# Политика

## Китай в мировом киберпространстве

 DOI: 10.31857/S013128120011435-9

***Исаев Александр Сергеевич***

Кандидат исторических наук, ведущий научный сотрудник, заместитель руководителя Центра изучения и прогнозирования российско-китайских отношений ИДВ РАН.
E-mail: aisaev51@mail.ru.

*Аннотация:*

В настоящее время в мировом киберпространстве складывается весьма напряженная ситуация, связанная с соперничеством за лидерство в цифровой среде. Автор анализирует роль и значение китайской стратегии в глобальном информпространстве и показывает рост влияния КНР на решение многих технических вопросов функционирования и управления им. В статье анализируется также оборонная политика КНР в этой сфере и показывается постепенное превращение Китая в одну из мировых киберсверхдержав, бросающих вызов американскому господству в Интернете, что уже привело к острому противостоянию и соперничеству КНР и США, к технологическим войнам между ними, к созданию с обеих сторон арсеналов боевых цифровых вирусов, а также разработке стратегии и тактики ведения информационных войн.

*Ключевые слова:*

Киберпространство, кибербезопасность, боевые вирусы, хакерские атаки, Интернет, информационное общество, цифровая экономика, информационная война.

*Для цитирования:*

Исаев А.С. Китай в мировом киберпространстве // Проблемы Дальнего Востока. 2020. № 4. С. 6–23. DOI: 10.31857/S013128120011435-9.

# Politics

## China in the Global Cyberspace

***Alexander Isaev***

Ph.D. in History, leading Researcher, deputy head of the Center for study and forecasting of the Russian-Chinese relations, Institute of Far Eastern Studies of the Russian academy of sciences.
E-mail: aisaev51@mail.ru.

*Abstract:*

Today the situation in the sphere of cyberspace is taking a very tense turn due to the rivalry between the world biggest economies for leadership in the digital environment. The author analyzes the role and importance of the Chinese strategy in the information space and shows the growing impact of China on the decision-making process that take place in the digital environment on the international arena regarding different technical issues and managing principles. The article also analyzes the Chinese defense policy in this area and demonstrates the gradual transformation of that country into one of the world's cyber superpowers that can challenge American dominance on the Internet, which has already led to sharp confrontation and rivalry between China and the USA in the modern information space, to technological wars, to the development of arsenals of military viruses on both sides as well as to the development of information wars strategies and tactics.

*Key words:*

Cyberspace, cybersecurity, war viruses, hacker attacks, Internet, information society, digital economy, information war.

*For citation:*

Isaev A.S. China in the Global Cyberspace // Far Eastern Affairs. 2020. No. 4. Pp. 6–23. DOI: 10.31857/S013128120011435-9.

Бурное развитие информационно-коммуникационных технологий в конце прошлого — начале нынешнего столетия привело к тому, что цифровизация проникла во многие сферы человеческой деятельности, начиная от экономики и заканчивая обороной. Сегодня сложно представить мир без компьютеров и смартфонов, без Интернета, социальных сетей и электронной торговли. В результате в обиход прочно вошли понятия цифровой экономики, информационного общества, киберпространства, виртуальной реальности, кибербезопасности, информационных войн и т.п.

## Положение Китая в современном мировом киберпространстве

Сегодня темы цифровизации всех сфер человеческой деятельности, прогнозирования развития информационно-коммуникационных технологий (ИКТ) и проблема обеспечения информационной безопасности — одни из самых обсуждаемых. А с начала нового столетия — они среди важнейших факторов, оказывающих влияние на международные отношения. Особую актуальность им придает серьезная экономическая составляющая. Отрасль ИКТ сегодня — одна из наиболее динамично развивающихся, и поглощающих многие миллиарды на разработку, внедрение, функционирование и энергетическое обеспечение новых технологий.

*Таблица 1*

**20 стран с самым большим числом Интернет-пользователей[1]**

*I квартал 2020 г.*

| # | Страна или Регион | Кол-во Интернет-пользователей на 1 кв. 2020 | Кол-во Интернет-пользователей на 4 кв. 2000 | Население, по состоянию на 2020 г. | Население по состоянию на 2000 г. | Прирост пользователей за 2000–2020 |
|---|---|---|---|---|---|---|
| 1 | Китай | 854 000 000 | 22 500 000 | 1 439 062 022 | 1 283 198 970 | 3 796% |
| 2 | Индия | 560 000 000 | 5 000 000 | 1 368 737 513 | 1 053 050 912 | 11 200% |
| 3 | США | 313 322 868 | 95 354 000 | 331 002 651 | 281 982 778 | 328% |
| 4 | Индонезия | 171 260 000 | 2 000 000 | 273 523 615 | 211 540 429 | 8 560% |
| 5 | Бразилия | 149 057 635 | 5 000 000 | 212 392 717 | 175 287 587 | 2 980% |
| 6 | Нигерия | 126 078 999 | 200 000 | 206 139 589 | 123 486 615 | 63 000% |
| 7 | Япония | 118 626 672 | 47 080 000 | 126 854 745 | 127 533 934 | 252% |
| 8 | Россия | 116 353 942 | 3 100 000 | 145 934 462 | 146 396 514 | 3 751% |
| 9 | Бангладеш | 94 199 000 | 100 000 | 164 689 383 | 131 581 243 | 94 199% |
| 10 | Мексика | 88 000 000 | 2 712 400 | 132 328 035 | 2 712 400 | 3 144% |
| 11 | Германия | 79 127 551 | 24 000 000 | 83 783 942 | 81 487 757 | 329% |
| 12 | Филиппины | 79 000 000 | 2 000 000 | 109 581 078 | 77 991 569 | 3 950% |
| 13 | Турция | 69 107 183 | 2 000 000 | 84 339 067 | 63 240 121 | 3 455% |
| 14 | Вьетнам | 68 541 344 | 200 000 | 68 541 344 | 200 000 | 34 250% |
| 15 | Великобритания | 63 544 106 | 15 400 000 | 67 886 011 | 58 950 848 | 413% |
| 16 | Иран | 67 602 731 | 250 000 | 83 992 949 | 66 131 854 | 27,040% |
| 17 | Франция | 60 421 689 | 8 500 000 | 65 273 511 | 59 608 201 | 710% |
| 18 | Таиланд | 57 000 000 | 2 300 000 | 69 799 978 | 62 958 021 | 2 478% |
| 19 | Италия | 54 798 299 | 13 200 000 | 60 461 826 | 57 293 721 | 415% |
| 20 | Египет | 49 231 493 | 450 000 | 102 334 404 | 69 905 988 | 10 940% |
| | Итого Топ 20 стран | 3 241 273 512 | 251 346 400 | 5 233 377 837 | 4 312 497 691 | 1 289% |
| | Остальные страны | 1 332 876 622 | 109 639 092 | 2 563 237 873 | 1 832 509 298 | 1 216% |
| | Всего в мире | 4 574 150 134 | 360 985 492 | 7 796 615 710 | 6 145 006 989 | 1 267% |

1. URL: www.internetworldstats.com/top20.htm (дата обращения: 22.04.2020).

Особенно актуально все это для Азиатско-Тихоокеанского региона, в котором сегодня концентрируются многочисленные конфликтные ситуации, экономические противоречия, территориальные споры и геополитические уязвимости, которые насыщают регион новыми рисками и угрозами. Азия — самый крупный по территории и численности населения континент мира. Здесь находится пять из семи мировых центров высоких технологий. В «двадцатку» ведущих мировых стран по количеству пользователей Интернета входит 12 азиатских государств (табл. 1). Число Интернет-пользователей в этих странах превысило 1 млрд 910 тысяч человек, что составляет почти 70% от общего числа пользователей Интернета, входящих в лидирующую двадцатку (табл. 2). Безусловным лидером является Китай — 854 млн пользователей больше чем все население Европы. Китайский язык также занял одно из первых мест среди языков, получивших наибольшее распространение в Интернете (табл. 2).

