**Китайская система обеспечения кибербезопасности**

**2018**

**Вернуться в каталог готовых дипломов и магистерских диссертаций –**

[**http://учебники.информ2000.рф/diplom.shtml**](http://учебники.информ2000.рф/diplom.shtml)

**Содержание**

Введение

. Структура системы обеспечения китайской кибербезопасности

.1 Подразделения КПК, отвечающие за кибербезопасность

.2 Военные структуры, ответственные за кибер-операции

.2.1 Третье управление НОАК

.2.2 Четвертое управление НОАК

.2.3 Военные реформы НОАК

.2.4 Китайское видение Третьей стратегии компенсации США

.3 Гражданские органы по управлению кибербезопасностью

. Контроль над интернетом в Китае

. Китай и международные отношения в киберпространстве

. Законодательный фрэймворк киберпространства

.1 Ключевые моменты закона о кибербезопасности

.2 Особенности нового закона о кибербезопасности

Заключение

Литература

**Введение**

Человечество вошло в новую эпоху информационной революции. Ускоренное развитие информационных и коммуникационных технологий, представленное в первую очередь Интернетом, изменило не только способ производства товаров и услуг, но и жизнь людей в целом — способствовало ускорению инноваций, экономическому процветанию и социальному развитию. Киберпространство (информационное пространство) стало новым каналом для распространения информации, новой областью жизни и работы людей, новым двигателем экономического роста, новым источником культурного богатства, новой платформой социального управления, новым средством для коммуникации и сотрудничества, а также и новой областью государственного суверенитета.

Однако киберпространство создает не только возможности, но и поднимает ряд вопросов. В данный момент на глобальной повестке дня стоит проблема безопасности и стабильности в киберпространстве, затрагиваются такие понятия как суверенитет, национальные интересы развития всех стран и безопасность. Для киберпространства как глобальной среды характерны неравномерное технологическое развитие, неполноценные «правила игры», неравноправный международный порядок. Стоит отметить, что информационный разрыв между странами и регионами постоянно увеличивается. Так, США объявили о Третьей стратегии компенсации — по мнению ряда исследователей, непосредственный ответ на активные военные и технологические преобразования в Китае.

|  |
| --- |
| [Вернуться в библиотеку по экономике и праву: учебники, дипломы, диссертации](http://учебники.информ2000.рф/index.shtml)[Рерайт текстов и уникализация 90 %](http://учебники.информ2000.рф/rerait-diplom.shtml)[Написание по заказу контрольных, дипломов, диссертаций. . .](http://учебники.информ2000.рф/napisat-diplom.shtml) |

Критически важная информационная инфраструктура подвержена все более значительным уязвимостям и потенциальным рискам. Существующая система глобального управления интернетом едва ли отражает желания и интересы большинства стран. Кибер-терроризм стал представлять опасность для всей глобальной общественности. Кибер-преступления распространились по всему миру. Вмешательство во внутренние дела государств посредством злоупотребления ИКТ и масштабной системой слежения происходит на регулярной основе. Отсутствие базовых международных правил в киберпространстве, которые бы эффективно управляли поведением всех сторон препятствует развитию кибер-среды.

Интерес Китая к киберпространству и возможностям его использования чрезвычайно велик. Си Цзиньпин неоднократно выступал с речью на форуме по кибербезопасности и информатизации, подчеркивая актуальность вопроса и представляя стратегические задачи КНР в информационном веке. Растущий интерес Китая к киберпространству и возможностям его использования подтверждается неоднократными обвинениями китайцев в кибер-шпионаже и злоупотреблении ИКТ в коммерческих целях. Китай всерьез занялся трансформацией системы кибербезопасности: от законодательных инициатив до стратегий международного сотрудничества в киберпространстве.

Чтобы понимать, действительно ли Китай может представлять угрозу в киберпространстве, необходимо разобраться в структуре обеспечения кибербезопасности в Китае, законодательной базе управления киберпространством в КНР. Кроме того, необходимо проанализировать восприятие Пекином киберпространства и рычагов его регулирования в международных отношениях. Хронологические рамки исследования — последнее десятилетие этого века. В 2016 году Китай принял первый закон, касающийся информационного пространства, выпустил стратегию сотрудничества в киберпространстве, а также начал осуществление реформ военной сферы, что непосредственно затронуло систему обеспечения кибербезопасности.

На настоящий момент в Китае насчитывается 731 млн интернет пользователей (практически население ЕС), 695 млн пользователей мобильными телефонами. Китай усовершенствовал скорость широкополосного интернета до 49 Мб/с и собирается отменить платежи за внутренний роуминг и звонки на дальние расстояния в 2017 году.

Согласно статистике Информационного центра интернет-инфраструктуры Китая, более 40% китайских предприятий в настоящее время предлагают покупки онлайн. Китай также пытается бороться с бедностью посредством развития и продвижения электронной коммерции.

Масштабы интернет аудитории во многом обостряют проблему кибербезопасности. Си Цзиньпин акцентировал на этом внимание на симпозиуме по информационной безопасности в 2016 году. Кроме того, были проведены кампании по интернет-чистке, проверки сайтов, поисковиков, мобильных приложений. Сайты с трансляциями были закрыты после нахождения нелегального контента.

марта 2017 года была впервые была выпущена стратегия международного сотрудничества в киберпространстве — начало построения сообщества с общей судьбой в киберпространстве, отражающая намерения по улучшению международной кооперации в данной сфере.

Объектом данного исследования является КНР. Предмет исследования — китайская система обеспечения кибербезопасности и контроля над интернетом. **Цель**: доказать и охарактеризовать специфичность и самобытность китайской системы кибербезопасности и сформировать позицию Китая в международном киберпространстве.

**Для этого необходимо** определить элементы структуры китайской системы обеспечения кибербезопасности, проанализировать изменения системы в связи с военной реформой в КНР, охарактеризовать законодательную базу контроля над интернетом в Китае, выделить ключевые тенденции нововведений, также необходимо рассмотреть основные положения закона о кибербезопасности, изучить подходы к киберпространству в китайской дискуссии, оценить взаимоотношения Китая с ключевыми игроками на международной арене, а также прояснить специфику позиции КНР по глобальному регулированию интернета.

**Гипотеза данного исследования состоит в том, что** благодаря недавним реформам и принятым документам Китай пытается создать мощнейшую систему обеспечения кибербезопасности — которая широко опирается на международный опыт, но в то же время обладает самобытностью и соответствует китайским условиям и особенностям политической системы, специфике КПК: распространению полномочий между военными и гражданскими органами.

В данной работе использовались официальные документы:

·        Закон о кибер-безопасности КНР (中华人民共和国网络安全法)

·        Положение об обеспечении безопасности компьютерных информационных систем, административные меры для информационных служб Интернета (计算机信息网络国际联网安全保护管理办法)

·        Стратегия международного сотрудничества в киберпространстве (网络空间国际合作战略)

·        Слушание комиссии конгресса по обзору отношений США и Китая в сфере экономики и безопасности от 9 июня 2016 года.

Выступления и заявления политических деятелей:

·        27 февраля 2014 года Си Цзиньпин председательствовал на первом заседании руководящей группы по кибербезопасности и информационным технологиям, подчеркнул, что безопасность и информатизация в Интернете являются важным стратегическим вопросом, касающимся безопасности и развития страны, а также жизни и работы людей. «Необходимо прилагать усилия к тому, чтобы превратить нашу страну в кибер-державу», — сказал он.

·        19 апреля 2016 года Си Цзиньпин произнес речь на симпозиуме по кибербезопасности и информатизации и определил цели развития Китая и важные задачи.

·        9 октября 2016 года Си Цзиньпин сделал замечания на учебной сессии, в которой участвовали члены Политбюро ЦК КПК. Он призвал к более независимым инновациям в Интернете и информационным технологиям, а также к усилению безопасности в киберпространстве.

·        Доклад о кибербезопасности в Китае за 2016 год《2016年中国互联网安全报告》.

Материалы СМИ:

·        Китай ужесточает контроль над интернетом.

·        Какие риски связаны с кибербезопасностью и страховыми продуктамив Китае?

·        В докладе CERT (Computer Emergency Response Team) подчеркивается рост кибер-угроз, связанных с приборами Интернета вещей и сетевыми промышленными системами.

Cоциально-экономическая статистика:

·        Информационный центр интернет-инфраструктуры Китая (中国互联网络信息中心第39次《中国互联网络发展状况统计报告》) в 39-ом докладе показывает, что на декабрь 2016 года количество интернет пользователей в Китае достигло 731 млн — по количеству юзеров Китай доминирует в мире. Степень проникновения интернета составляет 53,2%, что больше среднего глобального уровня на 3,1%. Интернет способствовал удобству человеческой жизни и производству, но также принес и ряд проблем безопасности.

·        Статистический отчет Китая о развитии Интернета, выпущенный 1 января 2017 года.

·        Национальный центр по чрезвычайным ситуациям в интернете в 2015 году насчитал 126 916 инцидентов с кибербезопасностью, что составило рост в 125,9% по сравнению с 2014 годом.

·        Отчет по безопасности в Интернете в Китае в 2016 году показывает, что 46,3% сайтов в Китае имеют бреши, из которых 7,1% представляют высокий риск уязвимости.

·        Согласно онлайн исследованию, проведенному в марте 2017 года Институтом инженеров по электротехнике и радиоэлектронике (电气与电子工程师协会) 45% управляющих в высокотехнологичных компаниях признали, что кибербезопасность была одним из главных вызовов в их работе в 2017 году.

Теоретической базой данного исследования послужил ряд таких теорий международных отношений как реализм — через призму которого Китай воспринимается на международной арене как наращивающая силу кибер-держава. Часть исследователей, занимающаяся китайской кибербезопасностью придерживается неолиберализма: международный порядок по сути своей анархичен, но ряд международных институтов может ее ослабить. Наибольший интерес представляет формирующаяся теория кибер-силы, представленная американским исследователям С. Старром.

Помимо общенаучных методов анализа и синтеза, классификации информации, а также систематизации, в данной работе использовались следующие научные методы: хронологический (рассмотрение событий в их последовательности и временной протяженности); метод когнитивного картирования (исследование восприятия международной обстановки лицами, принимающими решения).

В отечественной литературе основными авторами, занимающими проблемами кибербезопасности в Китае являются В. Б. Кашин, Г. Ибрагимова, М.Б. Касенова, Г. Юрченко, Е. Евдокимов, Е. Черненко и А.Т. Габуев.

В зарубежной науке основные работы представлены американскими авторами Mark A. Stokes, Jon R. Lindsay, John Costello, Peter Mattis, A. Segal, Ball D., John Markoff, Dennis J. Blasko, Peter Wood. Из китайских аналитиков стоит выделить.

Не изучена в достаточной степени структура, так как военная реформа приводится в действие в настоящее время. Отсутствие достоверных источников, так как Китай предпочитает не распространяться о своей системе обеспечения кибербезопасности.

**Новизна исследования** заключается в систематизации отечественных и зарубежных источников для исследования полной наглядной картины и структуры китайской системы кибербезопасности, анализ регуляторной базы киберпространства, а также оценка позиции Китая по киберпространству на международной арене позволит иметь более четкое представление о возможностях и угрозах со стороны КНР.

Поставленные задачи исследования обуславливают его структуру.В первой главе будетрассмотрен вопрос о структуре системы обеспечения кибербезопасности в КНР, охарактеризованы основные изменения в управлении в связи с военной реформой. Во второй главе будет проанализированы регуляторные рамки кибердеятельности и киберпространства в законодательстве КНР. Третья глава будет посвящена позиции Китая по кибербезопасности и контролю над интернетом на международной арене.

**1.       Структура системы обеспечения китайской кибербезопасности**

Специфика китайской системы кибербезопасности заключается в интеграции военных и гражданских органов управления, а также в основополагающей роли КПК. С одной стороны, данная особенность свидетельствует о значимости кибербезопасности для Китая, но с другой стороны это порождает неэффективность ее обеспечения.

**1.1 Подразделения КПК, отвечающие за кибербезопасность**

КПК — это ядро политической системы Китая. Впервые партийные лидеры серьезно осознали значимость информационной безопасности в 2001 году, когда была создана руководящая группа по государственной информатизации (State Informatization Leading Group (SILG)), возглавляемая премьером КПК. Данная группа отвечала за развитие национальной инфраструктуры ИТ, информатизацию. Ее подразделение — координационная группа по обеспечению государственной сетевой и информационной безопасности (State Network and Information Security Coordination Group (SNISCG)) несло ответственность за управление политикой безопасности. Руководящая группа по государственной информатизации и Канцелярия Государственного совета по информатизации (State Council Informatization Office) — напрямую ответственная за осуществление политики в киберпространстве, существовала до 2014 года.

