. Кибербезопасность – это сложный вопрос, который включает в себя не только технологические разработки, но и множество политических аспектов [Безкоровайный, 2014; Бородакий, 2014; Зубарев, 2016; Кузнецов, 2013; Лебедь, 2017]. Хотя цифровое пространство сблизило взаимосвязанных пользователей, оно также характеризуется специфическими политическими геомаркировками в международном политическом ландшафте. Ситуация с кибербезопасностью в Евразийском регионе стала очень серьезной после начала противостояния Запад-Восток, а региональные международные конфликты привели к частым атакам на критически важные цифровые инфраструктуры.

Кибербезопасность: определение и классификация

Кибербезопасность – это основная тема в данной статье, и поэтому необходимо уточнить ее определение и категоризацию. «*Кибербезопасность* – это понятие с широким спектром коннотаций, которое постоянно развивается в соответствии с реальной политикой киберпространства» [Лу Чуаньин, 2022, с. 113]. В настоящее время различные международные организации и национальные правительства дали свои собственные определения кибербезопасности, которые могут отличаться друг от друга по специфическим оттенкам, но довольно близки по общим параметрам. Термин «кибербезопасность» иногда используется взаимозаменяемо с такими понятиями, как «безопасность интернета (internet security)» и «информационная безопасность (information security)», а выбор и использование этих терминов в некоторых странах вызывает споры из-за различий в концепциях управления кибербезопасностью. Однако кибербезопасность является наиболее часто используемым понятием в современном международном управлении киберпространством, поэтому в данной статье используется именно эта общепринятая терминология для обозначения объективной тематической области исследования, без привлечения дебатов о коннотации кибербезопасности и предпочтительном выборе концепций управления.

Международный союз электросвязи (International Telecommunication Union) определяет кибербезопасность как «совокупность инструментов, политик, концепций безопасности, гарантий безопасности, рекомендаций, методик управления рисками, действий, обучения, передового опыта, гарантий и технологий, которые могут быть использованы для защиты сетевой среды, а также активов организаций и пользователей», при этом общие цели сетевых

систем и сред включают в себя «доступность, целостность и конфиденциальность» [ITU, 2024]. Закон о кибербезопасности в Китайской Народной Республике определяет кибербезопасность как «… способность поддерживать сеть в состоянии стабильной и надежной работы и обеспечивать целостность, конфиденциальность и доступность сетевых данных путем принятия необходимых мер для предотвращения атак, вторжения, вмешательства, разрушения и незаконного использования сети, а также аварий» [ВСНП, 2016]. Правительство США определяет кибербезопасность как «искусство защиты сетей, устройств и данных от несанкционированного доступа или преступного использования, а также практика обеспечения конфиденциальности, целостности и доступности информации» [CISA, 2020]. В «Концепции стратегии кибербезопасности Российской Федерации» подчеркивается, что кибербезопасность – это «совокупность условий, при которых все составляющие киберпространства защищены от максимально возможного числа угроз и воздействий с нежелательными последствиями» [Концепция стратегии …].

Как видно, хотя члены международного сообщества не пришли к единому мнению относительно определения кибербезопасности, эти определения имеют ряд общих черт в отношении параметров объектов безопасности (сети и связанное с ними оборудование, данные) и целей безопасности (целостность, конфиденциальность и доступность), и в данной работе понимание концепции кибербезопасности будет основано на этих консенсусных элементах, и в основном будет следовать официальному определению правительства Китая.

Для того, чтобы прояснить конкретное содержание тематической области кибербезопасности, необходимо обратиться к классификации подтем кибербезопасности – это является предметом обсуждения в данной работе. Классификация конкретных направлений кибербезопасности может быть основана на *трех критериях*: *во-первых*, тип угрожающего поведения, включая кражу данных, вмешательство в данные, кражу личных данных, сетевой саботаж и атаки типа «отказ в обслуживании» с различной степенью угрозы для сетевой системы; *во-вторых,* тип субъектов угрозы, которые могут включать преступников, хакеров, террористов, правительственные оборонные и военные ведомства; и *в-третьих*, тип угрожающих целей, охватывающий широкий спектр потенциальных целей – от частных лиц, предприятий и общественных организаций до критической инфраструктуры и военных объектов. [Кулбария, 2019].