*Таблица 2*

**Топ 10 языков, используемых в Интернете — 31 марта 2020 г.**
**(Число пользователей с разделением на языки)**

| 10 основных языков, используемых в Интернете | Население в мире, которое говорит на этом языке (по состоянию на 2020 г.) | Количество Интернет-пользователей, которые используют этот язык | Проникновение Интернета (% населения) | Прирост Интернет-пользователей (2000–2020) | Интернет-пользователи % от общего кол-ва в в мире (доля) |
|---|---|---|---|---|---|
| Английский | 1 531 179 460 | 1 186 451 052 | 77,5% | 742,9% | 25,9% |
| Китайский | 1 477 137 209 | 888 453 068 | 60,1% | 2 650,4% | 19,4% |
| Испанский | 516 655 099 | 363 684 593 | 70,4% | 1 511,0% | 7,9% |
| Арабский | 447 572 891 | 237 418 349 | 53,0% | 9 348,0% | 5,2% |
| Португальский | 290 939 425 | 171 750 818 | 59,0% | 2 167,0% | 3,7% |
| Индонезийский / Малазийский | 306 327 093 | 198 029 815 | 64,6% | 3 356,0% | 4,3% |
| Французский | 431 503 032 | 151 733 611 | 35,2% | 1 164,6% | 3,3% |
| Японский | 126 476 461 | 118 626 672 | 93,8% | 152,0% | 2,6% |
| Русский | 145 934 462 | 116 353 942 | 79,7% | 3 653,4% | 2,5% |
| Немецкий | 98 654 451 | 92 525 427 | 93,8% | 236,2% | 2,0% |
| Всего Топ 10 языков | 5 273 725 132 | 3 525 027 347 | 66,8% | 1 188,2% | 76,9% |
| Остальные языки | 2 522 890 578 | 1 060 551 371 | 42,0% | 1 114,1% | 23,1% |
| Всего в мире | 7 796 615 710 | 4 585 578 718 | 58,8% | 1 170,3% | 100,0% |

*Примечания: (1) Статистика для 10 основных языков, используемых в Интернете, была обновлена по состоянию на 31 января 2020 года. (2) Проникновение Интернета — это соотношение между суммой пользователей Интернета, говорящих на каком-либо языке, и общей оценкой населения, говорящей на этом конкретном языке. (3) Самая последняя информация об использовании Интернета взята из данных, опубликованных Nielsen Online, Международным союзом электросвязи, компанией GfK и других надежных источников. (4) Оценки населения основаны главным образом на данных Отдела народонаселения ООН и местных официальных источников. (5) Определения и методологию см. в Руководстве на сайте. (6) Можно ссылаться на данные с этого сайта с обязательным указанием ссылки www.internetworldstats.com. Copyright © 2020, Miniwatts Marketing Group. Все права защищены по всему миру.*

Среди стран-лидеров с наибольшим числом пользователей Интернета, как видно из табл. 1, то есть людей, работающих или обращающихся с разными запросами к киберпространству, находятся и другие азиатские страны — Индия (560,000,000 человек), Ин-

донезия (171,260,000), Вьетнам (68,541,344). Более того, из общего числа первой «двадцатки» стран с наибольшим количеством Интернет-пользователей 12 стран — это государства, расположенные в Азии либо примыкающие к азиатской зоне. Этот факт свидетельствует о том, что Китай постепенно становится современной киберсверхдержавой, способной бросить вызов любой высокоразвитой стране.

Анализ статистических данных в области развития мирового Интернета показывает, что азиатский континент занимает преобладающее положение в мировом киберпространстве. Больше половины всех пользователей Интернета живет сегодня в азиатских странах, и они составляют почти треть общего числа пользователей этой социальной сети в мире (табл. 3). С учетом остального мира соотношение по другим показателям почти не меняется. Азия лидирует и по количеству персональных компьютеров, и по количеству смартфонов. Причем этот показатель постоянно растет: общее количество подписчиков на мобильные Интернет-ресурсы в регионе выросло с 1,12 млрд в 2014 г. до 1,41 млрд в 2015 и 1,6 млрд в 2016 г.[2].

*Таблица 3*

**Использование Интернета в Азии[3]**

Количество пользователей Интернета, подписчики Facebook и статистика населения для 35 стран и регионов в Азии на 2020 год.

| Азиатский регион | Население (по состоянию на 2020 г.) | Население в % от мирового | Количество пользователей на 31 января 2020 г. | Проникновение Интернета (в % от населения) | % от всех пользователей Интернета | Пользователи Facebook на 31 января 2020 года |
|---|---|---|---|---|---|---|
| Азия | 4 294 516 659 | 55.1% | 2 300 469 859 | 53.6% | 50.3% | 867 984 000 |
| Остальные страны | 3 502 099 051 | 44.9% | 2 273 680 275 | 64.9% | 49.7% | 1 331 444 570 |
| Весь мир | 7 796 615 710 | 100.0% | 4 574 150 134 | 58.7% | 100.0% | 2 199 428 570 |

## Пользователи сети Facebook на 31 января 2020 года

Страны Азии являются лидерами и по числу участников социальной сети Фейсбук — почти 868 млн пользователей по состоянию на 1 февраля 2020 г. (табл. 3). Это составляет более половины от общего числа лидирующей двадцатки (1 млрд 51 млн) и больше 50% от общего количества пользователей Фейсбука во всем мире — 1 млрд 679 млн (табл. 3).

И эта цифра продолжает расти. Если учесть национальные социальные сети, то эта цифра увеличится в разы. Таким образом, Азия по этому показателю опережает Европу и обе Америки. В результате азиатский континент сегодня превратился в крайне важный перекресток в евразийском киберпространстве, где играет все более возрастающую роль в развитии цифровой экономики и электронной коммерции, а также в создании современного информационного общества.

Для того чтобы обеспечить континент и огромную армию сетевых пользователей необходимыми услугами, здесь создана, пожалуй, самая насыщенная, сверхмощная и разветвленная сервисная телекоммуникационная инфраструктура, которая опирается на

2. Asian mobile broadband market continues to grow strongly. URL: https://www.budde.com.au/Research/2017-Asia-Mobile-Infrastructure-and-Mobile-Broadband (дата обращения 27.04.2020).
3. Internet Usage in Asia. URL: https://www.internetworldstats.com/stats3.htm (дата обращения: 21.04.2020).