С 2014 года в КНР действует руководящая группа по кибербезопасности и информатизации, возглавляемая генеральным секретарем партии Си Цзиньпином. Стоит отметить, что в данную группу также входят премьер-министр Ли Кэцян и член Постоянного комитета Политбюро Лю Юньшань, с 19 (!) другими должностными лицами из Политбюро или на уровне министерств. Примечательно, что десять из одиннадцати членов Политбюро также входят в новую руководящую группу Си Цзиньпина по всестороннему углублению реформ. Это указывает на то, что новый президент Китая рассматривает кибербезопасность как важный аспект укрепления авторитета КПК в свете внутренних коррупционных скандалов и напряженных отношений с Соединенными Штатами.

Состав руководящей группа по кибербезопасности и информатизации

**Председатель**: Си Цзиньпин (председатель Центрального военного совета, генеральный секретарь КПК, президент КНР)

**Заместитель председателя:** Ли Кэцян (премьер)

**Заместитель председателя:** Лю Юньшань (Постоянный комитет, председатель Центральной партийной школы)

**Политбюро и старшие руководители:**

Ма Кай (вице-премьер)

Ван Хунин (директор Центра стратегических исследований, директор)

Лю Цибао (Центральный пропагандистский комитет, директор)

Фань Чанлун (Центральная военная комиссия, заместитель директора)

Мэн Цзяньчжу (Центральный политико-правовой комитет, секретарь)

Ли Чжаньшу (генеральный директор ЦК, директор)

Чжоу Сяочуань (губернатор Народного банка Китая)

**Министерства, занимающиеся внедрением политики кибербезопасности:**

**Директор офиса руководящей группы по кибербезопасности и информатизации:** Лу Вэй (вице-директор SCIO и директор SIIO / CAC)

Го Шенкунь (министр общественной безопасности)

Фан Фэнхуй (начальник Генерального штаба НОАК)

Ван И (министр иностранных дел)

Сю Шаоши (Национальная комиссия развития и реформ, директор)

Юань Гуйжэнь (министр образования)

Ван Чжиган (министерство науки и техники, секретарь)

Лоу Цзивэй (министр финансов)

Мяо Вэй (министр промышленности и информационных технологий)

Цай У (министр культуры)

Цай Фучао (Государственное управление печати, публикаций, радио, кино и телевидения, директор)

**Таблица 1.** Структура системы обеспечения кибербезопасности в КНР



Данная схема отражает официальные органы и институты, которые играют роль в управлении политикой кибербезопасности в КНР. Центральное положение занимают подразделения КПК, включая руководящую группу по кибербезопасности и информатизации. Также важную роль играет Государственное управление по защите государственной тайны КНР, которое управляет всей секретной информацией. Данное управление стало играть активную роль в выработке политики по кибербезопасности с момента пересмотра Закона о государственной секретности в 2009 году. Служба связи и шифрования Главного управления ЦК КПК несет ответственность за шифрование для правительства, военных и отдельных отраслей. Китайские усилия по обеспечению соблюдения специфических стандартов шифрования стали постоянным источником трений с иностранными фирмами в Китае.

**Таблица 2.** Интеграция гражданских и военных служб в управлении кибербезопасностью



В общей системе обеспечения кибербезопасности НОАК является одним из важнейших игроков — несет ответственность за военную электронную разведку и электронное вооружение, но некоторые органы НОАК также осуществляют экономический шпионаж. До реформы главными управлениями являлись операционные бюро и НИИ Третьего управления Генерального штаба (китайская версия АНБ). Четвертое управление Генштаба отвечало за электронное вооружение, кроме того отдельные полномочиями обладали технические разведывательные бюро военных округов и служб НОАК. До конца была не ясна степень сотрудничества между различными управлениями и подконтрольными им бюро.

Несмотря на то, что после реформы Третье и Четвертое управления Генштаба станут подконтрольными Войскам части стратегической поддержки, стоит рассмотреть подробнее структуру управлений НОАК.

**1.2     Военные структуры, ответственные за кибер-операции**

«Следует сразу отметить ключевое отличие китайской системы управления специальными службами и вооруженными силами от советской и российской, а именно, отсутствие всякого контроля органов госбезопасности и полицейских структур над военными. Насколько известно, ни МОБ, ни МГБ не имеют полномочий по ведению оперативной работы в войсках; их сотрудники не могут заходить на территорию военных объектов без разрешения представителей военных властей. Вопросы борьбы с преступностью в войсках, расследований преступлений и наказания провинившихся военнослужащих целиком относятся к компетенции Главного политического управления НОАК, которое, помимо службы безопасности, контролирует военные суды, военную прокуратуру и военную комиссию по проверке дисциплины (антикоррупционный орган). Даже финансовая отчетность в армии проверяется военными — аудиторским отделом Главного управления тыла НОАК».

**.2.1 Третье управление НОАК**

Третье управление обладает огромной коммуникационной инфраструктурой и системой кибер-слежения, нацеленной на иностранное дипломатическое взаимодействие, военную деятельность, экономические предприятия, государственные образовательные институты и отдельных персон. Комплекс штаб-квартир Третьего управления располагается вместе с операционным управлением Генштаба НОАК, включая также его 24-часовой центр наблюдения на горе Сишань в Академии военных наук. Согласно неподтвержденному исследованию (Easton I., Stokes M.) Третье управление насчитывает 130 тысяч служащих, работающих на основных позициях в штаб-квартирах, 12 операционных бюро, 3 исследовательских института. Офисы и площадки, расположенные по всему Китаю, отчитываются напрямую Пекину, они не находятся в административной юрисдикции командоров и комиссаров военных округов.

Центральное командование Третьего управления контролирует штаб-квартиры, политические и логистические департаменты, а также бюро научно-технической информации [科技情报局] и бюро научно-технического оборудования. Бюро научно-технического оборудования держит под контролем три исследовательских института, отвечающих за компьютеры, сенсорные технологии и криптографию.

-ой исследовательский институт. НОАК принадлежат одни из самых мощных (супербыстрых) компьютеров в мире. 56-ой исследовательский институт также известен как Исследовательский институт компьютерных технологий в Цзяннани [江南电脑科技研究所], — самая старая и масштабная научно-исследовательская организация НОАК. Расположенный в Уси в провинции Цзянсу институт инвестирует много в высокопроизводительные компьютеры и поддерживает центры Третьего управления и другие компьютерные центры национального уровня. Суперкомпьютеры позволяют создавать и взламывать сложные коды и пароли, которые являются миссией исследовательского института Третьего управления в Сычуани. Директор 56-го исследовательского института Хуан Йонцинь [黄永勤] является членом экспертной рабочей группы по компьютерам и программному обеспечению в программе 863 (государственная программа или план развития высоких технологий).

-ой исследовательский институт. Согласно исследованию Mark A. Stokes, Jenny Lin и L.C. Russell Hsiao, 57-ой исследовательский институт отвечает за развитие систем перехвата коммуникаций и обработки сигналов. Ранее взаимодействовал с комплексом Первого управления в районе Дуцзянянь, институт располагается в Чэнду и также известен как Юго-западный институт электронных и телекоммуникационных технологий [西南电子电信技术研究所]. Среди ключевых сфер интересов — спутниковые коммуникационные технологии, был замечен за работой над спутниковыми исследованиями с Китайской академией космических технологий.

-ой исследовательский институт. 58-ой исследовательский институт фокусируется на криптологии и технологиях информационной безопасности. Расположенный в Мяньян (провинция Сычуань), и также известный как Юго-западный исследовательский институт автоматики [西南自动化研究所]. 58-ой исследовательский институт кооперируется в работе с Нанкинским университетом науки и технологии [南京理工大学].

Третье управление несет ответственность за защиту компьютерных сетей НОАК и играет основную роль внутри сообщества информационной безопасности на национальном уровне Китая. Согласно одному американскому исследованию китайские аналитики полагают, что США уже осуществляют огромную эксплуатацию компьютерных сетей на китайских серверах. Поэтому с китайской точки зрения защита компьютерных сетей должна быть наивысшим приоритетом в мирное время. Организации, относящиеся к защите компьютерных сетей, контролируемые или аффилированные с Третьим управлением включают:

·        Информационная канцелярия НОАК [通信机要局], Китайский северный вычислительный центр [北方计算中心], вычислительный центр Третьего управления Генштаба [总参三部计算中心] в Пекине.

·        Основанный в 2005 году Национальный исследовательский центр технологий информационной безопасности обладает полномочиями оценки рисков Китайской сетевой безопасности.

·        Центр оценки информационной безопасности и сертификации НОАК [解放军信息安全测评认 证中心].

·        Исследовательский институт информационной безопасности [信息安全研究所] и национальный информационный центр [国家信息中心], который имеет тесные связи с Бюро научно-технического оборудования Третьего управления.

·        Национальный Центр инженерных технологий информационной безопасности [国家信息安全工程技术 研究中心] в Шанхае, руководимый наравне с Министерством науки и технологии Государственного совета, национальным центром криптологического управления, государственное секретное бюро и министерство государственной безопасности.

Подготовка и образование для персонала Третьего управления НОАК обычно осуществляется в одном из двух институтов. Большинство лингвистов, работающих в бюро Третьего управления, проходят языковое обучение и получают языковую практику в Университете иностранных языков НОАК [解放军洛阳外语学院] в Лояне. После выпуска студенты приписаны к бюро для технической тренировки для особых целей. Техническая практика для электронных инженеров, специалистов по коммуникациям, ученых компьютерных наук, персонала сетевой безопасности проводится в университете информационной инженерии НОАК [解放军信息工程 大 学 ] в Чжэнчжоу, провинции Хэнань. Персонал, отвечающий за регулярные полномочия обязанности, такие как водители, администрация, безопасность объектов и оборудования, набираются согласно обычному ежегодному приему. Обязанности персонала по обеспечению безопасности более строгие, чем в других частях НОАК, что обеспечивает политической системе комиссаров повышенное положение.

**Операционные бюро Третьего управления Генштаба НОАК**

Третье управления Генштаба НОАК обладает прямой ответственностью над 12 операционными бюро. 8 из 12 штаб-квартир бюро располагаются в Пекине, две другие — в Шанхае, одна в Циндао, другая в Ухани. 12 операционных бюро Третьего департамента с наибольшей вероятностью отчитываются в департамент штаб-квартир. Операционные бюро отделены друг от друга и отличаются от технических разведывательных бюро (ТРБ), подконтрольных семи военным округам НОАК и трем службам: воздушным силам, морской и второй артиллерии. Начальники ТРБ скорее всего отчитываются перед военными округами и и перед главой штаба службы. Однако, вполне вероятно, что Третье управление снабжает ТРБ заданиями по сбору и анализу.

Уровень контроля, которым располагают операционные бюро и ТРБ Третьего управления по отношению к милицейским кадрам и резерву в военных округах, неизвестен. Милиция составляет третий компонент вооруженных сил Китая, два других — НОАК и Народная вооруженная полиция. Оценка Сычуаньского военного округа (2004) призывает милицию и резервы играть более важную роль в сети обороны и атаки, технической инспекции (разведки) и психологических операций. Хубэйский военный округ, к примеру, имеет партнерские отношения с центром сетевых атак и обороны Уханьского университета [武汉大学网络攻防中心].

Директоры на уровне бюро и политические комиссары обладают рангами эквивалентными командирам военных дивизий, и присматривает примерно за 6-14 дочерними площадками или офисами （处）. Директоры офисов имеют ранг эквивалентный Заместителю командира дивизии или командира полка. Отделения, подконтрольные бюро — далее подразделяются на секции (科), хотя некоторые секции отчитываются прямо в штаб-квартиры бюро. В дополнение к отделению связи в Шанхае, Третье управление Генштаба НОАК возглавляет отделение связи Гонконга и Макао в Шэньчжень [总参三部港澳联络局].