В зависимости от выбора вышеуказанных критериев и их конкретных значений, существуют различные способы категоризации направлений кибербезопасности. Для того, чтобы сделать эту категоризацию как можно более краткой и соответствующей реалиям дипломатических процессов, в данной работе используется категоризация вопросов, касающихся угроз кибербезопасности на уровне национальной безопасности, предложенная Джозефом Наем [NYE J S., 2011]. Эта классификация основана на *двух основных критериях*: является ли источник угрозы правительственным актором или нет, и является ли цель инициации угрозы политической или нет (табли-

цу 1). Исходя из этих двух критериев можно выделить *четыре основные направления кибербезопасности*.

Таблица 1.

Классификация направлений кибербезопасности на национальном уровне

Цель / Источник	Правительственные субъекты	Неправительственные субъекты
Политические цели	Кибервойна/контроль над кибервооружениями	Кибер-терроризм
Неполитические цели	Кибер-экономический шпионаж	Киберпреступность

Источник таблицы: авторский

Первое – это киберпреступность, инициированная неправительственными субъектами с неполитическими целями, которая обычно относится к преступлениям, совершаемым через интернет и компьютерные системы. Эта киберпреступная деятельность включает в себя как действия, инициированные отдельными хакерами с целью взлома или нарушения безопасности программы, системы или сети, так и организованную преступную деятельность, осуществляемую преступниками на интернет-платформах с помощью компьютерных технологий. Хотя в юридической практике разных стран некоторые кибератаки, инициированные правительственными субъектами, или кибердеятельность, инициированная террористами, определяются как широкая киберпреступность, темы киберпреступлений, обсуждаемые в данной статье, будут следовать этому узкому определению направлений киберпреступлений и, в основном, относиться к неполитическим угрозам кибербезопасности, инициированным неправительственными субъектами.

Второе направление – это кибертерроризм, инициированный неправительственными субъектами с политическими целями, включая террористические атаки на компьютерные и сетевые системы, оборудование и данные, инициированные террористами и организациями, а также использование компьютеров и сетей в качестве инструментов для террористической деятельности, такой как нагнетание страха с помощью насилия и разрушение общественных объектов для достижения своих политических целей.

Третье направление – это киберэкономический шпионаж, или киберкоммерческое воровство, инициированное государственными субъектами с неполитическими целями. Появление этой угрозы обусловлено, главным образом, огромной экономической выгодой от использования в киберпространстве коммерчески конфиденциальной информации, например, прав на интеллектуальную собственность. Тема так называемого киберэкономического шпионажа, которую продвигают западные страны, такие как США, и которая привлекает все больше внимания, делает больший акцент на использовании киберпространства правительственными субъектами для получения коммерчески конфиденциальной информации от предприятий в другой стране. Интересно, что поскольку политический шпионаж прямо не запрещен международным правом, инициированный правительством киберполи-

тический шпионаж не стал официальной повесткой дня международного управления кибербезопасностью из-за стратегии «дихотомии» США в отношении кибершпионажа.

Четвертое направление – кибервойны, инициированные правительственными субъектами с политическими целями. Поскольку международное сообщество еще не пришло к единому мнению о том, какая интенсивность или последствия военного киберповедения могут рассматриваться как кибервойна, в данной статье мы придерживаемся простой классификации, основанной на типе действующих лиц и целей, и включаем в широкую категорию кибервойны как политические, так и военные кибератаки, инициированные правительственными субъектами. Это направление также можно рассматривать как вопрос контроля над кибервооружениями с точки зрения реагирования национальных правительств на эти виды угроз кибербезопасности и контроля над ними.