технологические разработки и техническое телекоммуникационное оборудование, нередко получаемое из Китая. Это обстоятельство создает для КНР ряд преимуществ, позволяющих контролировать столь обширную зону. Одновременно это делает регион очень уязвимым для внешнего вторжения и разрушения устойчивого функционирования находящихся в регионе телекоммуникационных систем, превращая проблему кибербезопасности в Азии в крайне актуальную в условиях острого противостояния США и КНР. Таким образом, можно констатировать, что лидерство Китая в сфере ИКТ и рост влияния Поднебесной на гигантском евразийском пространстве привели к американо-китайским технологическим войнам. А начинал Китай свой путь в киберпространстве очень скромно и без претензий. Амбиции появились позже.

## Как Интернет пришел в Китай

Интернет в КНР впервые был запущен 20 сентября 1987 г. В пекинском Институте физики и высоких энергий профессор Цянь Тянь-бай в рамках проекта CANET (Chinese Academic Network) отправил первое электронное письмо из Китая. Публичный доступ к Интернету был открыт лишь во второй половине 1990-х годов.

Одновременно Пекин стимулировал развитие сетевых ресурсов в стране, включая ведущие СМИ. Поскольку в 1990-х годах в мире началось развитие мультимедийных СМИ с использованием текстовой, фото- и видеоинформации, уже тогда возникло такое понятие, как «новые медиа». Развитие цифровых технологий и ИКТ, их внедрение фактически во все сферы государственной, экономической, производственной и общественной жизни обеспечивали рывок в научно-технологической сфере развитым странам мира.

Впервые с серьезными проблемами в информационном пространстве Китай столкнулся 26 апреля 1999 г., когда активизировался вирус «Чернобыль». Он повредил операционные системы более полумиллиона компьютеров по всему миру, уничтожил данные на жестких дисках и разрушил содержимое микросхем, отвечающих за работу системного программного обеспечения (ПО). Более трети поврежденных компьютеров оказались на территории континентального Китая. Чернобыльский вирус — это вредоносная компьютерная программа, предназначенная для заражения операционных систем на базе Windows®.

Первоначально он назывался вирусом CIH и Spacefiller. Название «Чернобыльский вирус» появилось потому, что его первая активация полезной нагрузки произошла 26 апреля 1999 г., в очередную годовщину Чернобыльской катастрофы. Вирус написан тайваньским студентом, который после активизации ВПО (вредоносное программное обеспечение) был арестован, отсидел в тюрьме, а после освобождения получил высокооплачиваемую работу в одной из крупнейших тайбэйских IT-компаний.

Однако после разрушительной атаки «Чернобыля» — самого настоящего боевого компьютерного вируса — использование боевых вирусов для подрыва кибервозможностей потенциального противника не прекратилось.

Вслед за первой последовала атака вируса «я люблю тебя», который также нанес значительный финансовый ущерб Интернет-пользователям в Азии и на Ближнем Востоке. Вирус поражал в первую очередь компьютеры с нелегальным и нелицензионным ПО, а также устройства, владельцы которых не желали использовать антивирусные программы. Очередная атака на компьютерные сети КНР произошла в начале нового столетия, когда вредоносному нападению подверглись сотни правительственных сайтов КНР, большая часть которых оказалась заблокирована более чем на сутки.

Под воздействием государства к началу 2000 гг. в КНР увеличилось число провайдеров Интернет-услуг. В настоящее время самыми крупными китайскими компаниями, предоставляющими услуги Интернета, являются China Telecom, China Mobile и China Unicom. Основная инфраструктура китайского сегмента Интернета состоит из девяти

Интернет-провайдеров, в ведении которых находятся все физические каналы, связывающие Китай с окружающим миром.

Китайский сегмент Интернета разделен на несколько специализированных сетей, в которые входят:

– научно-исследовательская сеть China Science and Technology Network (CSTNet, http://www.cnc.ac.cn), она объединяет НИИ, государственные научно-технические органы и некоторые академические учреждения;

– образовательная сеть China Education and Research Network (CERNET, http://www.edu.cn), объединяющая образовательные учреждения Китая, включая средние школы и университеты в крупных городах страны;

– коммерческие сети;

– наиболее крупные сети — China Net (http://www.bta.net.cn), государственная сеть, которая охватывает более 50% рынка Интернет-услуг в стране и предоставляет Интернет-сервис государственным организациям, а также Golden Bridge Network (GBNet, http://www.gb.co.cn).

Подобная специализация китайского Интернета облегчает работу пользователям в сети и позволяет быстро ориентироваться во всемирной паутине[4] в зависимости от целей и интересов; в то же время сегментация Интернета позволяет властям контролировать деятельность пользователей в киберпространстве. Со временем китайское руководство стало уделять больше внимания развитию Интернета и информационно-коммуникационных технологий.

На XIX съезде КПК в октябре 2017 г. Председатель КНР Си Цзиньпин, выступая с отчетным докладом, достаточно определенно высказался на этот счет: «Необходимо создать мощную опору для превращения Китая в одного из мировых лидеров в сфере науки и технологий, а также достижения качества продукции, космоплавания, сетевых технологий и транспорта, чтобы создать «цифровой Китай» и «умное общество»». Он подчеркнул, что необходимо уделять повышенное внимание созданию и обновлению средств распространения информации, наращивать потенциал СМИ в области распространения информации, ориентирования, оказания влияния и завоевания общественного доверия.

На XVIII съезде КПК было принято решение уделить особое внимание формированию «Чайна Нет» и придать этому процессу контролируемый и управляемый характер. В Отчетном докладе ЦК на сей счет подчеркивалась необходимость усиливать строительство Интернета и улучшать его содержание, во всеуслышание исполняя наш лейтмотив. Усиливать управление сетевым обществом, продвигая его нормированное и упорядоченное функционирование на правовой основе.

На следующем съезде эти тезисы были повторены: усилить работу по созданию контента сети Интернет, создать систему комплексного управления сетью и чистое киберпространство. Пятью годами раньше предыдущий генсек ЦК КПК Ху Цзиньтао, выступая на XVIII съезде КПК в ноябре 2012 г., также не прошел мимо темы строительства информационной системы и инфраструктуры. Он сказал, что важно приступить к созданию информационной инфраструктуры следующего поколения, обеспечивать развитие индустриальной системы современных информационных технологий, оздоровлять систему обеспечения информационной безопасности, поощрять широкое применение информационно-сетевых технологий.

При этом подчеркивалось, что…продолжают нарастать терроризм, киберугрозы, особо серьезные инфекционные заболевания, климатические изменения и другие нетрадиционные угрозы безопасности. Практическим результатом этих решений стало создание Руководящей группы и Администрации по делам киберпространства. В результате

4. *Англ.*: World Wide Web, сокр. www или Web.

система управления и контроля над информационным пространством страны приобрела целостный и четко структурированный характер. Это прослеживается, если мы обратимся к структуре Администрации по делам киберпространства (Схема 1).