Третье управление Генштаба НОАК с наибольшей вероятностью имеет особую миссию, такую как перехват радио или спутниковых сообщений, криптологическое шифрование, перевод, решение проблем целостности и безопасности информации, анализ разведданных. Вдобавок к мониторингу трафика внутренних коммуникаций НОАК на предмет нарушения безопасности, подразделения Третьего управления и перехватывательные станции расположены по периметру Китая и могут осуществлять мониторинг радио трафика и искать местонахождение источников посредством радио пеленгационных процедур (homing). Особые бюро Третьего управления, ответственные за эксплуатацию компьютерных сетей остаются до сих пор неясными. 7 бюро Третьего управления было ассоциировано с техническими аспектами кибер-операций. Региональные бюро, такие как 2 бюро в Шанхае или 4 бюро в Циндао могут быть ответственны за перевод информации собранной с перехваченных сообщений и кибер-надзора, а также за подготовку разведывательных отчетов на основе переведенных материалов. 12 бюро отвечает за техническую разведку, связанную с космическими программами.

**Первое бюро** (подразделение 61786). Штаб-квартира первого бюро находится с командным комплексом Третьего управления на северо-западе Пекина. Отвечая за 12 офисов, работающих в различных частях Китая, бюро скорее всего выполняет функциональную миссию, не региональную. Ранее располагавшееся в окрестностях Чэнду в Дуцзяняне, миссия бюро включает в себя шифрование, расшифровку и другие задачи информационной безопасности. Первое бюро является единственным военным представителем во время экспертной рабочей группы по программе информационного обеспечения. По крайней мере один элемент Первого бюро, вероятно 7ой офис, расположен на юге Дуцзяняня. Хотя не в формальных подчиненных отношениях Первое бюро установило тесные отношения с организациями в Чэнду, такие как Лаборатория информационной безопасности и сетевых атак и обороны Сычуаньского университета [四川大学信息安全及网络攻防研究室]. Чэнду также является базой для 57-го исследовательского института.

**[Смотрите также:   Дипломная работа по теме "Правовое регулирование самовольной постройки"](https://sprosi.xyz/works/diplomnaya-rabota-po-teme-pravovoe-regulirovanie-samovolnoj-postrojki/%22%20%5Ct%20%22_blank)**

**Второе бюро** (подразделение 61398). Второе бюро функционирует как показательная единица Третьего управления, отвечающая за США и Канаду, с наибольшей вероятностью фокусируется на политической, экономической и военной разведке.

**Третье бюро** (подразделение 61785). Штаб-квартира в окрестностях Дасиня на юге Пекина. Третье бюро имеет функциональную миссию. Благодаря разбросанности подчиненных офисов миссия Третьего бюро может заключаться в передовом сборе линии приема радио коммуникаций, включая контроль сетей на границах, также нахождение направления и контроль выбросов и безопасности. Бюро имеет по крайней мере 13 подразделений в подчинении. Офисы Третьего бюро находятся в Харбине, Даляне, Пекине, Ханчжоу, области Нинду (Цзянси), Сямэнь, Шэньчжень, Куньмин, Сянь и Урумчи. Офис в Шэньчжене обладает уникальной миссией, возможно отвечает за покрытие беспроводной сетью Гонконга и Макао.

**Четвертое бюро**. С штаб-квартирой в Циндао, 4 бюро фокусируется на Японии и Корее. Многие офисы 4 бюро, включая первый, располагаются в районе Циндао. Второй офис инкорпорирует лингвистов корейского языка. 7 офис Четвертого бюро расположен в Ханчжоу. Другие офисы, находящиеся в подчинении, также находятся в районе Циндао, Даляня, Пекина и Шанхая. Бюро прежде располагалось в провинциальном городе Синьчжоу в Шаньси, в особенности в деревне Хуанлун Вангоу. Пока штаб-квартира перемещалась в Циндао, Четвертое бюро может все еще иметь базу подготовки обучения в Синьчжоу.

**Пятое бюро** (подразделение 61565). Со штаб-квартирой в деревне Хуанцунь района Дасинь в Пекине, пятое бюро нацелено на Россию. Значительное число параболических круглых антенн, направленных в сторону разных азимутов могут быть видны на восточном. Офисы пятого бюро располагаются в Суйхуа, Цзюцюане и Синьцзяне провинции Хэйлунцзян.

**Шестое бюро** (подразделение 61726). Штаб-квартира Шестого бюро находится в районе Цчан в Ухани. Чжан Юньцзю [张运炬] служит политическим комиссаром Шестого бюро. Штаб-квартиры бюро были в центре районов Цзинмэнь, Хубэй, до того как перемещены в Ухань более 12 лет назад. Офисы Шестого бюро растянулись вдоль центрального Китая от восточного побережья города Сямэнь и до города Кньмин в Юньнани, указывая на миссию в отношении Тайваня и Южной Азии. Более специфично, офисы располагаются в Сямэни, Наньчане (Седьмой офис), Сянфане; деревня Сяобу области Нинду, Ухань, Цзинмэнь и район Паньлун в Куньмине (Четвертый офис). Нанчанских офис вполне возможно занимается подготовкой и обучением.

**Седьмое бюро** (подразделение 61580). Штаб-квартира в районе Шуцунь области Хайдянь на северо-западе Пекина, конкретная миссия Седьмого бюро пока не ясна. Избранные инженеры данного бюро специализируется на компьютерных сетях обороны и атаки, провели совместные учения с подразделением сети компьютерных атак и защиты академии информационного инжиниринга НОАК. Разделенное по крайней мере на 10 офисов, Седьмое бюро нанимает переводчиков английского языка.

**Восьмое бюро** (подразделение 61046). Расположившееся в Ханьцзячуани, Восьмое бюро привязано к штаб-квартире Третьего управления в северо-западных окрестностях Пекина. Основываясь на языковых возможностях сотрудников, Восьмое бюро фокусируется на Западной и Восточной Европе, а также возможно и всем остальном мире (включая Ближний Восток, Африку, Латинскую Америку). Среди его 10 офисов по крайней мере один главный офис находится в городе Хайкоу на острове Хайнань.

**Девятое бюро**. Девятое бюро обеспечивает основной стратегический разведывательный анализ и место базы управления данными Третьего департамента. Среди всех бюро, Девятое бюро самое скрытое. С весны 2010 года Чжан Циньчэнь служил директором Девятого бюро. Седьмой офис оказывается вовлечен в аудио-визуальные технологии, и управление базой данных огромного масштаба. Бывший директор Девятого бюро Куан Тао был выдающимся комментатором международных отношений со времен его ухода на пенсию в 2004 году.

**Десятое бюро** (подразделение 61886). Десятое бюро, иногда называемое подразделение 7911 имеет штаб-квартиру в окрестностях Шанди на северо-западе Пекина, возможно специально фокусируется на телеметрии и отслеживании боеголовок и ядерных испытаний. Первый офис Десятого бюро связан с штаб-квартирой. Второй офис находится в Инине в Синьцзяне рядом с границей с Казахстаном. Третий офис находится в деревне Бажэнь в Кашгаре. Другой офис расположен в Урумчи.

**Одиннадцатое бюро** (подразделение 61672). Одиннадцатое бюро с штаб-квартирой в сообществе Маляньва, на востоек от штаб-квартиры Третьего управления. Штаб-квартира бюро была прежде расположена в городе Цзямуси в провинции Хэйлунцзян до переезда в Пекин в 2011 году. Разброс офисов по северной части Китая и наем лингвистов русского языка указывают на то, что миссия имеет отношение к России. Интересно, что русские лингвисты приписаны и к Пятому и к Одиннадцатому бюро, однако разница между ними и их миссиями не ясна.

**Двенадцатое бюро** (подразделение 61486). Со штаб-квартирой в районе Чжабэй в Шанхае Двенадцатое бюро обладает функциональной миссией, включающей спутники, занимается инклюзивным перехватом спутниковых коммуникаций и возможно основано на сборе электронных разведданных из космоса.

Как можно было понять, у НОАК разветвленная сеть институтов, которые проводят исследования в области информационной безопасности. Эти и другие институты могут оказывать поддержку «кибер милиции», которая по мнению Robert Sheldon и Joe McReynolds играет периферийную и сфокусированную на защите роль в позиции НОАК относительно кибербезопасности. НОАК также обладает регуляторными функциями в таких гражданских секторах как транспортное сообщение, что позволяет НОАК запрашивать сертификации для гражданских технологий, приобретенных для этих отраслей.

**1.2.2 Четвертое управление НОАК**

Четвертое управление Генерального штаба НОАК (4 НОАК), также известное как департамент радиоэлектронных контрмер. Главная обязанность — электронные атаки (или глушение), электронная защита и меры электронной поддержки. 4 НОАК — единственная организация, несущая ответственность за электронную разведку в НОАК и покрывающая миссии и технической разведки, и операционной разведки. Его миссия эволюционировала и расширилась в последние несколько лет и стала включать атаки на компьютерные сети и более стратегические миссии электронного отказа систем, как например спутниковое глушение. Согласно некоторым аналитикам 4 НОАК способно нарушить коммуникации противника, срывать навигацию и подрывать установленный на спутнике радар с синтетической апертурой.

Кибер-миссии 4 НОАК в первую очередь и в основном фокусируются на подрыве и отказе компьютерных сетей врага. Чтобы от необходимого таргетирования осуществить успешно эти миссии необходимо 4 НОАК иметь такой сильный компонент как система слежения. Эта операционная постановка целей и в кибер пространстве и в электронной сфере формирует основу для роли 4 управления НОАК в качестве ключевой разведывательной службы.

Эта всеобъемлющая структура в генеральном штабе также отражена в военно-морском флоте НОАК, военно-воздушные силы НОАК, 2-й артиллерийский корпус и семи подчиненных военных регионах НОАК. Операционные подразделения 4 НОАК отражены в структурах-коллегах, существующих на национальном уровне для служб и воплощенных в групповых армиях для военных регионов. Степень, до которой эти параллельные структуры координируют с их коллегами из Генерального штаба — неясна и остается одним из главных вопросов как НОАК управляет, координирует и объединяет свои разведданные на региональном уровне.

**.2.3 Военные реформы НОАК**

В ноябре 2015 года Китай объявил о серии предстоящих реформ, которые перевернут военные службы и окончательно приведут к перестройке его институтов. Планировалась трансформация их устаревшей структуры еще советской эпохи в более современную, обновленные силы способные сражаться и выигрывать войны. Однако в самых огромных и радикальных реформах с времен 1950-х годов остается очень много не отвеченных вопросов. Статус главных разведывательных органов НОАК — 2 НОАК, 3 НОАК, 4 НОАК — это центр понимания, что будет следующим для китайской военной разведки.

**Управление объединенного штаба и Бюро разведки**

На самом верхнем уровне НОАК была реорганизована. Во время реформ Управление генерального штаба было реорганизовано в Управление объединенного штаба, с НОАК получающей новые независимые штаб-квартиры отдельно от Управления объединенного штаба. Управление объединенного штаба сформировало новое Бюро Разведки, вероятно в качестве преемника миссии 2 НОАК. Все еще неизвестно, однако, до какой степени сотрудники, миссия и организация были перемещены из предыдущего 2 НОАК или были созданы полностью заново.

Открытые вопросы в сторону, обе эти меры сокращают роль/главенство НОАК в бюрократическом аппарате разведки, и по крайней мере убирают многие институциональные барьеры, которые позволяли НОАК доминировать и в разведывательных властях, и в операционных властях. Это изменение по крайней мере обладает потенциалом для новых ресурсов стать доступными для использования другими службами, военно-морским флот, военно-воздушными силами и созданными ракетными силами НОАК.

Эти изменения должны также повлиять на операционный и тактический уровень. Реорганизация военных округов, первоначально возглавляемых армией, в объединенные военные театры или зоны сражений вызывает необходимость изменения в структуре и деятельности на уровне кампаний и техническом уровне в войнах. Театральное командование может полностью реорганизовать бюро технической разведки военного театра, разведывательные департаменты, бригады электронных контрмер в более объединенные силы, которые смогут лучшим образом поддерживать мандат театра действий «фокус на сражении».

**Войска стратегической поддержки**

Реформы ввели новую службу, называемую «войска стратегической поддержки», которая окажет серьезное влияние на сообщество военной разведки Китая и его возможности. Первоначальные отчеты предполагают, что силы в основном несут ответственность за миссии НОАК, связанный с контрмерами в космосе, киберпространстве и электронной сфере. На базовом уровне Войска стратегической поддержки могут оказаться эквивалентны Стратегическому командованию США. Как STRATCOM, силы намереваются совместить операции, касающиеся стратегической информации, такие как кибер-оружие и электронное оружие, со стратегическим C4SIR. Будет ли НОАК относиться к Войскам стратегической поддержки как к службе или больше как к функциональному и операционному набору подразделений остается непонятным. Их стратегические роли, миссия и административно-операционный контекст скорее всего останутся неясными в ближайшем будущем.