Конечно, эта классификация, состоящая из четырех направлений, не идеальна, и в реальном мире страны могут по-разному оценивать актуальность конкретного инцидента в сфере кибербезопасности, актуальность угрозы кибербезопасности может меняться, а некоторые угрозы кибербезопасности могут быть межтематическими по своей природе. Например, некоторые виды вредоносной кибердеятельности, не ограничивающиеся экономическими целями, также были включены в сферу киберпреступности на уровне внутреннего законодательства; среди правительств ведутся споры о том, достаточно ли высказываний в интернете для того, чтобы считать их киберпреступлением; вредоносная кибердеятельность кибертеррористов часто может быть вовлечена в киберпреступность на уровне внутреннего законодательства. Например, администрация Обамы в США предприняла ответ на действия Исламского государства, террористической организации, в сферу так называемого права на киберпреступность, а также право на киберсамооборону и объявила против него «кибервойну» [CBS News, 2016]. Однако в целом этот метод классификации позволяет выделить и обобщить различные темы разного характера в области кибербезопасности, сформировать международные правила в различных областях кибербезопасности, основываясь на текущих попытках международных сообществ.

В то же время, чтобы сделать содержание исследования более целенаправленным, проблемы и события в области кибербезопасности в данной работе будут в основном сосредоточены на вышеуказанных четырех направлениях. В обсуждение данной работы не включены некоторые вопросы, относящиеся к сфере безопасности в широком смысле, но выделены отдельные проблемы на уровне политики и практики (например, безопасность данных) или находящиеся на стадии зарождения (например, безопасность ИИ).

Распространение геополитических рисков в киберпространстве

В 1904 году британский географ Хэлфорд Макиндер (1861–1947 гг.) представил Королевскому географическому обществу в Лондоне доклад под названием «Географический стержень истории». Он утверждал, что Россия и большая часть Центральной Азии, «стержень» или «сердцевина» Евразии, являются ключом к мировому балансу сил, и что страна, которая будет контролировать их, сможет доминировать над Евразией и всем миром. Более века

спустя очевидно, что тема геополитики вызывает споры среди ученых всех мастей. «Сегодня глобальное управление ослабевает, центр власти смещается от традиционных государств к негосударственным акторам, что увеличивает вероятность политических кризисов» [Balli, 2022, с. 464]. Враждебность негосударственных субъектов по отношению к правительствам в некоторых случаях дестабилизировала общий геополитический ландшафт стран, тем самым повышая индекс глобальной эффективности правительств. Это было очевидно на протяжении всей войны в Афганистане, когда власть в значительной степени перешла от афганского правительства к Талибану. Беспрецедентный рост национальных чувств во всем мире за последнее десятилетие, особенно в США и Индии, и усиление ультранационализма представляют собой серьезную угрозу для глобального геополитического ландшафта. Для отдельных стран эта экстремистская идеология является потенциальным источником внутренних и внешних угроз, что в случае с Индией не только привело к внутреннему индуистско-мусульманскому расколу, но и усилило враждебность в индо-пакистанских отношениях. В то же время ограничения международного сообщества на распространение оружия массового уничтожения не привели к желаемым результатам, особенно в отношении ядерной программы Ирана и Северной Кореи, что еще больше усиливает потенциал геополитической напряженности между этими странами и крупными экономическими державами.

Дэвид Л. Хафф и Джеймс М. Лутц исследовали геопространственные формы передачи и распространения конфликта, утверждая, что процесс распространения конфликтов скорее заразен, чем иерархичен, и что исследования того времени просто предполагали наличие определенной корреляции между размером города и временем возникновения конфликта, и что культурные каналы коммуникации могут быть фактором, ограничивающим степень иерархического воздействия, но не уточняли механизм передачи конфликта [David L. Huff, 1974]. Исследования С. Хилла и Д. Ротчайлда позволили уточнить, что вхождение во внешнеполитический конфликт зависит от недавней истории внутренних гражданских конфликтов, и что степень участия во внешнеполитическом конфликте возрастает, если общество поляризовано между небольшим количеством конкурирующих групп [Hill, 1986]. Исследования Х. Бухауга и К. С. Гледича показали, что вооруженные конфликты действительно оказывают влияние на соседние страны. [Buhaug, 2008]. Таких же выводов придерживается Алекс Брейтуэйт, который утверждает, что заражение соседским конфликтом становится риском с уменьшающейся вероятностью для более развитых государств. Эта условная гипотеза подтверждается моделью заражения гражданской войной, которая предполагает, что возможности государства изменяют вероятность того, что государство имеет риск заражения от гражданской войны, происходящей в соседней стране [Braithwaite, 2010]. С. Б. Бломберг и Б. П. Розендорф использовали гравитационную модель для изучения влияния глобализации и демократизации на транснациональный терроризм и внешние конфликты, рассматривая мотивы террористических организаций и то, как демократия и глобальная интеграция влияют на негосударственные

экономические субъекты, и обнаружили, что демократия, граждане с более высоким уровнем дохода и открытые общества значительно снижают уровень конфликтов [Blomberg, 2006].