Канцелярия по делам киберпространства превратилась в главный контрольный орган, администрирующий национальное киберпространство в Китае. Канцелярия напрямую подчиняется Руководящей группе ЦК КПК по делам Интернета во главе с Си Цзиньпином и двумя заместителями (премьер Госсовета КНР Ли Кэцян и завотделом пропаганды ЦК КПК, член Политбюро Лю Юншань). В состав Руководящей группы входят 19 членов. Руководитель Канцелярии — Сюй Линь (он же — секретарь Руководящей группы). В структуру Канцелярии входят 9 департаментов, отвечающих за анализ состояния информационного пространства, координацию работы по обеспечению информбезопасности, международное сотрудничество, контроль над мобильным Интернетом, распространением онлайн новостей и так далее. В структуру входят также три Центра, которые занимаются реагированием на киберугрозы, исследовательской работой, сбором и обработкой заявлений от населения о распространении в сети зловредной и фейковой информации (Схема 1).

Сюй Линь руководил Администрацией по киберпространству до 31 июля 2018 г. и сегодня возглавляет Пресс-канцелярию Госсовета КНР. После него руководство Администрацией перешло к Си Цзиньпину, который сохранил за собой пост председателя Центральной Комиссии по делам киберпространства, а также контроль над руководящей группой по кибербезопасности и информатизации.

*Схема № 1*


Обратим внимание, что в 2006 г. в Китае была создана интернет-полиция. Первоначально на нее возлагались задачи по расследованию и пресечению киберпреступлений, различных видов мошенничества, финансовых пирамид, фактов незаконного оборота наркотиков и психотропных средств, огнестрельного оружия. Функции интернет-полиции со временем расширились. Сегодня на нее, по сути, возложены обязанности цензоров. Интернет-полиция отслеживает и пресекает распространение в сети ложной информации, необоснованных слухов и «фейков», которые возбуждают население, сеют межнациональную рознь или содержат призывы к борьбе против конституционной власти.

Одновременно Китай приступил к формированию юридическо-правовой базы для работы с цифровым пространством, обращая первостепенное внимание на вопросы обеспечения кибербезопасности. В течение короткого времени был принят ряд документов в этой сфере, в том числе:

– Закон о государственной безопасности (утвержден 1 июля 2015 года на 15-м заседании ПК ВСНП);

– Закон о кибербезопасности КНР (принят в октябре 2016 года, вступил в силу 1 июня 2017 года);

– «Международная стратегия сотрудничества в киберпространстве» (International Strategy of Cooperation on Cyberspace), опубликована 1 марта 2017 года;

– Поправки в Уголовный кодекс, внесенные в августе 2015 года, о наказаниях за правонарушения в киберпространстве;

– «Законодательные и нормативные акты по усилению законодательства в сети Интернет, совершенствованию сетевых информационных служб, обеспечению Интернет-безопасности, управлению Интернет-сообществом и приведению сети Интернет к нормам законодательного порядка».

За последние 17 лет Китай привел систему управления киберсферой в действующую на разных уровнях структуру, обладающую мощным кадровым составом и техническими возможностями. В 2001–2013 гг. Государственный совет КНР провел реформу кабинета министров, заново сформировав Министерство промышленности и информатизации. Таким образом, все рабочие обязанности, связанные с практическими проблемами информатизации страны, сосредоточены в данном министерстве. Также сформирована Государственная канцелярия по делам сети Интернет, отвечающая за распространение информации в сети в области политического курса и построения правовой системы.

Сформированы и неправительственные организации: 25 мая 2001 года было официально создано Общество Интернета КНР, состоящее более чем из семидесяти представителей интернет-отрасли Китая, среди которых — поставщики интернет-услуг, производители оборудования, системные интеграторы, научно-исследовательские компании, образовательные учреждения.

К марту 2016 г. в КНР приняли 41 закон, 46 административно-правовых актов Государственного совета КНР, 37 разъяснений по вопросам судебной практики, 274 регламента аппарата правительства, 133 местных нормативных акта, 138 регламентов местного значения, а всего — 669 документов, которые регулируют поведение в информационном поле страны.

Тем не менее, по мнению китайских специалистов в области информационной безопасности, Китай стоит лишь в начале пути по созданию правового фундамента в области регулирования этой сферы.

Параллельно с решением юридических и правовых вопросов функционирования цифрового пространства, укрепления регулирования и контроля над ним, Китай активно работал над техническими задачами по наращиванию скорости передачи информации по мобильным каналам. 23 апреля 2018 г. китайцы запустили в мегаполисе Чунцин первую тестовую сеть формата 5G. Его массовый запуск ожидается в 2020 г.

## Китайско-американский киберконфликт

Хотя это событие было ожидаемым, поскольку Пекин объявил о готовящемся запуске формата 5G, в Вашингтоне запаниковали и, как это уже случалось неоднократно, развернули санкционное давление по отношению к китайским компаниям, которые заняты разработкой и внедрением новейших ИКТ. Пожалуй, американцы впервые почувствовали, что теряют лидерство в технологической области, что, в свою очередь, угрожает американскому господству в киберпространстве, а также в сфере управления «всемир-

ной паутиной». Реакция Вашингтона не заставила себя ждать. Прямому давлению подверглись китайские успешные компании «Хуавэй»[5] и ZTE[6]. Были введены запреты на покупку китайского оборудования.

В 2018 г. доход Huawei превысил 100 млрд долл., позволив ей обогнать Ericsson и Boeing. В феврале 2020 г. появились сообщения о том, что американцы намерены заблокировать доступ компании «Хуавэй» к электронным компонентам американского и иного производства. 15 мая 2020 г. госсекретарь США Майк Помпео объявил о намерении Вашингтона запретить иностранным компаниям продавать микрочипы Китаю. Речь идет о производителях, которые используют американское оборудование и программное обеспечение (ПО) для производства микрочипов. Это решение Помпео мотивировал тем, что китайские хакеры неоднократно пытались нелегально проникнуть во внутренние сети исследовательских центров, которые занимаются разработкой вакцины против коронавируса и даже добились в этом успеха.

Следует также отметить, что продажа микрочипов Китаю была запрещена еще в первом десятилетии нового столетия, и поскольку Китай покупал микросхемы в Японии и Южной Корее, союзникам США в Восточной Азии было рекомендовано заблокировать доступ КНР к японским и южнокорейским микрочипам. Администрация США предприняла меры и для того, чтобы также ограничить доступ КНР к производителям микросхем на Тайване.

Ранее были введены ограничения на продажу в Китай не только микросхем и новейшего телекоммуникационного оборудования, но и американского программного обеспечения. Вашингтон потребовал от своих союзников сделать то же самое.

Одновременно американцы оказали на своих союзников в Европе грубое давление, для того чтобы они отказались приобретать оборудование китайских компаний или сотрудничать с ними. От использования оборудования этих компаний отказалась Польша. Сомнение в целесообразности сотрудничества с ZTE и «Хуавэй» выразила Германия. К бойкоту китайской телекоммуникационной продукции присоединились и другие европейские страны.