На фронте кибер-разведки, не очень понятно будут ли Войска стратегической поддержки централизованно управлять кибер-операциями Китая посредством сокращения институциональных барьеров, разделяющих атаки на компьютерные сети, шпионаж и оборону, которые традиционно существовали в раздробленном виде и управлялись отдельными организациями внутри НОАК. Практически совсем нет информации о статусах 3 НОАК или 4 НОАК — были ли они модифицированы, отменены или полностью отданы под руководство Войскам стратегической поддержки.

Картина немного яснее в отношении ведения разведки, наблюдения и рекогносцировки на основе данных из космоса, с первыми экспертами, предлагающими, что Войска стратегической поддержки будут почти в одиночки управлять китайской разведкой, наблюдением и рекогносцировкой в космосе, включая отслеживание и разведку, ежедневные операции спутниковой навигации, управление Beidouспутниками, управление космическими средствами разведки. Эти заявления валидированы недавними анонсами, которые Чжоу Чжисинь, бывший глава Аэрокосмического разведывательного бюро 2 НОАК, отвечающий за разведку, наблюдение и рекогносцировку в космосе, будет выставлять напоказ неопознанного бюро в Силах стратегической поддержки.

Что касается электронного оружия и мер электронной поддержки, 4 НОАК скорее всего сформирует главное ядро этой новой силы. Предполагаемые возможности стратегического электронного вооружения 4 НОАК против спутников и их доминирования в радарах и электронной разведке доказывает, что 4 НОАК будет являться неотъемлемой частью сил электронного вооружения Сил стратегической поддержки.

Несмотря на специфику как 3 НОАК и 4 НОАК будут интегрировать с этой новой силой, довольно очевидно, что концентрация миссий стратегической разведки, наблюдения и рекогносцировки внутри Сил стратегической поддержки позволит Центральному военному совету свободнее расставлять приоритеты, оценивать задачи и формировать силу для наилучшего выполнения военных целей.

Новый ведущий принцип реформ: «КПК будет вести, службы будут строить, а театры будут бороться», создает разделение труда, которое если действительно последует, то создаст окружающую среду, позволяющую службам создавать более испещренные методы сбора разведданных и позволит КПК более умело осуществлять (выкраивать/подстраивать) разведывательные операции для поддержания стратегических нужд военных сил Китая.

Централизация кибер-операций, также, окажет значительное влияние на НОАК, с большой вероятностью позволит осуществлять более эффективные и сложные кибер-миссии, состоящие из всех элементов операций по компьютерным сетям — разведка, эксплуатация, атака и оборона.

**Таблица 3.** После военной реформы Третье управление и Четвертое управления войдут в состав Войск стратегической поддержки



**.2.4 Китайское видение Третьей стратегии компенсации США**

Китай твердо придерживается проведения ряда военных реформ, включая реорганизацию, более реалистичные планы учебной подготовки, новейшие виды вооружения — все так или иначе связанные с информационными технологиями.

Однако с 2014 года политические деятели США, начиная с в последствии ставшим министром обороны США Чаком Хэйглом (Chuck Hagel) заявили о выводе военных преимуществ США на новый уровень, чтобы ответить на силовой паритет со стороны развивающихся обычного-военного вооружения, — третья стратегия компенсации. Китайские академики и военные практики тщательно наблюдают за Третьей стратегией компенсации и и рассматривают как реорганизовать планы китайской модернизации в соответствии с ТСК.

Третья стратегия компенсации (“第三个对消战略” or “第三次抵消战略”) регулярно появляется в китайских публикациях, включая статьи в People’s Daily, а также СМИ, концентрирующие свое внимание на обеспечении безопасности такие как People’s Liberation Army Daily. Статья, написанная профессорами Air Force Engineering College and Command Academy, Wang Peng (王鹏) Shao Dan (邵丹) появилась после речи министра Хейгела в 2014 году, отмечая тот факт, что стратегия представляла расширение уже существующих элементов текущей стратегии по отношению к Китаю. Ван и Шао также отметили, что такая стратегия потребует широкой помощи внутри правительства США из-за ее бюджетных требований, и учитывая с какой легкостью технологии распространяются, создать задел (отрыв) будет довольно непростой задачей.

Е Цзяньцзюнь (叶建军), профессор академии международных отношений НОАК, написал статью в Contemporary International Relations о концептуализации «Инновационная оборонная инициатива» (“Defense Innovation Initiative”) как часть мышления времен Холодной войны. Е в дальнейшем описал концепцию как дестабилизирующую и разрушительную для позитивного развития международных отношений.

Такое отношение не должно удивлять, так как Китай многими способами пытается завершить его собственный переход к технологиям «Второй стратегии компенсации», в том числе строя собственные мощности по информированию о местоположении, группировка глобальной системы позиционирования (Beidou) и самолеты-невидимки. Мощности Воздушных сил НОАК в большинстве своем представлен старыми самолетами такими как третье поколение J-8. Новый дизайн, к примеру невидимый бомбардировщик J-20, только недавно достиг «нижнего уровня первоначального производства», который рассматривается в качестве важной, хотя и ранней вехи. Более того, важно отметить, что китайская стратегия не полностью симметрична противодействию военным мощностям США.

Однако Китай уже проинвестировал в свои собственные высокотехнологичные разработки следующего поколения — от квантовых компьютеров до лазерных систем, с большей вероятностью не только ради увеличения скорости прогресса в достижении полных мощностей технологий Второй стратегии компенсации, но и для дальнейших инноваций. Китайское правительство смотрит на технологическую конкуренцию как на абсолютно невозможную без большей интеграции гражданских и военных технологий для достижения разумного задела.

Китайские гражданские и военные официальные лица главным образом инвестируют в искуственный интеллект (AI; 人工智能), в некоторых случаях сотрудничают с западными компаниями. В частности, в начале показаний Сноудена, Китай начал производство своего собственного программного обеспечения и харда, который рассматривается как сокращение главного потенциального источника уязвимостей.

В то время как этот первоначальный обзор показывает, что политические деятели, отвечающие за китайскую оборону — имеют представление и реагируют на Третью стратегию компенсации США, но все-таки требуется еще более тщательный анализ. Кроме того, будет интересно оценить как военная стратегия Китая эволюционировала и как она изменится.

**.3 Гражданские органы по управлению кибербезопасностью**

Большинство расползшегося аппарата по управлению гражданской кибербезопасностью находится в ведомстве Государственного Совета. Министерство индустриальных и информационных технологий содержит административные офисы группы SNISCG, но влияние на осуществление политики в области кибербезопасности утратило с 2008 года.

Подтверждением служит тот факт, что административный офис руководящей группы по кибербезопасноти и информатизации располагается не в министерстве промышленности и информационных технологий, а в Государственной канцелярии по делам интернет-информации**,**котораянесет ответственность за цензуру в интернете. Более того, министр Государственной канцелярии по делам интернет-информации (ГКДИ) — бывший генеральный директор новостного агентства Синьхуа. Заместители директора ГКДИ включают заместителей министра промышленности и информатизации КНР и министерства общественной безопасности. Данные изменения в свое время подчеркивали важность информационного контроля, а не только технической защиты сети в китайском понимании кибербезопасности. С момента реорганизации ГКДИ также негласно называют Администрацией кибербезопасности Китая. Министерство промышленности и информатизации КНР все еще играет важность, но сейчас в более операционном, а не направляющем смысле.

Китайский национальный центр компьютерной безопасности (National Computer Network Emergency Response Technical Team/Coordination Center) несет ответственность за аварийное реагирование на чрезвычайные ситуации заражения общественных компьютеров и ежегодно публикует отчет статистики кибератак против Китая. Источник статистики часто цитируется официальными лицами для подчеркивания уязвимости Китая. Китайский национальный центр компьютерной безопасности отвечает за управление доменами в интернете. Министерство промышленности и информационных технологий также регулирует деятельность шести провайдеров интернет услуг (ISP), которые в свою очередь мониторят и фильтруют контент в их сетях согласно руководству по цензуре, установленному Информационной канцелярией ГС и ГКДИ.

Отличительная характеристика китайской концепции кибербезопасности (信息安全) — придание огромного значения интернет контенту даже в большей степени, чем технической безопасности сети (网络安全). То, что руководящая группа по кибербезопасности и информатизации находится в ГКДИ (администрация кибербезопасности) подчеркивает важность двойственности значения. Особенно в сравнении с западным ограниченным пониманием кибербезопасности, подчеркивающим лишь техническую угрозу функционированию компьютеров. Бывший председатель руководящей группы по государственной информатизации описал информационную безопасность как «абсолютную необходимость для гаранта стабильного и безопасного применения ИТ», как «критически важный элемент системы национальной безопасности», а также как «необходимую для социальной стабильности и культурного и идеологического социалистического развития». Данный акцент превратился в более сконцентрированные национальные усилия по выстраиванию цензуры и инфраструктуры слежения (известной как Великий китайский файрвол), а не координации технических стандартов и механизмов обеспечения их соблюдения. В результате Китай имеет тенденцию прикладывать больше усилий на защиту против «терроризма, сепаратизма, экстремизма», а не на защиту от экономических преступлений и технической эксплуатации со стороны иностранных разведывательных служб.

Министерство общественной безопасности (МОБ) несет ответственность за расследование компьютерных преступлений через 11-e бюро и обеспечение соблюдения режима многоуровневой общественной безопасности, инициированным Документом 27. Третий НИИ МОБ проводит исследования в области информационной безопасности посредством таких баз, как например Национальный исследовательский центр по борьбе с компьютерными проникновениями и предотвращением вирусов. Министерство государственной безопасности (МГБ) — служба китайской разведки за иностранными подразделениями. МГБ обладает значительной технической кибер-экспертизой, которую он использует через Центр критериев оценки безопасности информационных технологий (China National Information Technology Security Evaluation Center), чтобы проводить тестирования на предмет уязвимости и оценивать надежность программного обеспечения.

Дополнительный регуляторный надзор возложен на министерство торговли, которое контролирует экспорт и импорт технологий. Главная таможенная администрация, которая управляет центром сертификации информационной безопасности; Комиссия по надзору и управлению государственными активами, которая контролирует государственные предприятия; Государственный комитет КНР по делам развития и реформам и другие. Даже главная администрация спорта может нуждаться в консультациях по чрезвычайным кибер-ситуациям, так как она отвечает за индустрии видеоигр. Как и во многих других сферах осуществления политики в Китае, управляющие власти раздроблены на множество бюрократических агентств, каждый со своими собственными требованиями. Многие акторы пытаются играть все большую роль в проведении политики и отдельных миссий, что надежда на последовательные политические решения мала. Такая неэффективность распространяется и на технологичные фирмы и пользователей.

Частные фирмы в Китае должны бороться с многочисленными стандартами соответствия и требованиями сертификации, которые выборочно применяются. Это создает для Китая возможность использовать политику безопасности для оправдания технических торговых барьеров или преследования/нарушения прав иностранных фирм. Постоянный вопрос для иностранных фирм в Китае, а также для торговых министерств или отраслевых групп, занимающихся Китаем, заключается в том, являются ли якобы меры безопасности в любом конкретном случае прикрытием протекционистских мотивов. Американское информационно-технологическое бюро/канцелярия (USITO), промышленный защитник американских компьютерных и телекоммуникационных фирм в Китае, сделало вывод о том, что китайская политика «систематически поддерживает продукты и услуги китайских производителей по сравнению с компаниями с иностранными инвестициями во многих отраслях и сферах, от разработки национальных стандартов и оценки соответствия, до политики конкуренции и местного фаворитизма в государственных закупках». Не удивительно, что Китай часто предъявляет одно и то же обвинение против других стран, особенно после обвинений США и Австралии в связях между китайской разведкой и Huawei, которые обе страны использовали для оправдания исключения китайского телекоммуникационного гиганта из правительственных заявок.