В контексте стремительного развития информационных технологий данная статья предполагает, что безопасность киберпространства и его уникальная структура превратились в новый тип распространения геополитических рисков.

Кибератаки часто происходят в результате международных конфликтов и распространяются на соседние страны

Международные конфликты в цифровую эпоху часто приводят к кибервойнам, которые, хотя и играют в основном лишь вспомогательную роль, представляют серьезную угрозу информационной безопасности соответствующих стран и распространяются на соседние государства.

По данным платформы «Кибератаки во время конфликтов» Института кибернетического мира (Cyber Peace Institute), некоммерческой организации, расположенной в Женеве, Швейцария, по состоянию на ноябрь 2023 г., с момента начала напряженной фазы противостояния Запад-Восток на территории Украины было совершено в общей сложности 3 069 кибератак, из которых 923 кибератаки произошли в России и Украине, причем 23 различные критически важные цифровые инфраструктуры подверглись прямому воздействию. Кибератаки все чаще проводятся параллельно с военными операциями, их основная цель – внедрить вредоносное программное обеспечение для удаления данных в критически важные цифровые инфраструктуры с целью уничтожения зашифрованных данных и парализовать работу сетевых систем.

В начале 2023 г. Николай Мурашов, заместитель руководителя Национального координационного центра по киберинцидентам Федеральной службы безопасности (ФСБ) России, заявил, что количество кибератак на российскую инфраструктуру значительно возросло после начала Специальной военной операции. Необходимость российского энергетического сектора оставаться на связи с внешним миром сделала его сети главной мишенью для кибератак иностранных хакерских групп. Согласно информации, опубликованной цифровым СМИ Cybernews в ноябре 2023 года, кибер-армия взломала «Газпром», а также ключевую цифровую инфраструктуру Федеральной налоговой службы России (ФНС), которая является одной из крупнейших налоговых администраций в мире. Связь между местными российскими налоговыми органами и Федеральной налоговой службой была нарушена.

Международные санкции вынудили российских ИТ-специалистов массово эмигрировать, что также повлияло на российскую кибербезопасность. Нет четких данных о том, сколько из этих эмигрировавших за границу российских ИТ-техников были использованы международными хакерскими организациями. Однако, судя по частоте и вредности кибер-инцидентов, в ходе которых атаковалась критически важная цифровая инфраструктура России, вероятность такого события очень высока.

В этих условиях Россия начала укреплять безопасность своей внутренней критической цифровой инфраструктуры с целью улучшения возможностей кибербезопасности, в том числе путем внесения поправок в законодательство о кибербезопасности с

целью ужесточения контроля над операторами данных. 1 марта 2023 г. в России вступил в силу новый измененный Закон о защите персональных данных. Среди прочего, статьи 178 и 179 предусматривают, что операторы данных должны оценивать ущерб, нанесенный субъекту данных, и соответствие выявленного ущерба действиям, предпринятым оператором данных. В то же время, новая редакция Закона о защите персональных данных также предусматривает, что операторы данных должны информировать Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций РФ о действиях, связанных с трансграничной передачей данных.

Антон Демохин, заместитель министра иностранных дел Украины и главный специалист по цифровым преобразованиям, сказал в интервью СМИ в Сингапуре в октябре 2023 г., что, хотя Украине в основном удалось остановить кибератаки, она заплатила за это немалую цену [ITU].

Украина постоянно модернизирует свою киберзащиту с помощью США и ЕС. В 2023 г. США предоставили Украине помощь в размере 37 млн долларов на цели кибербезопасности, направленную на улучшение способности Украины реагировать на угрозу киберинцидентов и защищать критически важную цифровую инфраструктуру. Агентство кибербезопасности ЕС также подписало с Украиной Рабочее соглашение по кибербезопасности 13 ноября 2023 г., цель которого – усилить сотрудничество с Украиной в области цифровой обороны и тем самым защитить Украину и страны ЕС от потенциальных киберугроз.