Давление США на «Хуавэй» и ZTE обозначило начало американо-китайских технологических войн и откровенное вторжение в международную торговую политику, а также перенос в информационное пространство методов американского торгового про-

5. Компания «Хуавэй» — Huawei Technologies Co. Ltd. (华为技术有限公司, Huáwèi Jìshù Yǒuxiàn Gōngsī) — одна из крупнейших мировых компаний в сфере телекоммуникаций. Основана в 1987 г. бывшим инженером Народно-освободительной армии Китая Жэнь Чжэнфэем. Председатель совета директоров — Сунь Яфан, Штаб-квартира находится в Шэньчжэне, исследовательский центр — в Пекине. Продукция: телекоммуникационное оборудование, оборудование беспроводных сетей (LTE/HSDPA/W-CDMA/EDGE/GPRS/GSM, CDMA2000 1xEV-DO/CDMA2000 1X, TD-SCDMA), оборудование базовой сети (IMS, Mobile Softswitch, NGN), сетевые устройства (FTTx, xDSL, оптические устройства, маршрутизаторы, сетевые коммутаторы). Занимается также разработкой программ ОС для своей продукции, оборот: 75,103 млрд долл. (2016 г).
6. ZTE Corporation (中兴通讯) — китайская компания, второй по величине производитель телекоммуникационного оборудования и мобильных телефонов в Китае (на 2011 год). Основана в 1985 г. Штаб-квартира находится в городе Шэньчжэне. В 1997 г. компания внесена в листинг Шэньчжэньской фондовой биржи, а с декабря 2004 г. зарегистрирована на Гонконгской фондовой бирже. Входит в состав индекса Hang Seng China Enterprises Index. Председатель совета директоров — Ли Цзысюэ (李自学). Продукция: телефоны, телекоммуникационное оборудование для фиксированной и мобильной связи. Оборот 12,2 млрд долл. (2013 г.). В компании работают более 85 тыс. сотрудников (на 2010 г.). По результатам 2010 г. на рынке мобильных телефонов по версии IDC компания заняла 4-е место среди крупнейших производителей (в штучном выражении).

текционизма, ставшего отныне новой формой недобросовестной конкуренции — киберпротекционизмом, что означало также перенос конкурентной борьбы в киберпространство. Американцы особенно не скрывали, что китайские технологии создают прямую угрозу США в области военного применения новых телекоммуникационных технологий. К тому времени стало ясно, что запуск формата 5G неизбежно дает владеющему этой технологией преимущества в оборонной сфере, потому что скорость передачи цифровой информации в мобильном сегменте непосредственно влияет на повышение эффективности применения БПЛА и других беспилотных военных аппаратов.

Стало известно, что Китай проводит активные исследования в области создания искусственного интеллекта. Работы в этом направлении ведутся в Академии национальной обороны, в ведущих исследовательских учреждениях Пекина, Шанхая, Гуанчжоу, Чэнду и других городов КНР.

В настоящее время образовалось несколько направлений, на которых развернулось острое противостояние США и КНР: площадка двусторонней торговли, борьба с коронавирус и, разумеется, информационно-коммуникационные технологии. Причем представляется, что площадка ИКТ рассматривается Вашингтоном в качестве той, где он сможет обыграть Пекин и принудить его принять американские условия по другим двусторонним проблемам. Сегодня китайцы добились определенных успехов в области кибероборонны, противодействия внешним киберугрозам и информационным атакам.

Следует отметить, что Китай уделяет повышенное внимание вопросам разработки современных средств кибервойны. Исследователь ПИР-Центра Галия Ибрагимова убеждена, что в китайской армии существуют хорошо обученные специальные подразделения, специализирующиеся на кибервойнах и способные при необходимости вывести из строя большинство объектов информационной инфраструктуры США.

## Китайские подходы к проблемам ведения войны в киберпространстве

Согласно распространенной в Китае точке зрения, киберпространство несет две основные угрозы государству: кибершпионаж и ведение активных информационных операций с целью подрыва социально-политической стабильности и вовлечения широких слоев китайской общественности в антиправительственные протестные акции. Медийно-информационная сфера — единственное направление кибердеятельности, где американцы имеют богатейший опыт и преимущества перед китайцами, которые слишком много внимания уделяют идеологическим аспектам в проведении информационной политики. Американцы вот уже много лет используют огромный и мощный арсенал подрывной информационной работы, а также широкий набор методов ведения психологической войны. Но как бы то ни было, противоборство в киберпространстве рассматривается специалистами КНР по аналогии с военными действиями на трех уровнях: тактическом, оперативном и стратегическом.

Тактический уровень противоборства в киберпространстве — это «рутинная», ежедневная деятельность, которая заключается в попытках хищения информации и атаках на компьютерные системы рядовых граждан, фирм и компаний. Оперативный уровень предполагает крупномасштабные атаки, такие как DDoS-атаки на Bank of America и другие банки, или применение вируса Stuxnet, как в Иране. На данном уровне противоборства в киберпространстве можно спровоцировать социальное недовольство внутри страны (как в случае с Эстонией в 2007 г.), а также рост напряженности в отношениях между странами. На тактическом и оперативном уровнях противоборство в киберпространстве становится предметом юридического внимания и требует внедрения единообразной терминологии и исследования с точки зрения права.

Согласно сообщениям западных СМИ, Китай развивает практически все направления военной деятельности в цифровой среде: занимается активной разведдеятельно-

стью, проведением кибератак, кражами документации технологического и военного характера и пр. Сообщение в июне 2010 г. о том, что компьютерный вирус американского происхождения под названием Stuxnet[7] поразил иранскую атомную электростанцию Натанц, означало, что сложились условия для информационной войны. Stuxnet инфицировал более 60000 компьютеров. Из них свыше половины находились в Иране, остальные пострадавшие страны — это Индия, Индонезия, Китай, Азербайджан, Северная Корея, Малайзия, США, Великобритания, Австралия, Финляндия и Германия.

Заметим, что благодаря разработке новых антивирусных программ и встроенной дате окончания срока действия вируса способность этого «троянского коня» к дальнейшему распространению ослабла.

Китай стал одной из первых стран, испытавших на себе разрушительную мощь кибероружия. Именно это обстоятельство заставило Пекин заняться разработкой и формированием арсенала кибероружия, а также изучением методов ведения кибервойн. Хотя достоверной информации на этот счет чрезвычайно мало (в основном, это ангажированные американские источники, ведущие против Китая открытую информационную войну), не приходится сомневаться в том, что в КНР такие разработки проводятся. Между тем, лидирующая роль в разработке боевых вирусов и создании соответствующих арсеналов принадлежит США.

В ходе XVIII съезда КПК были поставлены новые задачи для дальнейшего военного строительства в Китае с учетом бурного развития информатизации, киберпространства и новых телекоммуникационных систем. «Необходимо, продолжая ориентироваться на самые основные потребности безопасности страны, — подчеркивалось на съезде, — планируя вместе экономическое и оборонное строительство и держась «трехшагового» стратегического плана модернизации национальной обороны и армии, форсировать выполнение механизации и информатизации, как двойной исторической задачи, и постараться к 2020 году в основном закончить механизацию, а в области информатизации обеспечить серьезные сдвиги».

В 2016 г. было официально объявлено о создании в составе НОАК специальных формирований для обеспечения кибероборонны и противодействия кибератакам, направленным на критически важные инфраструктурные объекты Китая. Как показывает анализ китайской политики в области кибероборонны, Пекин решил не отставать от лидеров разработки военной киберстратегии, в частности — от США, поскольку в американской стратегии современного военного строительства информационным войнам отводится чрезвычайно важная роль.

