**Содержание**

Введение...................................................................................................................3

# 1. Информационная безопасность по-китайски...................................................5

# 2. Китайские спецслужбы.......................................................................................6

# Заключение.............................................................................................................12

# Список литературы................................................................................................13

**Введение**

Власти Китайской Народной Республики огласили в начале недели недавно принятые законы, призванные обеспечить виртуальную безопасность страны. Согласно новому законодательству - "субъект, причастный к шпионажу, краже или разглашению государственных тайн" через Интернет, будет по решению суда приговорен к высшей мере наказания; пожизненному тюремному заключению; десяти годам лишения свободы. Согласно официальному сообщению, имущество осужденного за подобные правонарушения подлежит конфискации. В декабре минувшего года Всекитайское собрание народных представителей (ВСНП) приняло ряд законов, направленных против "преступного использования" Интернета, в первую очередь в антигосударственных целях (см. отчет американского посольства "Кто пользуется Интернетом в Китае"). Затем Постоянный комитет ВСНП составил список "Интернет - преступлений". В него, в частности, вошли: проникновение в государственные сайты, шпионаж в сфере передовых технологий, а также распространение компьютерных вирусов[[1]](#footnote-1).

Таким образом, КНР даже в Интернете следует заветам легизма ("фа-цзя") - политической доктрины Древнего Китая, учившей, что "управление при помощи наказаний приводит к тому, что народ боится и поэтому не совершает мерзостей".

Не стоит забывать, что китайские спецслужбы в настоящее время уделяют самое пристальное внимание технологиями информационной войны. Руководство Народно-освободительной армии Китая (НОАК) официально признало, что по обычным видам вооружения китайская армия не в состоянии достигнуть паритета с США, и в начале 2000 года главный штаб НОАК разработал программу модернизации средств информационной войны. А первым подопытным кроликом для обкатки военными информационных методов ведения войны стал Тайвань, никак не желающий превращаться во второй Гонконг. Тайваньцы забили тревогу еще в декабре, признавшись в том, что с августа 1999 года китайские хакеры взламывали сети госструктур острова до 165 раз. Целями взломщиков были сайты вооруженных сил, министерств юстиции, экономики и Национальной ассамблеи. Добавим, что в то же время нападениям китайских хакеров подверглись японские компьютерные сети.

# 1. Информационная безопасность по-китайски

**Структура армейской разведки в составе Народной освободительной армии Китая[[2]](#footnote-2):**

* Второй департамент - агентурная разведка, координация резидентур;
* Третий департамент - радиоэлектронная разведка.

**Структура министерства государственной безопасности КНР (подчиняется ЦК компартии Китая):**

* Первое бюро - агентурная разведка на территории Китая;
* Второе бюро - зарубежные операции;
* Третье бюро - операции в Гонконге, Макао, Тайване;
* Четвертое бюро - оперативно-техническое обеспечение;
* Пятое бюро - координация региональных отделов МГБ;
* Шестое бюро - контрразведка;
* Седьмое бюро - обработка и анализ поступающих разведданных;
* Восьмое бюро - Институт современных международных отношений;
* Девятое бюро - управление собственной безопасности, координация особых отделов в армии;
* Десятое бюро - сбор научно-технической информации;
* Одиннадцатое бюро - радиоэлектронная разведка и компьютерная безопасность (аналог АНБ США);
* Бюро иностранных дел - официальные контакты с иностранными спецслужбами;
* Синьхуа - информационное агентство.

# 2. Китайские спецслужбы

### 1. Радиоэлектронная разведка

Китайские рыцари плаща и кинжала смотрят в будущее (причем в самое ближайшее) с нескрываемым оптимизмом: силовые структуры страны переживают настоящую революцию. На этот раз техническую. Руководство Народно-освободительной армии Китая (НОАК) официально признало, что по обычным видам вооружения китайская армия не в состоянии достигнуть паритета с США, и в начале 2000 года главный штаб НОАК разработал программу модернизации средств информационной войны. А первым подопытным кроликом для обкатки военными информационных методов ведения войны стал Тайвань, никак не желающий превращаться во второй Гонконг. Тайваньцы забили тревогу еще в декабре, признавшись в том, что с августа 1999 года китайские хакеры взламывали сети госструктур острова аж 165 раз. Целями взломщиков были сайты вооруженных сил, министерств юстиции, экономики и Национальной ассамблеи. Добавим, что в то же время нападениям китайских хакеров подверглись японские компьютерные сети[[3]](#footnote-3).