Нагорно-карабахский конфликт – это вооруженный конфликт, произошедший в Нагорном Карабахе на юго-западе Азербайджана между Республикой Арцах (которая принадлежит к политическому образованию с ограниченным признанием), поддерживаемой Республикой Армения, и Азербайджанской Республикой. 19-20 сентября 2023 г. Азербайджан начал широкомасштабное военное наступление на Республику Арцах, известное как третий нагорно-карабахский конфликт. Этот конфликт повлиял на нормализацию отношений между Азербайджаном и Арменией и стал причиной различных видов кибератак.

В августе 2023 г. Forti Guard Labs обнаружила в Азербайджане зараженную вредоносным ПО служебную записку. Записка была замаскирована под электронное письмо от руководителя азербайджанского предприятия, утверждавшего, что у него есть информация о пограничном конфликте между Азербайджаном и Арменией. Со своей стороны Армения сообщила о многочисленных кибератаках, предшествовавших третьему конфликту. Самвел Мартиросян, армянский эксперт по кибербезопасности, сказал, что международные аэропорты и правительственные учреждения Армении подверглись серьезным кибератакам до нападения Азербайджана на Нагорный Карабах. По данным армянского новостного агентства Arka, опубликованным в сентябре 2023 г. со ссылкой на Службу национальной безопасности Армении (СНБ), количество кибератак на Армению резко возросло с сентября 2023 года. Эти атаки включали в себя, в частности, попытки распространения ложной информации и кражи данных. Кроме того, 1 ноября 2023 г. армянское государственное информационное

агентство Арменпресс сообщило, что компания Apple Inc. предупредила пользователей телефонов Apple в Армении о том, что хакеры атакуют их с помощью программного обеспечения “Pegasus”. Армянский эксперт по кибербезопасности Мартиросян считает, что эти хакеры были связаны с правительством Азербайджана [U.S. cybersecurity …].

В 2023 г. Азербайджан увеличил распространение интернета на 5 % по сравнению с 2022 г. В августе 2023 г. Азербайджан представил свою первую стратегию кибербезопасности – Стратегию информационной и кибербезопасности Азербайджанской Республики на 2023-2027 гг. Стратегия направлена на повышение безопасности информационно-коммуникационных технологий (*далее ИКТ*) страны и безопасности ее граждан. Стратегия направлена на повышение национальных стандартов информационной безопасности и способствует достижению общей цели – дать возможность государству, обществу и отдельным людям безопасно использовать современные ИКТ. Кроме того, Стратегия фокусируется на защите персональных данных и определяет девять последующих приоритетных направлений, а для реализации Стратегии были назначены 23 агентства.

В 2023 г. распространение интернета в Армении увеличилось на 12,1 %. В 2023 г. в Армении насчитывалось более 3 000 компаний, работающих в секторе ИКТ, в которых трудилось около 20 000 квалифицированных ИТ-специалистов, а годовой объем производства превышал $1 млрд. Армения постоянно укрепляет международное сотрудничество в области кибербезопасности. Например, в апреле 2023 г. Армения и Россия подписали соглашение о сотрудничестве в области информационной безопасности; в июле Армения и США обсудили возможность сотрудничества в области кибербезопасности; в октябре правительства Армении и Ирана договорились об укреплении связей в области ИКТ и обсудили возможность совместного создания центра обработки данных; в декабре ОАЭ и Армения подписали Меморандум о взаимопонимании по сотрудничеству в области кибербезопасности.

Заключение

Таким образом, ситуация с кибербезопасностью в Евразийском регионе с началом противостояния Запад-Восток стала критической, а количество инцидентов кибербезопасности в Евразийском регионе остается высоким. К непосредственным причинам такой ситуации относятся:

− прямое влияние региональных международных конфликтов и распространение инцидентов кибербезопасности из стран, находящихся в центре конфликтов, на соседние страны;

− проблемы уязвимости сетей, слабых паролей и раскрытия конфиденциальной информации спровоцировали ряд инцидентов кибербезопасности в районах с высоким уровнем проникновения интернета в странах Евразии;

– страны Евразии с медленным развитием интернета из-за недостатка инвестиций в кибербезопасность стали более уязвимыми.