К настоящему времени возникла ситуация, при которой киберпространство рассматривается, как зона ведения информационных, финансовых, экономических и иных войн. Выработка взаимоприемлемых подходов и правил организации деятельности в Интернете требует учета как всего многообразия и многофункциональности киберпро-

7. Stuxnet — сложная компьютерная вредоносная программа, предназначенная для проникновения в удаленные системы и установления над ними контроля в квазиавтономном режиме. Она представляет собой новое поколение вирусов «запусти и забудь», которые могут быть нацелены на определенные объекты в киберпространстве. Те объекты, на которые был направлен Stuxnet, располагались в «воздушном мешке», другими словами, они не были подключены к общественной сети Интернет и проникновение в них требовало использования промежуточных устройств, например, флеш-накопителей, чтобы получить доступ к ним и установить контроль. Используя четыре «уязвимости нулевого дня» (ранее неизвестные уязвимости, чтобы не было времени создать и распространить патчи), вирус Stuxnet задействует базовые пароли Siemens для доступа к операционным системам Windows, на которых запущены программы WinCC и PCS 7.5. Это программируемые логические контроллеры (PLC), управляющие промышленными предприятиями.

странства в целом, так и особенностей национальных сегментов Интернета. Активно создаются арсеналы боевых вирусов, разрабатываются инструменты, тактика и стратегия военных действий в киберпространстве, целью которых становятся намерения нанести как можно больший экономический, социально-политический и технологический ущерб потенциальному противнику.

Следует отметить, что тенденции к консолидации действий в киберпространстве, к выработке кодекса поведения испытывают на себе всю специфику развития современной международной обстановки. Европейские страны НАТО и Соединённые Штаты вырабатывают обособленные нормы поведения в киберпространстве, привлекая к этому процессу Южную Корею и Японию. Вопросы сотрудничества в обеспечении безопасности в киберпространстве находятся и в поле зрения членов Шанхайской организации сотрудничества (ШОС).

* * *

В основе американской стратегии в области кибероборонs лежит противодействие планам Пекина по достижению Китаем превосходства над Америкой в цифровой зоне, достижению технологических преимуществ в сфере современных информационно-коммуникационных технологий. Американцы также стремятся не допустить выхода Китая на внешние рынки со своими ИКТ, способными составить конкуренцию американским телекоммуникационным компаниям, которые сегодня сохраняют американскую монополию на продажу базового оборудования для развития и обслуживания современной киберсреды. Кроме того, США стремятся к лидирующей роли в информационном пространстве и в области телекоммуникационных технологий. Для них необходимо обеспечить защиту от китайских кибератак критически важной инфраструктуры, и прежде всего — в оборонной области и сфере ИКТ. С этой целью американцы активно используют свои конкурентные преимущества, оказывают давление на страны, приобретающие китайское оборудование, стремятся подорвать критически значимую для развития ИКТ инфраструктуру, организуя кибератаки и оказывая прямое давление на китайские компании типа «Хуавэй» или ZTE.

Более 10 лет Китай ведет переговоры по проблемам кибернетической безопасности с США и рядом других стран. Определяющими для него в этой области являются киберотношения с Америкой. Именно оттуда нарастает давление на КНР по вопросам кибербезопасности, развития цифровой среды и новых технологий, а сам Китай обвиняется в организации проникновений в сетевые ресурсы минобороны, спецслужб, крупнейших компаний США, занятых, в первую очередь, в сфере военного производства. Начиная с 2016 г. напряжение в китайско-американском диалоге по информационной безопасности уменьшилось. США сконцентрировали свое внимание на так называемом вмешательстве России в президентские выборы в США 2016 года и деятельности «пропагандистских СМИ Москвы».

Впервые китайские армейские подразделения для противодействия кибератакам, пресечения незаконной деятельности по выявлению уязвимостей в национальном сегменте киберпространства и противостояния зарубежным кибератакам были созданы в 2012 г. В задачу киберсолдат НОАК входили не только вопросы защиты национального киберпространства и объектов критической инфраструктуры, но также ведение разведки по отношению к потенциальным противникам, проникновение в закрытые цифровые сети с целью получения доступа к информационно-коммуникационным технологиям, в центры контроля и управления боевыми дронами и БПЛА.

Судя по резко негативной риторике Вашингтона, первоочередной целью китайского кибершпионажа и взлома закрытых информационных ресурсов стали объекты, расположенные на территории США. Вместе с тем аналогичные операции проводились против Южной Кореи, Японии, где также были созданы военные структуры, специализи-

рующиеся на кибероборо не, и которые были вовлечены в проведение кибероперaций НАТО против КНР.

Южнокорейские и японские киберсолдаты проходили переподготовку на базе таллинского Руководства в области кибероборо ны, которое является структурой Североатлантического альянса и создано в Эстонии для проведения тайных кибероперaций против России и ее союзников по ОДКБ и ШОС, против КНДР и других стран. После 2010 г. южнокорейские и японские киберспециалисты неоднократно участвовали в военных киберучениях НАТО, проходили переподготовку в киберструктурах альянса. Япония впоследствии официально присоединилась к таллинскому Руководству в области кибероборо ны.

В этом контексте уместно напомнить, что и Токио, и Сеул официально являются военными союзниками США и, разумеется, могут быть привлечены к участию в тайных кибероперaциях против КНР, Северной Кореи, России и других стран Восточной Азии. Важно при этом обратить внимание на оборонную сферу в киберполитике Китая. По мнению европейских и американских экспертов, в Китае уже разработана и применяется соответствующая военная стратегия в кибернетической сфере, включая возможность ведения информационной войны (ИВ).

В китайской стратегии информационных войн обычно выделяют три аспекта. Во-первых, китайские военные исходят из того, что ИВ является продуктом эпохи информатизации, при этом используются цифровые технологии и информационное оружие. Происходит «сетевизация» (wangluohua) поля боя, и в центре противостояния оказываются борьба за контроль над информационным пространством и нейтрализация средств информационной безопасности потенциального противника.

Во-вторых, информационная война — это высокотехнологичное поле боя, в котором противники используют информационно-технологические средства, оборудование или системы в борьбе за преобладающее влияние в киберпространстве и захват инициативы на поле боя; при этом основной боевой силой являются цифровые устройства. В-третьих, главная цель ИВ должна состоять в нападении на информационные системы противника при защите собственной информационной инфраструктуры.

По мнению зарубежных аналитиков, изучавших китайские источники, целью ИВ, судя по китайской литературе, является информационное господство [制信息权]. Подобно американскому понятию «информационного превосходства» в ИВ, китайцы будут стремиться разрушить процесс принятия решения противником, оказывая воздействие на его способность получать, обрабатывать, передавать и использовать информацию. Паралич системы информации и процесса принятия решений противником должен, в свою очередь, подавить волю соперника к сопротивлению или борьбе.

По мнению американского исследователя проблем информбезопасности в АТР Тоши Ёшихара, Китай продемонстрировал интенсивное увлечение информационной войной. Потенциальное продвижение в китайскую военную доктрину ИВ имеет прямое отношение к национальной безопасности США. Способность Китая к ведению ИВ против Соединённых Штатов в мирное время может создать серьезные проблемы перед теми, кто занимается планированием в области обороны.

Еще одной важной сферой для китайской стратегии информационной безопасности стала защита внутреннего информационного пространства от вмешательства извне, а также противодействие попыткам разрушить идеологический контроль властей над Интернетом.