После нескольких лет относительной запущенности, бюрократического тупика и растущего числа международных споров о киберугрозах, китайские лидеры недавно начали уделять внимание кибербезопасности. В июле 2012 года Госсовет опубликовал обновленную версию Документа 27. Вновь подтверждая знакомые темы, такие как необходимость улучшения шифрования, экспертизы и регулирования, также была подчеркнута необходимость защиты критически важных систем управления инфраструктурой и защиты конфиденциальности пользователей Интернета. Вероятно, не случайно, в 2014 году международные СМИ сообщали об использовании США и Израилем Stuxnet против Ирана, а также некоторых крупных инцидентах компрометации китайских сайтов (упомянутых в главе Чжуге Цзянвэй, Гу Лиона, Дуань Хайсиня и Тейлора Робертса). Новое мнение было откровенным в отношении проблем, стоящих перед Китаем: «отставание от развитых стран в области развития широкополосной информационной инфраструктуры увеличилось; невысокий уровень сотрудничества между деловыми кругами и правительственным обменом информацией; основные технологии контролируются другими; недостаточная координация общей стратегии; слабая защита критически важной инфраструктуры; мобильный интернет и другие технологии представляют собой серьезные проблемы». Важно признать, что многие из этих проблем являются результатом запутанной системы принятия политических решений по кибербезопасности в Китае, а не отсутствия ранее разработанных рекомендаций.

**[Смотрите также:   Дипломная работа по теме "Использование положительного образа христианства в литературе как способ управления религиозным сознанием"](https://sprosi.xyz/works/diplomnaya-rabota-po-teme-ispolzovanie-polozhitelnogo-obraza-hristianstva-v-literature-kak-sposob-upravleniya-religioznym-soznaniem/%22%20%5Ct%20%22_blank)**

По мнению ряда исследователей, кибербезопасность стала одной из главных проблем китайского правительства и привлекает внимание ее самых высокопоставленных руководителей. Тем не менее требуется координации в рамках обширного и сложного аппарата для выработки политики, что является сложной задачей. Национальная киберполитика в любой стране должна уравновешивать конкурирующие цели национальной безопасности, правоохранительной деятельности и регулирования промышленности в контексте международного рынка быстрых технологических изменений. Попытка Китая защитить контент Интернета, одновременно стремясь содействовать экономическому росту за счет Интернета, еще более затрудняет этот трудный баланс. Внимание элит делает более вероятным сценарий, в котором бюрократические трения в повседневном управлении политикой в области кибербезопасности будут продолжаться, что усилит неэффективность китайских средств защиты.

Вернемся к кибербезопасности Китая и, в более общем плане, к национальной стратегии и политике, которые принимаются государствами для смягчения киберугроз. Во главе Ли Юйсяо, директора Центра исследований и исследований в области интернет-технологий Пекинского университета почтовых и телекоммуникаций, и его соавтора Сюй Лу содержится китайская перспектива в отношении вызовов в киберпространстве, стоящих перед страной, неадекватность ответов Китая в области политики на сегодняшний день, и необходимость международного сотрудничества для снижения растущих рисков. Хотя Китай добился определенного прогресса в противостоянии растущей волны киберпреступности, включив массовые вспышки «поиска человеческой плоти» или кибер-издевательства, когда пользователи сети все вместе порочат жертву, Ли и Сюй утверждают, что серьезные недостатки сохраняются. К числу проблем относятся отсутствие постоянной ориентации на кибербезопасность со стороны правительства, неадекватная правовая основа как для облегчения координации в области безопасности, так и для защиты прав пользователей, несовершенного согласования между быстроизменяющимися технологиями и медленной политикой и недостаточного просвещения общественности о рисках киберпространства. Кроме того, Ли и Сюй утверждают, поскольку киберпространство является международным, международное сотрудничество необходимо для повышения его безопасности и надежности. В них освещаются причины недоверия между Соединенными Штатами и Китаем в этой области, ситуация только усугубляется непрерывным потоком сообщений СМИ о систематическом шпионаже со стороны каждого правительства. Однако, как и многие из китайских авторов, они по-прежнему оптимистично смотрят в будущее и предлагают изучить возможные пути повышения взаимного доверия.

Учитывая известную жестокость китайского контроля над интернетом, на Западе широко, но ошибочно полагают, что у Китая мало смысловой концепции личной неприкосновенности или правовой защиты. Сюй Цзинхон показывает, что Интернет в Китае действительно создает растущий спрос на право на неприкосновенность частной жизни, и законодательная поддержка конфиденциальности постепенно улучшается в ответ. (что в принципе доказывает закон, который вступит в силу с 1 июня 2017 года) Сюй прослеживает эволюцию концепции неприкосновенности частной жизни в китайском дискурсе от ссылки на постыдную или смущающую личную информацию на более широкую концепцию персональных данных, транзакций и мнений. Он описывает соответствующие законы и исследует причины их возникновения и их эффективность на практике. Конфиденциальность важна для надежной электронной коммерции и благосостояния уязвимых пользователей, но она также напряжена правительственными императивами для наблюдения за населением. Сюй приходит к выводу о том, что институциональные основы китайского киберпространства по-прежнему имеют возможность пойти на технологический прогресс.

**2. Контроль над интернетом в Китае**

«Интернет — это орудие работы, а не средство времяпрепровождения», — этот лозунг, широко распространенный в стране, четко отражает отношение властей к новым средствам массовой коммуникации. В ноябре 2005 г. в Китае принята Государственная стратегия развития информатизации на 2006-2020 гг. В ней были сформулированы основные направления развития интернета.

В 2009 г. около 95% городов и поселков имели высокоскоростной доступ к глобальной сети, а жители 92,5% китайских деревень — возможность подключиться к интернету через телефонную линию. Под воздействием государства быстро увеличивается число провайдеров интернет-услуг. Коммерческим провайдерам официально было разрешено заниматься предоставлением интернет-услуг в 1995 г. В настоящее время самыми крупными 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 состоит из нескольких специализированных сетей, в которые входят:

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

Ø  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;

Ø  коммерческие сети; наиболее крупные — China Net (http://www.bta.net.cn), государственная сеть, которая охватывает более 50% рынка интернет-услуг в стране и предоставляет интернет-сервис государственным организациям21, а также Golden Bridge Network (GBNet, http://www.gb.co.cn).

Данная сегментация позволяет пользователям интернета в Китае ориентироваться в зависимости от интересов и целей. Власти благодаря специализации контролируют деятельность пользователей и отслеживают противоправные действия.

Широкое распространение интернета в КНР не свидетельствует о том, что КПК ослабила контроль над ним. Скорее прослеживается обратный тренд — борьба против негативных последствий от информации лишь усиливается. На усиление сетевой цензуры направлены значительные усилия. С момента регистрации пользователей начинается слежение за его работой на местах. Если физическое лицо хочет стать интернет-пользователем — ему необходимо пройти проверку в местном полицейском отделении и предоставить справку установленного образца для провайдера. Согласно некоторым исследователям, кадровые работники Министерства общественной безопасности зачастую назначаются на высшие должности в крупных провайдерских компаниях.

Когда китайские власти осознали, что уследить за всеми пользователями сложно, они перераспределили функции контроля над сетью между операторами связи и органами власти на местах. Главный орган, который контролирует Интернет в КНР — Министерство промышленности и информатизации. В 2008 году его создали с целью развития интернета в Китае, распространения беспроводной связи, производства электронных и информационных товаров, индустрии программного обеспечения. На данное министерство возложено обеспечение технического функционирования интернета и информационных технологий.

За регулирование контента и электронную медиаиндустрию несет ответственность Государственное управление по делам радиовещания, кинематографии и телевидения. Управление ответственно за блокирование интернет-провайдерами доступа к порнографическим ресурсам и сайтам с азартными играми на централизованном уровне. Провайдеры интернета на собственные средства устанавливают специальные фильтры, также в их обязанности входит блокировка доступа к зарубежным ресурсам политического содержания, используя ключевые слова «диссидент», «Тайвань», «Тибет» и др. Алгоритм заменяет их на точки, сообщения удаляются. Многие западные СМИ, сайты большинства университетов США попали в перечень ресурсов, подвергающихся цензуре. Важно понимать, что нарушение данных правил может повлечь серьезное наказание: провайдер может лишиться лицензии на предоставление услуг связи, частным лицам предусмотрена смертная казнь за публикацию материалов, не угодных правительству.

Китайские законы и нормативные акты в отношении Интернета известны особой жестокостью. В 1994 году Госсоветом КНР были выпущены Правила регулирования, обеспечивающие безопасность компьютерных и информационных систем, — тем самым Министерство государственной безопасности получило права и полномочия на управление сетью. Правительство обладает правом нейтрализовать (практически) любой неугодный ресурс. Ответственность предусматривается за публикацию «материалов, вредящих репутации государства». Однако не существует никаких способов определения, вреден ли материал или нет.

Согласно национальному законодательству, в КНР доступ к интернету разделен на две ступени. На первой ступени пользователи имеют возможность выйти в мировую сеть посредством магистральных узлов (backbone networks). Существует несколько подобных ключевых узлов. Они подконтрольны центральным министерствам или группам, обладающим мощной политической поддержкой власти. На китайский интернет-трафик наложена система файрволов, которая ограничивает доступ к проблемным, по мнению государства, внешним ресурсам. В Китае реализуется проект Золотой щит — сложная система фильтрации содержимого интернета. Благодаря проекту функционирует система серверов на интернет-канале между провайдерами и международными сетями передачи информации, которая фильтрует информацию. Файрволы применяются китайскими провайдерами для защиты от вирусов и хакеров, а также для блокирования доступа к определенным сайтам.

Для обеспечения успешного построения коммунизма к гражданам не должна попадать лишняя информация. Интернет в Китае рассматривается как средство, способствующее эффективной работе, а не место для развлечения. Если на вебсайте находится лишняя информация — он подвергается фильтрации, доступ к нему приостанавливается. Под данную категорию «лишней» информации попадают не только антикоммунистические сайты, но и многие мировые ресурсы, к примеру, Википедия. Власти также проводят репрессивные меры по отношению к антиправительственным акциям в интернете. В категорию государственных преступлений попадает и пересылка секретных или реакционных материалов по IP-сетям. Наказания предусматривают и денежные штрафы, и лишение права выхода в интернет.

В 2001 году начало работу Китайское общество пользователей интернета, которое в действительности было создано для проведения в жизнь решений правительства по контролю над глобальной сетью. К настоящему моменту общество приняло ряд документов по регуляции деятельности интернет-пользователей.

Ø  Конвенция об отраслевой самодисциплине в сфере интернета в Китае

Ø  Правила самодисциплины о запрете на распространение в интернете развратной, порнографической и другой недолжной информации

Ø  Конвенция о бойкотировании вредоносных программ

Ø  Конвенция о самодисциплине в области обслуживания блогосферы

Ø  Конвенция о самодисциплине в области борьбы с сетевыми вирусами

Ø  Манифест об отраслевой самодисциплине в области издательского права в интернете

В 2005 году было запрещено анонимное общение, введена обязательная регистрация сайтов, проведена серия облавов (?) на владельцев нелегальных интернет-кафе. Тенденция к ужесточению продолжалась. В 2006 году было создано специальное полицейское ведомство для контроля за интернетом. Интернет-полицейские следят за содержанием сайтов, онлайн-форумами и социальными сетями. Многие крупные китайские сайты требуют обязательной регистрации — ввод настоящих личных данных, включая имя, адрес, идентификационный номер — даже чтобы просто оставить сообщение или завести свой блог. Достоверность данных проверяется через компьютерный банк данных, только после этого регистрация считается пройденной.

В отношении корпораций и компаний действуют еще более жесткие правила. Любая фирма, чтобы подключиться к интернету, должна пройти тщательную проверку на протяжении нескольких месяцев. Действия всех корпоративных клиентов фиксируются, нарушители несут наказание. На предприятиях ведется журнал, где хранятся аргументы в пользу посещения каждого сомнительного вебсайта. Существует практика внедрения публичной электронной почты — группе сотрудников присваивается один адрес, переадресация писем производится через системного оператора или дежурного администратора локальной сети.

Если юридическое лицо желает создать сайт, ему необходимо получить лицензию, выдаваемую Министерством промышленности и информатизации. Уставный капитал компании должен внушать доверие. С 2008 года, согласно новым правилам, подавать заявки на получение лицензий на радиовещание или потоковую трансляцию (видео) онлайн могут только компании, принадлежащие властям или контролируемые государством. В 2009 г. вступил в силу закон о том, что для регистрации доменных имен в зоне .cn необходимо подавать письменное заявление, в котором помимо всех личных данных надо

указывать и номер лицензии предприятия на коммерческую деятельность.

Кибербезопасность стала ключевым приоритетом не только для НОАК, но и для китайского правительства, которое сделало несколько важных шагов, чтобы бороться с вызовами законодательных уязвимостей, несовершенных институтов и неудовлетворительного уровня образования среди общественности.