Страны Евразии также подвержены инцидентам, связанным с кибербезопасностью из-за недостаточных инвестиций в кибербезопасность.

Столкнувшись с проблемой кибербезопасности, страны Евразийского региона приняли различные меры по улучшению кибербезопасности с уче-

том собственных реалий. Во-первых, они увеличили инвестиции в инфраструктуру кибербезопасности на государственном, деловом и общественном уровнях, а также приняли соответствующие законы, регулирующие поведение соответствующих цифровых предприятий и повышающие осведомленность людей в вопросах защиты цифровой информации. Во-вторых, отмечается активное совершенствование потенциала кибербезопасности посредством международного сотрудничества, включая обмен данными между правительствами, обучение талантливых специалистов и помощь (займы) от международных организаций или иностранных правительств. Эти меры положительно влияют на повышение уровня кибербезопасности в Евразийском регионе, но если региональные международные конфликты, связанные с противостоянием Запад-Восток, не будут разрешены своевременно и эффективно, то в краткосрочной перспективе будет трудно кардинально изменить критическую ситуацию с кибербезопасностью в Евразийском регионе.

В то же время ШОС может играть более значительную роль в сотрудничестве в области кибербезопасности:

− во-первых, это укрепление сотрудничества в области кибербезопасности со странами-членами. Сотрудничество включает обмен данными и их совместное использование, обучение персонала и создание институционализированных механизмов двустороннего сотрудничества с ключевыми странами для совместного поддержания кибербезопасности. Это также, может быть, использовано для разрядки возможных споров по кибербезопасности между странами-участницами путем создания регионального центра по кибербезопасности и координации действий со странами-участницами для улучшения наращивания потенциала кибербезопасности;

− во-вторых, это повышение цифровой грамотности всех людей в странах-участницах. Чтобы усилить проактивный характер социального управления кибербезопасностью и превратить пассивную защиту кибербезопасности в проактивное нападение, необходимо создать «цифровой щит» на социальном уровне. Для этого ШОС должна запустить специальную «программу повышения грамотности в области кибербезопасности», включающую подготовку талантов в области кибербезопасности, усиление пропаганды кибербезопасности и повышение осведомленности об информационной безопасности;

− в-третьих, ШОС должна сотрудничать с Международным союзом электросвязи (МСЭ). Пять стратегических столпов глобальной повестки дня МСЭ в области кибербезопасности (правовой, технический, организационный, наращивание потенциала и сотрудничество) должны быть интегрированы в институционализированное сотрудничество в области кибербезопасности между странами-членами ШОС.

Противостояние Запад-Восток будет продолжать оказывать устойчивое влияние на киберситуацию в Евразийском регионе: кибератаки станут неотъемлемой частью военных операций, кибершпионаж и инциденты в сфере кибербезопасности не прекратятся, а ситуация с кибербезопасностью останется очень серьезной. В то же время с развитием технологий искусственного интеллекта постепенно возникают новые проблемы регулиро-

вания и риски безопасности, что ставит новые задачи перед некоторыми странами Евразийского региона, отстающими в развитии цифровой инфраструктуры.

Библиографический список

1. Безкоровайный М. М. Кибер-безопасность – подходы к определению понятия / М. М. Безкоровайный, А. Л. Татузов // Журнал Вопросы кибербезопасности. 2014. Выпуск №1 (2). С. 22–27.

2. Бородакий Ю. В. Кибербезопасность как основной фактор национальной и международной безопасности XXI века (часть 2) / Ю. В. Бородакий, А. Ю. Добродеев, И. В. Бутусов // Вопросы кибербезопасности. 2014. №1(2). С. 5–12.

3. Всекитайское собрание народных представителей: Закон о сетевой безопасности Китайской Народной Республики. URL: http://www.npc.gov.cn/zgrdw/npc/xinwen/2016-11/07/content_2001605.htm (Дата обращения: 23.05.2024) (на кит. языке).