Следует обратить внимание еще на одно обстоятельство: в рамках модернизации НОАК основное внимание уделяется информатизации и компьютеризации войск и сил флота, усилению боевых возможностей вооруженных сил за счет повышения эффективности взаимодействия видов вооруженных сил и родов войск в совместных операциях. Конечная цель при этом заключается в создании вооруженных сил, способных эффектив-

но осуществлять стратегическое ядерное сдерживание, успешно действовать в высокотехнологичной войне локального масштаба, а также при проведении антитеррористических операций.

Справедливости ради стоит отметить, что Китай в рамках киберсоперничества с США находится в положении догоняющей стороны. Более того, разрабатывая собственную методику ведения ИВ, он заимствует, активно использует и применяет американский опыт подготовки к кибервойнам. Данное обстоятельство касается как создания национальных кибервойск, так и арсеналов боевых вирусов, а также использования нелегальных хакерских группировок против своих соперников.

При этом китайская дипломатия ведет широкий диалог по проблемам корректного поведения в современном киберпространстве. Это обсуждение происходит как в рамках китайско-американского стратегического диалога, так и на уровне спецпредставителей. Тем не менее, между китайскими и американскими властями сохраняются острые противоречия по вопросу безопасности в киберпространстве.

13 сентября 2015 г. специальный представитель правительства Китая Мэн Цзяньчжу обсудил в Вашингтоне с коллегами из администрации США вопросы киберпротивостояния, вызывающие серьезные противоречия между двумя странами, а также проблемы кибербезопасности. Однако диалог между китайскими и американскими властями так и не сгладил острые противоречия между ними по этим пунктам.

По утверждению американских и европейских источников, Китай привлекает местные хакерские группировки к проведению кибероперациий. Сегодня одной их самых известных групп, действующих с территории Китая, является «Альянс красных хакеров» (англ. Red Hacker Alliance, кит. 中国 红 客 联盟) — неформальное объединение китайских хакеров, численность которого, по некоторым оценкам, составляет более 80 тыс. человек, что делает его одной из крупнейших хакерских групп в мире. Альянс позиционирует себя как китайская общественная организация. Однако зарубежные источники отмечают, что действия и операции Альянса координирует известное подразделение НОАК № 61398, которое базируется в Шанхае и на которое возложена задача проведения военных операций в компьютерных сетях. По оценкам российских экспертов в сфере информационной безопасности В. Овчинского и Е. Лариной, Альянс включает хакеров не только из самого Китая, но и из китайской диаспоры во всем мире и тесно взаимодействует с Третьим и Четвертым управлениями Генерального штаба НОАК.

Западные источники утверждают, что именно хакеры Альянса несут ответственность за организацию DDoS-атак на ведущие СМИ США. Другие источники уверены, что опыт Альянса в организации DDoS-атак был также использован летом 2019 г. против участников массовых протестов в Гонконге. Тогда в результате DDoS-операции удалось заблокировать мессенджеры смартфонов, через которые осуществлялась координация действий протестующих. Одновременно DDoS-атаке в Азии подвергся популярный сервис обмена сообщениями Telegram. В результате в среду, 12 июня 2019 г., этот сервис на короткое время стал недоступен для сотен тысяч пользователей по всему миру[8].

В январе 2016 г. было официально объявлено о создании в армии КНР кибервойск. В рамках углубленной реформы вооруженных сил Центральный военный совет (ЦВС) Китайской Народной Республики анонсировал появление новых родов войск. В составе Народно-Освободительной армии Китая (НОАК) появились Силы стратегической поддержки, куда вошли ракетные войска, кибервойска и Центр армейского командования[9].

8. DDoS-атака лишила сотни тысяч пользователей доступа к Telegram. URL: https://www.securitylab.ru/news/499455.php (дата обращения: 30.042020).
9. В армии КНР официально созданы кибервойска. Сообщение securenews.ru от 6 января 2016 г. URL: https://securenews.ru/chinese_cyberarmy/ (дата обращения. 19.05.2020).

На официальном сайте китайского Министерства национальной обороны указывается, что 31 декабря 2015 г. Председатель КНР Си Цзиньпин, являющийся одновременно главой Центрального военного совета, вручил знамена новых родов войск их командующим. Си Цзиньпин подчеркнул необходимость укреплять возможности страны в области кибероборонны. Основные направления обеспечения защиты информационного, сетевого пространства сегодня выглядят следующим образом:

– защита персональной информации и Big Data;

– защита финансово-банковской системы страны;

– защита от проникновения и кибератак на отраслевые сети (энергетика, производство, стратегические отрасли) и информационные системы управления;

– выявление и ликвидация последствий киберпреступлений;

– борьба с кибертерроризмом;

– контроль за распространением всех видов информации; недопущение циркуляции слухов, «непроверенной» информации, которые наносят вред национальной безопасности и нарушают закон о гостайне;

– обеспечение безопасности телекоммуникационных сетей, защита программ, связанных с развитием ИКТ;

– обеспечение безопасной электронной торговли и ресурсов по развитию цифровой экономики;

– защита отечественных производителей в области ИКТ;

– обеспечение развития информационного общества с китайской спецификой;

– развитие международного сотрудничества.

Еще одним направлением деятельности подразделений кибероборонны Китая стало использование арсеналов информационного противодействия в отношении организаторов массовых протестов и политических демонстраций.

Как заявил Си Цзиньпин, переформатирование структуры войск осуществляется с целью превращения НОАК из армии регионального и оборонительного типа в армию, которая будет способна вести весь спектр боевых операций. Председатель КНР также отметил, что формирование новых родов войск — важный стратегический шаг на пути к созданию современной военной системы с учетом китайской специфики.

Процесс преобразования китайских вооруженных сил предполагалось завершить к 2020 г., а реализация основных структурных изменений в рамках реформы будет осуществлена до конца того же года. Силовые структуры для работы с киберпространством в Китае появились фактически в первом десятилетии нового века.

Таким образом, современная деятельность Китая в мировом киберпространстве свидетельствует о том, что Пекин усиливает свое присутствие в цифровой зоне, в том числе и военное.

Китайские хакерские объединения стремятся получить доступ к военным, технологическим и коммерческим секретам других стран. Выявилась также тенденция применения хакерских арсеналов и методик для нейтрализации социально-политических протестов внутри своей страны, и эта тенденция, судя по всему, будет усиливаться. В то же время необходимо признать, что Китай и сам часто превращается в объект серьезных атак в национальном сегменте Интернета, а потому заинтересован в решении проблем обеспечения кибербезопасности в национальном сегменте киберпространства.

Вот уже многие годы Китай борется за то, чтобы стать полноценным участником управления информационным пространством, и объясняет свое желание тем, что является одним из мировых лидеров в области разработки и производства телекоммуникационного оборудования.