Разумеется, переход на рельсы информационной войны не мог состояться без разведслужб Китая. И упор был сделан на радиоэлектронную разведку. Так, в мае 1999 года министры обороны Китая и Кубы подписали соглашение о создании на острове Свободы китайского центра радиоперехвата и слежения за американскими спутниками. Кстати, до этого на Кубе существовал только один центр перехвата - в Лурдесе, эксплуатируемый российскими спецслужбами. Не забыт и космос: в 1999 году Китай запустил четыре спутника фотосъемки и два спутника радиоперехвата над Азией, а в марте этого года Цзян Цземинь на заседании центральной военной комиссии отдал приказ о работе над программой "1-26" по созданию новых видов высокотехнологичного оружия, включая разведывательные спутники.

Но, оказывается, еще раньше, в 1994 году Китай арендовал у Бирмы три острова для развертывания на них центров радиoразведки (они "покрывают" Индийский океан, Бенгальский залив и Малаккский пролив). А в 1995 году, по сведениям американцев, модернизации были подвергнуты все китайские центры радиоперехвата в Азии: на одном из Парасельских островов и на острове Хайнань в Южно-Китайском море. Кроме того, был восстановлен центр радиоперехвата Соп-Хау вблизи Лаоса, активно функционировавший в 60-70 гг. во время войны во Вьетнаме[[4]](#footnote-4).

### 2. Планирование

Бывший шеф контрразведки ЦРУ Пол Редмонд как-то заявил по поводу поимки в Америке очередного китайского шпиона: "На культурном уровне они (китайцы) живут совсем в другой среде и в других временных рамках. Китайцы мыслят не в категориях часов, дней или недель, а десятилетий. Они - древняя цивилизация, и умеют планировать на долгие годы". Одним из результатов такого мышления стало, в частности то, что некогда одна из самых отсталых азиатских стран, Китай умудрился заполучить ядерное оружие у СССР, не приняв на себя никаких обязательств. В самые лучшие годы сотрудничества с режимом Мао Цзэдуна нашим военным в Китае не дозволялось совать свой нос на закрытые объекты, а китайская разведка никогда не была "на посылках" у КГБ - в отличие от своих восточноевропейских коллег. Китайским спецслужбам даже удавалось шантажировать США, которым многие годы приходится фактически мириться с кражей секретных военных технологий, чтобы не допускать разрыва отношений. Не секрет, что и космическую ракету китайцы запустили, заставив американцев выдать им ученого-ракетчика китайского происхождения (правда, в обмен на охлаждение отношений с Советским Союзом). Не менее феноменальное достижение китайских спецслужб - установление контроля над многими крупнейшими банками стран из числа "азиатских тигров". Утверждают даже, что наиболее значимые оргпреступные группировки в Юго-Восточной Азии - знаменитые "триады" - находятся "под колпаком" у министерства госбезопасности КНР.

### 3. Контрразведка

Впрочем, возможности китайских спецслужб лучше всего иллюстрируют личные впечатления собеседников корреспондента "Сегодня". Скажем, вряд ли в другой стране возможна ситуация, описанная бывшим сотрудником ГРУ, вышедшим в отставку в середине 90-х: "После отставки мне приходилось бывать в Китае в качестве переводчика. Но свободное общение на китайском языке тут же привлекало ко мне внимание бойцов народной вооруженной милиции (НВМ). Как-то в одном из захолустных городков я собрался пойти в бар. При входе меня встретили два незнакомца, которые очень вежливо спросили, что я собираюсь делать. Я честно ответил, что хочу выпить. Мы вместе поднялись в бар, по знаку одного из провожатых нам освободили столик, и выпивать мне пришлось уже в компании двух спутников. Спустя полчаса к нам подсел еще один китаец, который уже прекрасно говорил по-русски. Они ничуть не скрывали, что служат в НВМ. Первым вопросом было: "А где ты выучил язык?" Я, естественно, ответил: "В Институте стран Азии и Африки". Они дружно рассмеялись: "Это вы все так говорите. Ладно, фамилию твоего преподавателя спрашивать не будем". В общем, мы поняли друг друга"[[5]](#footnote-5).

А вот свидетельство сотрудника внешней разведки, долгие годы прослужившего в резидентуре в Китае: "Во время "культурной революции" китайские спецслужбы возродили древнюю систему доносов, придуманную еще при императорах. Она называется "У Ши Бай" (пятерка, десятка, сотня). Это когда старший пятерки "стучит" на членов своей семьи, старший десятки - на своих сотрудников или соседей и т.д. В результате мы сталкивались с почти полной невозможностью заниматься агентурной работой внутри Китая, так как огромное количество "инициативников" следит за каждым твоим шагом. Причем включая детей, потому что в бригады наружного наблюдения включали подростков. Намного проще было вербовать агентов где-нибудь за пределами Китая - например, студентов в СССР".