4. Зубарев И. В. Уязвимости информационных систем / И. В. Зубарев, И. В. Жидков, И. В. Кадушкин, С. А. Медовщикова // Информационные и математические технологии в науке и управлении. 2016. №3. С. 174–184.

5. Концепция стратегии кибербезопасности Российской Федерации. URL: http://www.council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf (дата обращения: 23.05.2024).

6. Кузнецов С. Кибербезопасность в 21 веке // Открытие системы СУБД. №5. 2013. URL: http://www.osp.ru (дата обращения: 23.05.2024).

7. Кулбария Управление интернетом (互联网治理) / Кулбария, Лу Чуаньин [и др.]. Пекин : Изд-во Университета Цинхуа, 2019. (на кит. языке).

8. Лебедь В. Н. Управление процессами обеспечения кибербезопасности как фактор международной стабильности / В. Н. Лебедь, Б. И. Терещенко, К. А. Восканян // Коммуникология: электронный научный журнал. 2017. Т.2, №4. С. 30–37.

9. Лу Чуаньин (鲁传颖). Эволюция стабильной власти, дилемма безопасности и построение системы управления в глобальном киберпространстве (全球网络空间稳定权力演变、安全困境与治理体系构建) [M]. Шанхай : Гэчжэ/Шанхайское народное издательство, 2022.

10. ITU. Cybersecurity. URL: https://www.itu.int/itu-d/sites/cybersecurity/ (дата обращения: 23.05.2024).

11. U. S. cybersecurity and infrastructure security agency. What is cybersecurity? URL: https://www.cisa.gov/news-events/news/what-cybersecurity (дата обращения: 23.05.2024).

12. 库尔巴利亚, 鲁传颖等. 互联网治理[M]. 北京: 清华大学出版社, 2019: 93.

13. NYE J S. Nuclear lessons for cyber security? // Strategic studies quarterly, 2011, 5(4). P. 21–22.

14. CBS News. AP: U. S. military launches aggressive cyberwar on ISIS. 2016-2-26 URL: https://www.cbsnews.com/news/isis-targeted-us-military-cyberwar/ (дата обращения: 23.05.2024).

15. Balli, F., Balli, H. O., Hasan, M. et al. Geopolitical risk spillovers and its determinants // The annals of regional science. 2022. Vol. 68, p.464.

16. David L. Huff & James M. Lutz. The contagion of political unrest in independent Black Africa // Economic Geography. 1974. Vol. 50(4), p. 352–367.

17. Hill S., & Rothchild, D. The contagion of political conflict in Africa and the world // The journal of conflict resolution. 1986. Vol.30(4), p.716–735.

18. Buhaug H., & Gleditsch, K. S. Contagion or confusion? Why conflicts cluster in space // International studies quarterly. 2008. 52(2), p.215–233.

19. Braithwaite A. Resisting infection: How state capacity conditions conflict contagion // Journal of peace research. 2010. 47(3), p. 311–319.

20. Blomberg S. Brock and Rosendorff, Bryan Peter, A gravity model of globalization, democracy and transnational terrorism (January 2006). USC CLEO Research paper No. C06-6, Available at URL: http://dx.doi.org/10.2139/ssrn.904204.

Reference list

1. Bezkorovajnyj M. M. Kiber-bezopasnost' – podhody k opredeleniju ponjatija = Cyber security – approaches to defining the concept / M. M. Bezkorovajnyj, A. L. Tatuzov // Zhurnal Voprosy kiberbezopasnosti. 2014. Vypusk №1 (2). S. 22–27.

2. Borodakij Ju.V. Kiberbezopasnost' kak osnovnoj faktor nacional'noj i mezhdunarodnoj bezopasnosti XXI veka (chast' 2) = Cybersecurity as a major factor in xxi century national and international security (Part 2) / Ju.V. Borodakij, A.Ju. Dobrodeev, I. V. Butusov // Voprosy kiberbezopasnosti. 2014. №1(2). S. 5–12.

3. Vsekitajskoe sobranie narodnyh predstavitelej: Zakon o setevoj bezopasnosti Kitajskoj Narodnoj Respubliki = National People's Congress: network security law of the People's Republic of China. URL: http://www.npc.gov.cn/zgrdw/npc/xinwen/2016-11/07/content_2001605.htm (data obrashhenija: 23.05.2024) (na kit. jazyke).