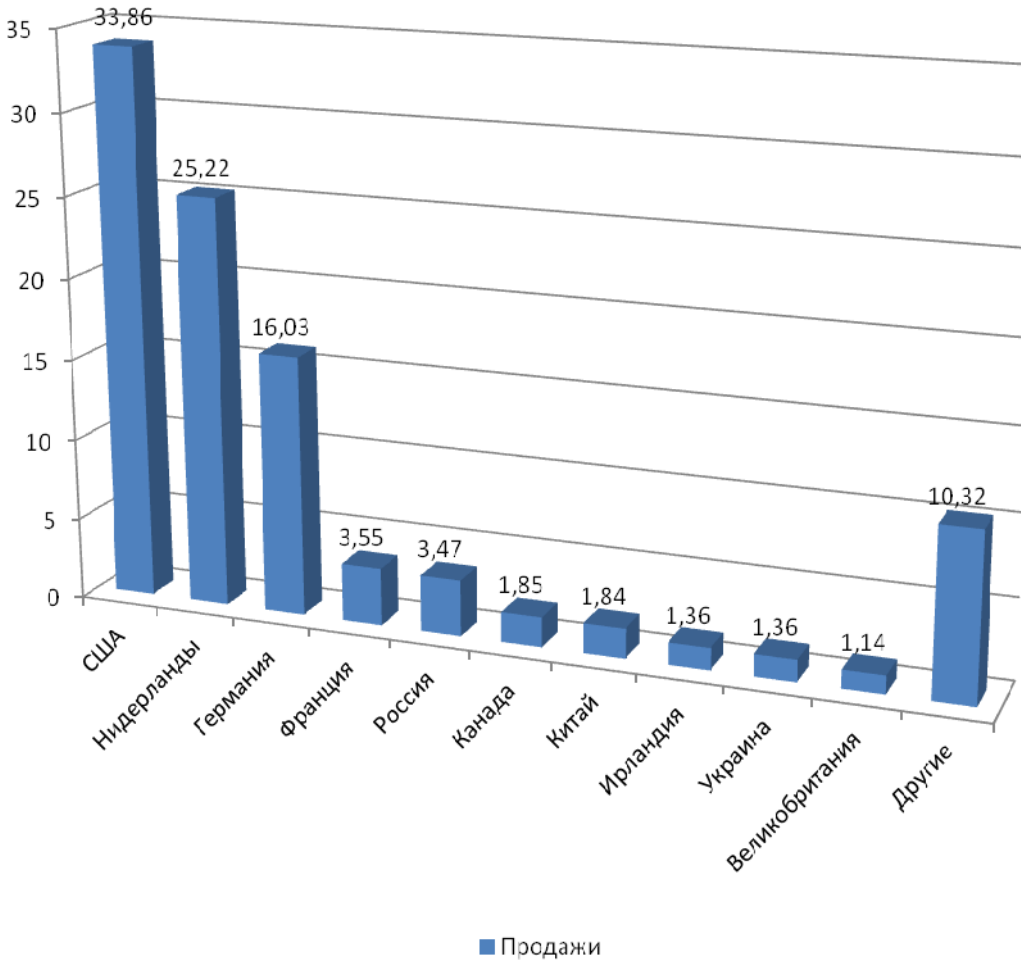
Следует отметить, что в настоящее время Китай уделяет повышенное внимание вопросам разработки современных средств кибервойны. Эксперты убеждены, что китай-

ские специальные подразделения способны при необходимости вывести из строя большинство объектов информационной инфраструктуры США[10].

*Диаграмма 1*

**Страны- источники веб-атак: «Первая десятка»**
**(сентябрь — декабрь 2017 года)**

*(по данным аналитиков Лаборатории Касперского)*




Справедливости ради отметим, что лидерство во вредоносной деятельности в информационном пространстве принадлежит вовсе не Китаю. По данным Лаборатории Касперского за сентябрь-декабрь 2017 г. — рекордного года по количеству вирусных атак во втором десятилетии XXI века — вирусные атаки, в основном, исходили от Соединённых Штатов. Более трети всех кибератак в мире в четвертом квартале 2017 г. было осуществлено с территории США (диаграмма 1).

10. *Галия Ибрагимова.* Стратегия КНР в области управления интернетом // Индекс безопасности. No. 1. (104). 2013. С. 169.

Еще одной важной сферой для китайской стратегии информационной безопасности стала защита внутреннего информационного пространства от вмешательства извне, идеологический контроль над ним. Как отмечалось выше, одной из форм обеспечения безопасности в социально-политической сфере стало блокирование доступа к сетевым ресурсам и информационным сервисам, содержание которых противоречит политико-идеологическим установкам официального руководства страны и затрагивает систему государственной власти в КНР. Представляется, что такая форма в определенной степени противоречит сегодняшней тенденции к созданию информационного общества, нарушает права людей на открытый доступ к информации.

## Заключение

Подводя итоги, следует отметить, что:

1. за последнее десятилетие благодаря успешному развитию собственных информационно-коммуникационных технологий, Китай значительно укрепил свои позиции в мировом киберпространстве.

2. Пекин обращает первостепенное внимание на развитие собственных сил реагирования на случай возникновения угроз и рисков национальной безопасности страны, и в первую очередь это касается развития способности ведения боевых действий в цифровой среде и создания средств защиты критически важной информационной инфраструктуры.

3. Китай активно ищет возможности решения проблем кибербезопасности на международном уровне как на двусторонней, так и на многосторонней основе.

4. Одной из важнейших целей китайской стратегии в цифровом пространстве стала задача по достижению статуса государства, являющегося признанным участником международной системы управления Интернетом.

5. Большое внимание в киберстратегии Китая уделяется оборонным аспектам развития цифровой среды. При этом основной упор делается на достижение военно-технологического превосходства в киберпространстве.

6. Понимая, что независимая и самостоятельная политика в информационном пространстве, а также сохранение суверенитета в национальном сегменте Интернета могут быть обеспечены только благодаря техническим и технологическим возможностям и собственной производственной базе по выпуску необходимого телекоммуникационного оборудования, Китай активно стимулирует научные исследования и развитие производства в области ИКТ, включая производство микросхем и мощных серверов.

7. Американо-китайское соперничество в киберсреде выявило явное отставание КНР в области программирования, необходимого для функционирования мобильного Интернета и других современных информационных систем. Эта проблема нарастает по мере того, как США выстраивают систему преград и ограничений для доступа китайцев к американскому программному обеспечению.

8. Запуск китайцами в 2017 г. формата 5G выявил достаточно высокий уровень научных исследований в Китае в области современных информационных технологий, позволяющих ему добиться технологического превосходства над американцами. В то же время это обстоятельство привело к обострению американо-китайского киберсоперничества и заставило говорить о возникновении нового фактора нестабильности в киберпространстве — технологических войн между конкурирующими странами.

9. Принимая во внимание весь комплекс факторов, определяющих рост влияния КНР в информационном пространстве, а также современные производственно-технологические возможности Пекина, можно с полной уверенностью констатировать, что Китай превращается в мировую киберсверхдержаву, и это обстоятельство будет стимулировать американо-китайское противостояние в информационном пространстве.

В целом же следует отметить необходимость и крайнюю актуальность разработки новых подходов к решению проблем кибербезопасности и избавления цифровой среды от милитаризации.

## Литература

*Галия Ибрагимова.* Стратегия КНР в области управления Интернетом // Индекс безопасности. No. 1. (104). 2013.

## References

Galiya Ibragimova, Strategiya KNR v oblasti upravleniya internetom, zhurnal «Indeks bezopasnosti» No. 1 (104) 2013.