### 4. Участие в экономике

В середине 80-х, когда Дэн Сяопин выбирал стратегию китайских реформ, в недрах МГБ была разработана глобальная программа добывания финансовых ресурсов и передовых технологий. Эта программа так понравилась китайскому лидеру, что тот принял стратегическое решение о приоритетном финансировании и укреплении МГБ как инструмента обеспечения радикальных реформ в КНР. Последствия того решения ощущаются и теперь[[6]](#footnote-6).

К примеру, ныне многие полагают, что избранный в конце 1996 года главой администрации Гонконга владелец судоходной фирмы "Ориент оверсиз интернейшнл" Тун Чжихуа - сотрудник МГБ. По некоторым данным, под "крышей" этой крупнейшей компании (личное состояние Туна Чжихуа оценивается в сумму свыше миллиарда долларов) китайская разведка успешно действует с конца 70-х годов. Именно тогда она "спасла" уроженца Шанхая Туна от банкротства, посодействовав в получении льготного кредита в 120 млн долларов. В результате МГБ удалось избежать эксцессов при присоединении Гонконга к материковому Китаю.

Или такая любопытная фигура, как гонконгский бизнесмен Ли Ка Шин. Сегодня многие отчеты ЦРУ посвящены его деятельности. Впервые Ли Ка Шин напугал американцев в 1998 году, когда стало известно, что он намерен ни больше ни меньше как получить контроль над Панамским каналом. В 1996 году его компания Hutchison Whampoa, ныне зовущаяся Panama Ports Co., получила в аренду на 50 лет от панамского правительства ключевые порты на канале как со стороны Атлантического, так и Тихого океанов. Госдеп США тут же объявил это соглашение "незаконным" и "полностью коррумпированным". В январе этого года появился отчет Пентагона, где Ли Ка Шин обвиняется в том, что собирался использовать Панамский канал "для контрабанды технологий с Запада в Китай или для облегчения доставки вооружений на территорию США". Доподлинно неизвестно, почему Ли Ка Шин работает на китайскую разведку - сыграли ли роль личные отношения бизнесмена с руководителями Китая, как утверждают одни газеты, или это взаимовыгодное сотрудничество. Однако вот примечательный факт. В марте 2000 года сын Ли Ка Шина Ричард Ли провел сделку по приобретению гонконгского телефонного оператора Cable&Wireless HKT за 38 млрд долларов. А ведь без позволения властей Китая такая сделка не состоялась бы. По оценкам американцев, в настоящее время Ли Ка Шин и его сын контролируют примерно одну треть всех акций, котирующихся на фондовом рынке Гонконга. Однако вполне возможно, что тесное сотрудничество Ли Ка Шина с властями Китая объясняется тем, что он, также как и Тун Чжихуа, в долгу перед спецслужбами КНР. Дело в том, что в 1996-97 годах бандой Большого транжира в Гонконге были похищены два крупных бизнесмена. Одним из них был Виктор Ли, второй сын Ли Ка Шина. Требуемый выкуп в 205 млн долл. был выплачен, а за бандой "Большого транжиры", который скрылся в Китае, началась национальная охота. Наконец в январе 1998 года в городе Гуанчжоу на юге Китая была арестована вся группировка из 35 человек во главе с самим Большим транжиром, 43-летним жителем Гонконга Чеунгмо Тзе Кеунгом. Вряд ли когда-нибудь Ли Ка Шин забудет о столь любезной услуге китайских спецслужб[[7]](#footnote-7).

### 5. Агентурная разведка

Известно, что последние двадцать лет ведущие разведки мира все больше внимания уделяют высоким технологиям. Ведь выбить из бюджета деньги на очередную серию спутников-шпионов, понастроить станций радиоперехвата гораздо проще, чем вести скрупулезную и небезопасную агентурную работу. По крайней мере, риск международных скандалов при аресте агента резко снижается. Однако у Китая и здесь свой собственный путь: он продолжает делать ставку на агентурную работу. Вот свидетельство сотрудника ФАПСИ, в начале 90-х несколько лет прослужившего на станции радиоперехвата на китайской границе вблизи Благовещенска: "Китайские зашифрованные сообщения мы часто "ломали вручную", такой у них был невысокий уровень. В то время как даже Индия уже использовала электронные шифраторы, китайцы обходились самыми простыми шифрами. Конечно, некоторые объекты "не читались", например, база на озере Лобнор, где китайцы проводят ядерные испытания. Но таких объектов было раз-два и обчелся". И китайцев это вполне устраивало. Все средства вкладывались в агентурную работу, но это не было простым упрямством.