**Гражданские документы информационной безопасности:**

До создания национального плана гражданской безопасности Китая, который известен как Документ 27, несколько рабочих групп затронули связанные с этим вопросы. Однако отсутствие координации и постоянной реструктуризации вызвало большую неуверенность для всех игроков. Национальное внимание к информационным технологиям началось в 1986 году с создания малой руководящей группы по управлению государственной экономической информацией и было поддержано в 1999 году и 2001 году созданием руководящей группы по информатизации государства (SILG). В 2003 году небольшая группа по координации государственной сети и координации информационной безопасности (SNISCSG) была создана в качестве подгруппы в рамках SILG под председательством нынешнего премьер-министра Ли Кэцяна. Цели этих трех групп состояли в том, чтобы развить местные информационные технологии и включить их в контекст национальной безопасности. Десятый пятилетний план Китая 2001 года уделял приоритетное внимание развитию национальной инфраструктуры информационной безопасности и поддержке крупных инвестиций в государственные и частные ИТ-фирмы, которые должны были сосредоточиться на защите от вредоносных программ и общей интернет-безопасности.

В начале 2000-х годов развитию ИКТ было уделено внимание как со стороны президента Цзян Цзэминь и президента Ху Цзиньтао, который начал говорить о национальной безопасности и экономической безопасности как о неделимой паре, отсюда следует необходимость «скачка» над конкурентами, чтобы превратить исторические недостатки Китая в сильные стороны посредством инновационного развития. В 2003 году SNISCSG выпустил Документ 27, в котором были реализованы основные направления политики в области кибербезопасности и национальные стратегии, в том числе планы аварийного восстановления, управления инцидентами и обеспечения безопасности электронного правительства.

Заключение руководящей группы по государственной информатизации от 2003 года (Документ 27) стало фундаментом всей национальной политики в области кибербезопасности. Оно описывало ряд инициатив, включая схему многоуровневой защиты для критически важной инфраструктуры, криптографию для достоверных систем, мониторинговые системы для информационной безопасности, процессы управления в аварийных ситуациях, поддержка исследований в области безопасности, определения технических стандартов, расширенное профессиональное обучение, гарантированное финансирование для проведения инициатив. Заключение было сфокусировано главным образом на оборонительных мерах, в нем не упоминалось о наступательных возможностях в киберпространстве, в основном как и в документах национальной политики в киберпространстве в других странах.

После 2008 года активность SNISCG пошла на убыль. Фокус Государственного Совета был временно смещен на проведение Олимпиады и глобальный финансовый кризис. На протяжение следующего десятилетия финансирование по Документу 27 позволило агентствам расти и защищаться друг от друга или перспективных новичков. Отрасль китайской информационной безопасности выросла с 3,4 млрд юаней в 2003 году до 17,9 млрд в 2011 году. Национальные компании рынка включают Хуавэй (защита роутеров и переключателей (switch)), Venustech (защита от проникновения и угроза систем менеджмента), Qiho 360 (антивирусное ПО), Leadsec (файрвол), Westone (шифрование).

Однако стоит понимать, что прибыльность данных компаний не конвертируется напрямую в мощную кибербезопасность Китая, однако, по мнению Совета/комиссии по развитию и реформам и регулятора продовольственной безопасности. Это вылилось по мнению одного аналитика китайской отрасли в «недостаток всеобщего планирования», децентрализацию силы, принимающей политические решения, недостаток адекватной коммуникации.

Первоначально засекреченной идеей Документа 27 была концепция «активной защиты», разработки различных стратегий защиты критической инфраструктуры, увеличения шифрования и динамического мониторинга, совершенствования редких инноваций, а также было затронуто руководство по кибербезопасности, улучшения его координации и финансирования. Документ 27 был полезен при разработке необходимой политики, но увольнение SNISCSG в 2008 году привело к дезорганизации гражданской кибербезопасности Китая, что привело к различным отдельным, неприсоединившимся политическим инициативам различных органов. Несмотря на то, что SNISCSG был восстановлен в 2009 году, открытых отчетов о его заседаниях нет, а различным министерствам было поручено внедрить стратегии. Однако успешность их имплементаций до конца не ясна.

Начиная с февраля 2006 года все события в сфере информационной безопасности и связанные с ними политики могут так или иначе быть связаны с 15-летней великой стратегией Китая в отношении будущих инноваций. Госсовет выпустил «Национальную программу развития науки и техники в средне- и долгосрочной перспективе на 2006-2020 годы». Дитер Эрнст из Центра Восток-Запад считает этот документ краеугольным камнем общей стратегии стандартизации Китая, который состоит из различных правовых документов и политических инициатив. Он также считает, что стратегия должна быть проанализирована в более широком контексте — Китай стремится достичь уровня и качества жизни Запада, а не только преследует технологические задачи, касающиеся киберпространства. Для достижения этой цели вместо того, чтобы просто принимать действующие стандарты, китайское правительство хочет стать ведущим актором, задающим международные стандарты посредством инноваций. Соответственно, в документе перечислены цели Китая в области технологических прорывных инноваций, также правительство признает необходимость увеличения инвестиций в научные исследования и разработки.

Другие исследования предполагают, что этот план отражает решимость Китая преодолевать внутренние, социальные и экологические проблемы посредством технологических новшеств, продолжая при этом твердо придерживаться понимания, что только правительство может стимулировать такие инновации, направляя и поддерживая предприятия и бизнес-сектор, которые будут непосредственно осуществлять стратегии. Возможно, самым важным аспектом для международного сообщества является решимость Пекина ослаблять связи с иностранными инновационными фирмами, для того чтобы заложить основу для независимой базы знаний. Поэтому опасения по поводу возможного появления «техно-национализма» также имеют место.

План призывает Китай не приобретать «основные технологии в ключевых областях, которые влияют на жизненную основу национальной экономики и национальной безопасности» из-за рубежа, включая интернет-технологии следующего поколения, станки с цифровым управлением и системы наблюдения Земли с высоким разрешением. Для достижения этой цели правительство увеличило расходы на исследования и разработки, которые к 2020 году вырастут до 2,5% ВВП. Считается, что Китай обойдет США к 2020 году. Оценочные данные по Китаю в 2016 году остаются примерно на уровне 2% или 396,3 млрд. долл. США, в то время как расходы США составляют 2,77% и 514 млрд. долл. США соответственно, при этом остается существенный разрыв между странами. Несмотря на то, что цифры Китая показывают почти двукратное увеличение с 213,4 долл. США в 2010 году, к ним необходимо относится с некоторой долей скептицизма, поскольку большая часть бюджета расходуется на развитие инфраструктуры, а не на научные исследования. Тем не менее, у китайских исследователей и предприятий все больше появляется стимулов и поддержки для развития интеллектуальной собственности, выполняя желание правительства уменьшить зависимость от иностранных технологий. Несмотря на добрые намерения, такая политика может фактически усилить промышленный шпионаж, поскольку многие местные предприятия испытывают недостаток в необходимых навыках и, таким образом, приобретают необходимые технологии из-за рубежа и просто изменяют их по мере необходимости, часто нелегально. Здесь можно найти еще одно противоречие: Китайское понимание «коренных» особенностей — подразумевает создание оригинальных инноваций, новых продуктов и услуг. Это судя по всему противоречит цели китайского кибер-шпионажа, который позволяет нарушителям оставаться вдалеке от оригинальности и полагаться на установленные модели. Стратегия на 15 лет не затрагивает каких-либо конкретных военных целей или проблем.

В 2007 году была введена обширная «Многоуровневая схема защиты», направленная на защиту национальной безопасности, подразумевала запрет иностранным компаниям продавать какие-либо основные продукты государственным, банковским, транспортным и другим важным компаниям инфраструктуры. Также обязательная сертификация 2010 года «Система защиты информации» требовала, чтобы иностранные компании, желающие продавать китайскому правительству продукты, должны были предоставить свои продукты интеллектуальной собственности правительству. Продолжение этой тенденции в феврале 2015 года ознаменовало начало «нового режима кибербезопасности», который предполагает, что все иностранные технологические фирмы, поставляющие услуги китайским банкам, могут потребовать разделить их исходный код и даже внедрить «backdoor» в аппаратное и программное обеспечение. Все, что связано с киберпространством и информационными технологиями, постоянно доказывает тот факт, что китайцы не отказываются от своих амбиций.

**Новое политическое заключение Канцелярии Государственного совета по информации**

В июле 2012 года Информационное бюро Государственного совета (SCIO) опубликовал новое политическое заключение (NPO). Даже несмотря на то, что он был выпущен спустя почти десятилетие после Документа 27 и более чем через полвека после 15-летней стратегии, его общие проблемы остаются теми же, показывая, что не все цели были достигнуты. Он настойчиво отмечает подверженность Китая неотложным вызовам в международной конкуренции за контроль, использование и приобретение информации. Точнее, дисбаланс между Западом и Китаем в цифровой инфраструктуре, неэффективный обмен информацией между правительством и промышленностью, плохое планирование обеспечения кибербезопасности, неадекватные оборонные возможности и постоянно большая доля контроля над основными технологиями со стороны иностранцев привлекают наибольшее внимание. В отличие от предыдущих документов, НПЗ связывает развитие информационной безопасности с экономическим и социальным улучшением жизни людей. Это свидетельствует о расширении «защиты информации о национальной безопасности» до «содействия стабильному и быстрому экономическому развитию, социальной гармонии и стабильности». Джайлс и Хагестад подготовили четыре стратегических мандата НПЗ, которые, как и ранее проанализированные документы сосредоточили внимание на гражданской киберзащите:

Ø  Во-первых, НПЗ уделяет большое внимание безопасности всех важнейших информационных систем и инфраструктуре, особое внимание — информационным сетям. Это можно интерпретировать как заказ, а не руководство, на то, что политики должны защищать — интернет, радиосети и частные телекоммуникации, а также информационные сети, связанные со сферами финансов, энергетикой и транспортом. Его явная цель — защита тех отраслей, где кибератака нанесет огромный ущерб экономике Китая.

Ø  Во-вторых, НПЗ стремится укрепить государственные и секретные системы информационной безопасности, которые часто являются привлекательными целями для хактивистов и анонимов. Для исполнения Госсовет ожидает, что правительственные агентства, чтобы уменьшить их интернет-связность и повысить безопасность информации и мониторинг защиты конфиденциальности путем создания иерархической системы защиты секретной информации.

Ø  В-третьих, НПЗ стремится к усилению защиты промышленных систем управления объектами, такими как трубопроводы нефти и газа, ядерной и энергетической инфраструктур, а также транспортных и городских объектов. Это должно быть достигнуто путем укрепления нормативных положений и проведения более частые проверов безопасности и оценки рисков.

Ø  Наконец, НПЗ обращается к защите личной информации китайских граждан, отмечая ее значимость в достижении общего благосостояния страны. Этот шаг можно рассматривать как противодействие атаке в 2012 году, которая скомпрометировала миллионы пользователей на форуме мнений Tianya и сайте 360buy.com.

НПЗ, безусловно, является очень всеобъемлющим документом, который охватывает большинство важных областей кибербезопасности. Рекомендации Госсовета указывают на основные недостатки китайской модели информационной безопасности и на возросшую уязвимость от растущей кибер-зависимости. Постоянная враждебность по отношению к зарубежным технологиям также предполагает, что соответствующие торговые барьеры не будут отменены в ближайшем будущем. Однако, как интригующий момент в свете антикоррупционной кампании президента Си, НПЗ, похоже, не рассматривает коррупцию, которая довольно широко распространена в технологической отрасли. Поскольку разгон не был полностью успешным, правительство могло бы подумать о награждении законных чиновников и предпринимателей, чтобы устранить нечестных акторов, ставящих под угрозу развитие отрасли. В целом, НПЗ указывает, что информационная безопасность к 2012 году уже стала одним из приоритетов правительства.

**[Смотрите также:   Дипломная работа по теме "Проект офисного здания"](https://sprosi.xyz/works/diplomnaya-rabota-po-teme-proekt-ofisnogo-zdaniya/%22%20%5Ct%20%22_blank)**

**3. Китай и международные отношения в киберпространстве**

Было время, когда киберпространство характеризовалось незначительным количеством угрозам и широко распространенным согласием относительно полезности Интернета. Тем не менее, текущие тенденции движут киберпространство к меньшему сотрудничеству и большей конкуренции. Выход Китая на глобальную арену способствовал нестабильности в международном киберпространстве, так как экономические императивы и желание политического доминирования способствуют шпионажу за рубежом. Императивы одной политической партии способствуют жесткой цензуре в интернете на национальном уровне. Однако и в Китае, и Соединенных Штатах, как и во многих развитых индустриальных странах, раскол между правительственными бюрократиями, которые будут регулировать безопасность, и промышленными субъектами, которые изобретают и эксплуатируют информационные технологии, еще больше усугубляет уязвимость Интернета.