4. Zubarev I. V. Ujazvimosti informacionnyh sistem = Vulnerabilities of information systems / I. V. Zubarev, I. V. Zhidkov, I. V. Kadushkin, S. A. Medovshhikova // Informacionnye i matematicheskie tehnologii v nauke i upravlenii. 2016. №3. S. 174-184.

5. Koncepcija strategii kiberbezopasnosti Rossijskoj Federacii = The concept of the cybersecurity strategy of the Russian Federation. URL: http://www.council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf (data obrashhenija: 23.05.2024).

6. Kuznecov S. Kiberbezopasnost' v 21 veke = Cybersecurity in the XXI Century // Otkrytie sistemy SUBD. №5. 2013. URL: http://www.osp.ru (data obrashhenija: 23.05.2024).

7. Kulbarija Upravlenie internetom = Internet management (互联网治理) / Kulbarija, Lu Chuan'in [i dr.]. Pekin : Izd-vo Universiteta Cinhua, 2019. (na kit. jazyke).

8. Lebed' V. N. Upravlenie processami obespechenija kiberbezopasnosti kak faktor mezhdunarodnoj stabil'nosti = Managing cybersecurity processes as a factor of international stability / V. N. Lebed', B. I. Tereshhenko, K. A. Voskanjan // Kommunikologija: jelektronnyj nauchnyj zhurnal. 2017. T.2, №4. S. 30–37.

9. Lu Chuan'in (鲁传颖). Jevoljucija stabil'noj vlasti, dilemma bezopasnosti i postroenie sistemy upravlenija v global'nom kiberprostranstve = The evolution of stable power, the security dilemma and the construction of a governance system in global cyberspace (全球网络空间稳定权力演变、安全困境与治理体系构建) [M]. Shanhaj : Gjechzhje/Shanhajskoe narodnoe izdatel'stvo, 2022.

10. ITU. Cybersecurity. URL: https://www.itu.int/itu-d/sites/cybersecurity/ (data obrashhenija: 23.05.2024).

11. U. S. cybersecurity and infrastructure security agency. What is cybersecurity? URL: https://www.cisa.gov/news-events/news/what-cybersecurity (data obrashhenija: 23.05.2024).

12. 库尔巴利亚, 鲁传颖等. 互联网治理[M]. 北京: 清华大学出版社, 2019: 93.

13. NYE J S. Nuclear lessons for cyber security? // Strategic studies quarterly, 2011, 5(4). P. 21–22.

14. CBS News. AP: U. S. military launches aggressive cyberwar on ISIS. 2016-2-26 URL: https://www.cbsnews.com/news/isis-targeted-us-military-cyberwar/ (data obrashhenija: 23.05.2024).

15. Balli F., Balli, H. O., Hasan M. et al. Geopolitical risk spillovers and its determinants // The annals of regional science. 2022. Vol. 68, p.464.

16. David L. Huff & James M. Lutz. The contagion of political unrest in independent Black Africa // Economic Geography. 1974. Vol. 50(4), p. 352–367.

17. Hill S., & Rothchild, D. The contagion of political conflict in Africa and the world // The journal of conflict resolution. 1986. Vol.30(4), p.716–735.

18. Buhaug H., & Gleditsch, K. S. Contagion or confusion? Why conflicts cluster in space // International studies quarterly. 2008. 52(2), p. 215–233.

19. Braithwaite A. Resisting infection: How state capacity conditions conflict contagion // Journal of peace research. 2010. 47(3), r. 311–319.

20. Blomberg S. Brock and Rosendorff, Bryan Peter, A gravity model of globalization, democracy and transnational terrorism (January 2006). USC CLEO Research paper No. C06-6, Available at. http://dx.doi.org/10.2139/ssrn.904204.

Статья поступила в редакцию 27.09.2024; одобрена после рецензирования 19.10.2024; принята к публикации 12.11.2024.
The article was submitted on 27.09.2024; approved after reviewing 19.10.2024; accepted for publication on 12.11.2024