Китай занимает 13 место в рейтинге кибермогущества (34,6), первую пятерку представляют Великобритания (76,8), США (75,4), Австралия (71), Германия (68,2), Канада (66,6).

В рейтинге регуляторных рамок/фрэймворков занимает 18 место, 27.4, (26,3% в общем рейтинге), Германия здесь занимает первое место (99,3), далее США, Великобритания, Франция, Япония. В экономическом и социальном контексте Китай располагается на восьмой строчке (50,9), США, Япония, Австралия, Канада, Великобритания составили пятерку лидеров.

В рейтинге технологической инфраструктуры Китай находится на 14 месте, в индустриальном применении — 11 место. Другие азиатские страны как Япония и Южная Корея в принципе также, как и Китай, находятся в середине индекса — восьмое и седьмое места соответственно.

Во многом это связано с тем, что Китай только еще формулирует политику защиты киберпространства (cyber protection policy). Кроме того, в Китае отсутствует свободный поток информации из-за высокого уровня цензуры, поэтому в рейтинге регуляторных рамок Китай находится в конце списка вместе с Саудовской Аравией. В январе 2010 года между Китаем и корпорацией Гугл было заведено судебное дело по поводу цензуры, что привело к уходу компании с рынка.

Саммит Большой Двадцатки в Ханчжоу выпустил Инициативу по сотрудничеству и развитию электронной экономики стран Большой двадцатки. кибербезопасность китайский законодательный

В марте 2017 года была выпущена Международная стратегия сотрудничества в киберпространстве (International Strategy of Cooperation on Cyberspace). В данном разделе будет представлено объяснение китайской политики и позиции в международных отношениях, касающихся киберпространства. Кроме того, мы рассмотрим основные принципы, стратегические цели и план действий в отношениях с третьими сторонами в данной сфере. Стратегия предписывает участие Китая в международном обмене и сотрудничестве в киберпространстве на следующий период и побуждает международное сообщество собраться вместе и усилить диалог и кооперацию и построить мирное, безопасное, открытое, кооперативное и упорядоченное кибепространство, а также многостороннюю, демократичную и прозрачную глобальную систему управления Интернетом.

**Основные принципы:**

Китай всегда стоял за международный мир, вносил свой вклад в глобальное развитие и защищал международный порядок. Быстро и неуклонно преследовал путь мирного развития, руководствуясь сотрудничеством win-win.

2.       Принцип суверенитета

3.       Принцип совместного правительства разделенной ответственности

4.       Принцип разделяемых выгод

Стратегические цели:

.         Защита суверенитета и безопасности

.         Разработка системы международных правил

.         Продвижение справедливого руководства интернетом

4.       Защита законных прав и интересов граждан

.         Продвижение сотрудничества по электронной экономике

.         Строительство платформы для культурного обмени в сети

План действий:

.         Мир и стабильность в киберпространстве

.         Порядок основанный на правилах в киберпространстве

.         Партнерство в киберпространстве

.         Реформа системы глобального управления интернетом

.         Международное сотрудничество по кибертерроризму и киберпреступлениям

.         Защита прав и интересов граждан, включая конфиденциальность

.         Экономика sharing и разделение электронных дивидендов

.         Развиие и защита глобальной информационной инфраструктуры

.         Культурный обмен в киберпространстве

Рабочая группа по кибербезопасности между США и Китаем была отозвана после инцидента с хаккерами в мае 2014 года. Тот факт, что 8ой раунд диалога между США и Китаем затронул проблему кибербезопасности свидетельствует о попытках поиска общего основания для начала диалога. Весь вопрос сводится к пониманию: будут ли США и Китай придерживаться общих интересов, или же стратегическая конкуренция возьмет верх в новом анархическом состоянии.

В 2015 году КНР согласилась с отчетом UN’s Group of Government Experts, что определенные нормы и аспекты существующего международного права, включая Устав ООН действительно применимы к киберпространству.

В сентябре 2015 года во время государственного визита Си Цзиньпина в США он согласился ограничить кибершпионаж в коммерческих целях и пообещал, как и Барак Обама, воздержаться от кибератак на критическую гражданскую инфраструктуру в мирное время.

Хотя такие результаты обнадеживают, перспективы будущего прогресса в кибер-проблемах должны оцениваться с учетом соответствующих аспектов китайского, особенно НОАК, стратегического мышления в кибер-сетевых войнах. Если дипломатическая активность не окажет влияния на стратегическое мышление НОАК и не ограничит его оперативный подход к «военной борьбе в киберпространстве», доверие к риторическим обязательствам Пекина останется под вопросом. Конечно, продолжение усилий по решению кибербезопасности в китайско-американских отношениях может иметь решающее значение для улучшения взаимных неправильных представлений, создания механизмов управления кризисами для уменьшения рисков эскалации и, возможно, в конечном счете для продвижения к формированию консенсуса относительно потенциальных «правил игры» для киберпространства. Однако эти усилия должны быть основаны на понимании мнения различных стратегов и операторов в НОАК, которые часто значительно отличаются от сформулированных дипломатических позиций Китая по этой теме. Этот анализ является первоначальной попыткой обрисовать эти перспективы, чтобы понять возможные ограничения и потенциальные возможности для соглашения между США и Китаем относительно будущего международного кибер-порядка.

Стратеги в НОАК рассматривают формирование правила для киберпространства в большинстве случаев как стратегическую конкуренцию великих держав. Генерал Хао Ели, вице-президент китайского института инноваций и стратегии развития и бывший замдиректор Четвертого управления НОАК утверждает, что «формирование правил для киберпространства в действительности представляет собой процесс игры в шахматы между великими державами».

Отношения между Китаем и США в сфере кибербезопасности достигли пика в 2013 году, что привлекло внимание высших руководителей обеих стран. В январе крупнейшие американские газеты обвинили Китай в том, что он взломал компьютеры, чтобы преследовать журналистов и мешать сообщать о китайских чиновниках. В феврале фирма по предоставлению услуг кибербезопасности «Mandiant» опубликовала крупный разоблачительный материал о китайском экономическом шпионаже, связанный с конкретным подразделением НОАК в Шанхае. Официальные лица США усилили риторическое давление на КНР, называя и осуждая китайское государство за поддержку кибершпионажа. Затем Эдвард Сноуден совершил разоблачительное признание. После утечки высоко секретных документов о программах кибершпионажа АНБ журналистам, Сноуден бежал в Гонконг в июне, где дал интервью местным журналистам, утверждая, что АНБ взломало китайские университеты, телекоммуникационные фирмы и подводные кабели. Обнародование широкомасштабного надзора со стороны АНБ через американские интернет-фирмы (описанные в Китае как «Prism-gate» после названия одной из скомпрометированных программ АНБ) подорвало одним ударом усилия Вашингтона, направленные на то, чтобы занять высокие позиции в отношении китайского шпионажа и усилия американских фирм по выстраиванию репутации независимости от Вашингтона. Более того, разоблачения Сноудена случились за несколько дней до первой встречи Си Цзиньпина на посту президента Китая с президентом Обамой, СМИ писали только о Сноудене. Дальнейшие откровения Сноудена, кульминацией которых стало подтверждение о глубоком проникновении АНБ в Huawei, укрепили китайскую позицию по поводу американского шпионажа, даже когда средства массовой информации, сообщающие о китайском шпионаже сократились (во многом благодаря тому, что высокопоставленные китайские лидеры сдерживали активность НОАК после отчета Mandiant и после того как западные журналисты стали больше интересоваться сообщениями о файлах Сноудена). Американские попытки сформулировать различие между политико-военными целями кибершпионажа США и экономическими целями китайского шпионажа или китайским контролем над интернетом, и сбором метаданных со стороны АНБ, как правило, не увенчались успехом/остались без комментариев.

**4. Законодательный фрэймворк киберпространства**

До 2014 года

Более ранние законы и нормативные акты, которые больше ориентированы на безопасность системы и инфраструктуры, включают:

•Положение Государственного совета об обеспечении безопасности компьютерных информационных систем, административные меры для информационных служб Интернета (计算机信息网络国际联网安全保护管理办法)

•Административные меры по предупреждению и лечению компьютерных вирусов, выпущенные Министерством общественной безопасности.

•Административные меры для иерархического обеспечения защиты информационной безопасности, выпущенные Министерством общественной безопасности и пятью другими министерствами.

• Закон о защите государственных секретов (Постоянный комитет ВСНП).

год

Генеральный секретарь ЦК КПК Си Цзиньпин был назначен главой Руководящей группы по кибербезопасности, которая была создана в феврале 2014 года. «Поддержание кибербезопасности» впервые было включено в отчет о работе правительства во время Всекитайского собрания народных представителей и Народной политической консультативной конференции.

год

В июне 2015 года XII Всекитайское собрание народных представителей обсудило проект Закона о кибербезопасности КНР. В июле 2015 года на основе комментариев общественности и отзывов членов Постоянного комитета ВСНП и других сторон, был изменен проект Закона о кибербезопасности, на основе второго заседания был создан второй проект Закона о кибербезопасности.

год

В июне 2016 года XII Всекитайское собрание народных представителей обсудило проект Закона о кибербезопасности второй раз. В июле 2016 года проект Закона о кибербезопасности для второго обсуждения был опубликован на сайте Народного конгресса для общественного обсуждения. В ноябре Закон о кибербезопасности Китайской Народной Республики был принят на 24-м заседании Постоянного комитета XII Всекитайского собрания народных представителей 7-го созыва с 154 голосами «за» и одним воздержавшимся.

Официально закон вступит в силу с 1 июня 2017 года.

**.1 Ключевые моменты закона о кибербезопасности**

·        Закон уделяет особое внимание защите персональной информации и индивидуальной конфиденциальности.

·        Закон стандартизирует сбор и использование персональной информации

·        Компании должны концентрироваться не только на безопасности данных, но также на защите от вмешательства в частную жизнь (право на неприкосновенность частной жизни), что по сути очень важно.

Требования к безопасности для сетевых операторов:

·        Закон представляет четкие определения сетевых операторов и требования к безопасности;

·        Большинство крупных финансовых институтов могут стать «сетевыми операторами»;

В отношении критически важной информационной инфраструктуры:

·        Закон предъявляет большие требования к защите инфраструктуры ключевой информации;

·        Закон определяет специфику объема критически важной информационной инфраструктуры;

Ограничения на передачу персональной информации и коммерческих данных за рубеж:

·        Зарубежные компании и организации обычно нуждаются в передаче информации за пределы Китая

·        Закон о кибербезопасности предусматривает, что конфиденциальные данные должны хранится внутри страны

Наказания и штрафы:

·        Наказания за нарушение закона четко сформулированы, включают приостановление предпринимательской деятельности

·        Серьезная незаконная деятельность может привести к закрытию бизнесов или к отзыву лицензий

·        Максимальный штраф может достигать одного миллиона юаней

Таблица 3

|  |  |  |
| --- | --- | --- |
| Статья | Итоговая версия | Значительная поправка |
| Статья 31 | Статья 31. В отношении обеспечения кибербезопасности, государство акцентирует внимание на защите критической информационной инфраструктуры в общественных информационных и коммуникационных службах, энергетике, финансах, транспорте, водном хозяйстве, коммунальных услугах и электронном управлении и других важных с информационной точки зрения инфраструктурных отраслях, которые могут причинить серьезный ущерб национальной безопасности, национальной экономике и общественным интересам в случае разрушения, утраты функциональности или потери и утечки данных. | Статья проясняет отрасли и сектора, в которых защите критической информационной инфраструктуры будет отдан приоритет. |
| Статья 43 | Физические лица вправе требовать от операторов сети внесения исправлений в личную информацию, которую они собирают и хранят. Операторы сети должен принять меры для удаления или исправления ошибок. | Данная статья дает гражданам больше прав для защиты их персональной информации, а также увеличивает обязательства операторов сети по своевременному исправлению ошибок. |
| Статья 46 | Физические лица и организации, ответственные за использование их сетей, не должны создавать сайты и коммуникационные группы для мошеннических целей и других видов незаконной деятельности. | Данная статья подчеркивает, что физические лица и организации несут ответственность за использование их сетей. |
| Статья 76 (5) | Персональная информация относится ко всем видам информации, записываемой в электронном виде или посредством других средств, которые могут установить личность независимо или в совокупности с другой информацией, включая, но не ограничиваясь настоящим именем человека, датой рождения, номером паспорта, персональной биометрической информацией, адресом и номером телефона. |  |
| Статья 63 | Люди, нарушившие Статью 27 Закона и участвующие в деятельности, угрожающей кибербезопасности могут быть задержаны на срок от 5 до 15 дней и могут быть оштрафованы на сумму от 100 000 до одного миллиона юаней, в зависимости от серьезности инцидента. | Максимальное наказание за нарушение закона о кибербезопасности было увеличено до одного миллиона юаней. |

**4.2 Особенности нового закона о кибербезопасности**

Закон о кибербезопасности содержит ряд требований к кибербезопасности, включая гарантии национального суверенитета киберпространства, защиту критической информационной инфраструктуры и данных, а также защиту частной жизни. Закон также определяет обязательства по кибербезопасности для всех сторон. Предприятиям и смежным организациям следует установить приоритетность следующих основных положений Закона о кибербезопасности:

·        В Законе о кибербезопасности четко указаны требования к сбору, использованию и защите личной информации.

·        Критическая информационная инфраструктура: В Законе о кибербезопасности часто упоминается «критически важная информационная инфраструктура».

·        Сетевые операторы: «Операторы сети» являются владельцами и администраторами сетей и поставщиков сетевых услуг. Закон о кибербезопасности разъясняет обязанности операторов по обеспечению безопасности.

·        Сохранность конфиденциальной информации: Закон о кибербезопасности выдвигает требование обработки и хранения личной информации / важных данных внутри страны.

·        Сертификация продуктов безопасности: Критическое кибер-оборудование и специальные продукты для обеспечения кибербезопасности могут быть проданы или предоставлены для использования только после получения сертификатов.

·        Юридическая ответственность: Предприятия и организации, нарушающие Закон о кибербезопасности могут быть оштрафованы на сумму до 1 000 000 юаней.

В китайском источнике подчеркивается важность соответствующих карательных мер по отношению атак со стороны зарубежных организаций, атакующих критически важную информационную инфраструктуру. Регулирование зарубежных властей также может осуществляться в соответствии с этим законом — департаменты общественной безопасности и соответствующие подразделения могут решить заморозить их деятельность.

По мнению китайских должностных лиц, в век информации укрепление сетевой безопасности является основой фундамента национальной безопасности, стратегической необходимостью поддержания общей безопасности в стране. Обеспечение охраны идеологии в киберпространстве является реальная необходимостью для Китая.По мнению Си Цзиньпина**,**без сетевой безопасности — нет национальной безопасности; нет информатизации — нет модернизации. Департаментам всех уровней провинций настоятельно рекомендовали тщательно изучить и реализовать дух выступлений Генерального секретаря Си Цзиньпина, чтобы постоянно совершенствовать чувство безотлагательности и ответственности за работу по кибербезопасности.

Закон о кибербезопасности является первым основным законом Китая о кибербезопасности. Для стратегии государства в киберпространстве это является важной вехой.

**Заключение**

Кибер-шпионаж представляет собой непрекращающуюся постоянную угрозу национальной и экономической безопасности любой страны во всем мире. В последние годы Китай стремительно развивается и стал уделять особое внимание обеспечению своей кибербезопасности.

Широко признано, что китайская кибер-разведка растет изощренно, постоянно используя новые технологии и методы наряду со своими традиционными источниками внутреннего контроля и наблюдения и внешними операциями. Китай находится в переходном периоде создания полноценной инфраструктуры обеспечения кибербезопасности и контроля над интернетом.

В данной работе мы доказали и охарактеризовали специфичность и самобытность китайской системы кибербезопасности — интеграция военных и гражданских структур, а также описали позицию Китая в международном киберпространстве — стремление к сотрудничеству и пересмотру глобального интернет регулирования.

В исследовании были подробно рассмотрены структуры китайской системы обеспечения кибербезопасности — руководящая группа по кибербезопасности и информатизации, возглавляемой Си Цзиньпином, подразделения Министерства общественной безопасности и Министерства государственной безопасности, а также подразделения НОАК (Третье и Четвертое управления), отвечающие в основном за разведывательные операции в киберпространстве. Мы проанализированы изменения после военной реформой в КНР, а именно создание Войск стратегической поддержки, которые будут включать в себя и Третье управление, и Четвертое управление. В данном исследовании была охарактеризована законодательная база контроля над интернетом в Китае — новый Закон о кибербезопасности, выделены ключевые тенденции нововведений, рассмотрены основные положения законов о кибербезопасности, оценены взаимоотношения Китая с ключевыми игроками на международной арене (США), а также прояснить специфику позиции КНР по глобальному регулированию интернета.

Китай действительно пытается создать мощнейшую систему обеспечения кибербезопасности — которая широко опирается на международный опыт, но в то же время обладает самобытностью и соответствует китайским условиям и особенностям политической системы, специфике КПК.

**Литература**

Научная литература

1.      Е. Евдокимов. Политика Китая в глобальном информационном пространстве. Международные процессы: журнал теории международных отношений и мировой политики. Том 9. № 1 (25), Январь — Апрель. М., 2011. 152 с.

2.       Ибрагимова Г. Стратегия КНР в области управления интернетом и обеспечения информационной безопасности. ПИР-центр. [Электронный ресурс] URL: http://www.pircenter.org/media/content/files/10/13559.. (дата обращения 9.05.2017)

.         Кашин В.Б. КНР и «третья стратегия компенсации» Министерства обороны США. Вестник Московского университета. Серия 25: Международные отношения и мировая политика, Изд-во Моск. ун-та (М.), том 8, № 3, 2016.

.         Кашин В. Б. Китайские разведывательные службы: общая структура, основные направления деятельности. Экспорт вооружений, № 3, 2014.

.         Кибербезопасность и управление интернетом: Документы и материалы для российских регуляторов и экспертов / Отв. ред. М.Б. Касенова; сост. О.В. Демидов и М.Б. Касенова. — М.: Статут, 2013. — с.461.

.         Китайская научно-техническая программа «863»(звук). Международное радио Китая. 28.02.2007. [Электронный ресурс] URL http://russian.cri.cn/307/2007/02/28/1@162708.htm (дата обращения 04.05.2017)

.         Черненко Е., Габуев А. Оружие к сбою! // Коммерсант. 15.02.2011 . [Электронный ресурс] URL: http://www.kommersant.ru/doc/1585823 (дата обращения 9.05.2017)

.         Юрченко Г. Киберборьба по взглядам руководства Китая. Военное обозрение. [Электронный ресурс] URL: http://www.belvpo.com/ru/13593.html (дата обращения 11.05.2017)

Зарубежные источники литературы

9.      Ball, D. China’s cyber warfare capabilities. Security Challenges, 7(2), 2011. P. 81-103.

10.     Bhunia P. China CERT report highlights rise in cyberthreats associated with IoT devices and networked industrial systems. 23.04.2017. [Электронный ресурс] URL: http://www.opengovasia.com/articles/7544 (дата обращения 30.04.2017)

11.     Blasko D. The New PLA Joint Headquarters and Internal Assessments of PLA Capabilities. China Brief, Volume 16, Issue 10. https://jamestown.org/program/the-new-pla-joint-headq..

12.     Chinese Cultural Market Network. [Электронный ресурс] URL: http://www.ccm.gov.cn/swordcms/publish/default/static.. (дата обращения 30.04.2017)

13.     China Daily. ‘Sense of benefit’ highlighted as China strives to build cyber power. [Электронный ресурс] URL: http://www.chinadaily.com.cn/business/tech/2017-04/19.. (дата обращения 29.04.2017)

14.     International Strategy of Cooperation on Cyberspace. Full Text: [Электронный ресурс] URL: http://news.xinhuanet.com/english/china/2017-03/01/c\_.. (дата обращения 30.04.2017)

15.     A ChinaFile Conversation. Can China’s Approach to Internet Control Spread around the World? 09.05.2017. [Электронный ресурс] URL: http://www.chinafile.com/conversation/can-chinas-appr..

16.     China’s Intelligence Services and Espionage Operations. Hearing Before the U.S.-China Economic and Security Review Commission, One Hundred Fourteenth Congress, Second Session. Thursday, June 09, 2016. Washington: 2016.

17.     China Statistical Report on Internet Development. January 1, 2017. [Электронный ресурс] URL: http://www.cnnic.cn/hlwfzyj/hlwxzbg/hlwtjbg/201701/P0.. (дата обращения 30.04.2017)

18.     China’s Xi calls for better development of Internet. [Электронный ресурс] URL: http://news.xinhuanet.com/english/2016-04/19/c\_135294.. (дата обращения 30.04.2017)

19.     Costello J. The Strategic Support Force: Update and Overview. China Brief, Volume 16, Issue 19. [Электронный ресурс] URL: https://jamestown.org/program/strategic-support-force.. (дата обращения 9.05.2017)

20.     Cyberpower and National Security / edited by Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz. — 1st ed. NDU Press and Potomac Books. Washington, D.C., 2009. P. 642.

21.     Easton I, Stokes M. China’s Electronic Intelligence Satellite Developments: Implications for U.S. Air and Naval Operations (Arlington, VA: Project 2049 Institute, 23 February 2011).

22.     Hsiao R., Lin J., Stokes M. The Chinese People’s Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure. November 11, 2011. P. 5.

23.     Hsiao R., Lin J., Stokes M Opt. cit. p. 5.

24.     Kania E., Costello J. Quantum Leap (Part 1): China’s Advances in Quantum Information Science. China Brief Volume 16, Issue 18. [Электронный ресурс] URL: https://jamestown.org/program/quantum-leap-part-1-chi.. (дата обращения 04.05.2017)

25.     Kania E., Mattis P. Modernizing Military Intelligence: Playing Catchup (Part Two). China Brief, Volume 16, Issue 19. [Электронный ресурс] URL: https://jamestown.org/program/modernizing-military-in.. (дата обращения 05.05.2017)

26.     Lindsay, J. R., Cheung, T. M. (2015). From Exploitation to Innovation. China and cybersecurity: espionage, strategy, and politics in the digital domain. London, Oxford University Press.

27.     Markoff J. Cyberattack on Google Said to Hit Password System // NY Times, April 19, 2010. [Электронный ресурс] URL: http://www.nytimes.com/2010/04/20/technology/20google.. (дата обращения 9.05.2017)

28.     People Daily. Китай обнародовал стратегию международного сотрудничества в киберпространстве. [Электронный ресурс] URL: http://russian.peopledaily.com.cn/n3/2017/0302/c31521.. (дата обращения 29.04.2017)

29.     Segal A. How China is preparing for cyberwar. CS Monitor. [Электронный ресурс] URL: http://www.csmonitor.com/World/Passcode/Passcode-Voic.. (дата обращения 9.05.2017)

30.     The State Council Information Office of the People’s Republic of China. Chinese Net users top 731 million in 2016: report. [Электронный ресурс] URL: http://www.scio.gov.cn/32618/Document/1541204/1541204.. (дата обращения 29.04.2017)

31.     Stokes, M.A. The PLA General Staff Department Third Department Second Bureau / An Organizational Overview of Unit 61398. London, Oxford University Press, 2015.

32.     Sheldon R., McReynolds J. Civil-Military Integration and Cybersecurity. In China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain, edited by Jon R. Lindsay, Tai Ming Cheung, and Derek S. Reveron,. New York: Oxford University Press, 2015. P. 191.

33.     Wood P. Chinese Perceptions of the “Third Offset Strategy”. China Brief, Volume 16, Issue 15. [Электронный ресурс] URL: https://jamestown.org/program/chinese-perceptions-thi.. (дата обращения 9.05.2017)

34.     Xinhuanet. Xi Jinping leads Internet security group. [Электронный ресурс] URL: http://news.xinhuanet.com/english/china/2014-02/27/c\_.. (дата обращения 30.04.2017)

35.     “Xi Jinping Leads Internet Security Group,” Xinhua, February 27, 2014. [Электронный ресурс] URL: http://news.xinhuanet.com/english/china/2014-02/27/c\_… (дата обращения 08.05.2017)

|  |
| --- |
| [Вернуться в библиотеку по экономике и праву: учебники, дипломы, диссертации](http://учебники.информ2000.рф/index.shtml)[Рерайт текстов и уникализация 90 %](http://учебники.информ2000.рф/rerait-diplom.shtml)[Написание по заказу контрольных, дипломов, диссертаций. . .](http://учебники.информ2000.рф/napisat-diplom.shtml) |