Перенаселенный Китай сегодня является главным поставщиком эмигрантов. К настоящему времени численность китайской диаспоры в Америке превышает 1,3 миллиона человек, в России на Дальнем Востоке и в Сибири за последние пять лет численность китайцев превысила один миллион человек, китайцы активно проникают в Европу - наиболее сильные диаспоры сформированы в Румынии и Венгрии. Именно эта стратегия - работа с агентурой внутри диаспор по всему миру - и принесла китайской разведке лавры третьей по силе в мире[[8]](#footnote-8).

И все же то, что теперь китайцы решили догнать разведки других стран по техническому уровню, не может не насторожить США и Россию. Впрочем, Россия, похоже, вновь налаживает отношения с Китаем в военной сфере - недавно состоялись контакты на уровне руководителей военных ведомств двух стран.

**Заключение**

Сфера обеспечения информационной безопасности в Китае намного отстает от стремительно развивающейся отрасли информатики, что представляет серьезную угрозу для создания в Китае информационного общества. Такое предупреждение сделал академик Инженерной академии Китая Хэ Дэцюань[[9]](#footnote-9).

Принимая участие в форуме по вопросам информатизации страны, проходящем в г. Ханчжоу, Хэ Дэцюань отметил, что в настоящее время производство программного обеспечения информационной безопасности составляет всего 2 - 3 процента от общей продукции отрасли информатики. При этом, отсутствует продукция, произведенная с применением высоких информационных технологий.

Согласно статистике, с 2000 года около 59 процентов компьютеров в Китае более трех раз подвергались атаке вирусов. В октябре 2001 года 88 процентов владельцев Интернет - сайтов признали, что за последний год они пострадали от компьютерных вирусов, несмотря на то, что 90 процентов из них пользовались стандартными защитными программами.

Как стало известно, мировое производство программного обеспечения информационной безопасности оценивается в 23,2 млрд. долларов, в том числе на США, ЕС и страны Азии проходится 12,7 млрд., 5,8 млрд. и 4,6 млрд. долларов соответственно. Однако данный показатель в Китае в 2001 году составил лишь 1,9 млрд. юаней (примерно 230 млн. долларов).

Хэ Дэцюань уверен, что наращивание мощностей производства программного обеспечения информационной безопасности не только укрепит позиции Китая в этой области, но и стимулирует развитие отрасли информатики в целом.

# Список литературы

* 1. Аверкиев С.Д. Современные проблемы развития информационной безопасности. – М, 2005. – 132 с.
  2. Буланов М.И. Экономика Азии. – С-Пб, 2005. – 76 с.
  3. Глушкова Г.В., Семагин Ю.А. Тесты и задания по экономической и социальной географии мира. – М.: Владос, 2004. – 103 с.
  4. Демографический справочник-ежегодник// под ред. Васильева В.И. – М.: Геолайн, 2006. – 329 с.
  5. Кезлинг А.Б., Филатов В.И. Страны мира и международные организации: Справочник. – М.: УНИИНТЕХ, 2007. – 282 с.
  6. КНР. Экономические связи в 2007 году: Ежегодный справочник. – М, 2008. – 190 с.
  7. Ломакин В. К. Мировая экономика: Учебник для вузов. – М.: Финансы, ЮНИТИ, 2005. – 727 с.
  8. Лунев А.А. КНР в свете политических событий. – С-ПБ, 2007. – 113 с.
  9. www.security-data.ru
  10. www.fondiv.ru

1. www.security-data.ru   [↑](#footnote-ref-1)
2. www.security-data.ru   [↑](#footnote-ref-2)
3. Аверкиев С.Д. Современные проблемы развития информационной безопасности. – М, 2005. – 132 с. [↑](#footnote-ref-3)
4. Лунев А.А. КНР в свете политических событий. – С-ПБ, 2007. – 113 с. [↑](#footnote-ref-4)
5. www.fondiv.ru [↑](#footnote-ref-5)
6. КНР. Экономические связи в 2007 году: Ежегодный справочник. – М, 2008. – 190 с. [↑](#footnote-ref-6)
7. Лунев А.А. КНР в свете политических событий. – С-ПБ, 2007. – 113 с. [↑](#footnote-ref-7)
8. Аверкиев С.Д. Современные проблемы развития информационной безопасности. – М, 2005. – 132 с. [↑](#footnote-ref-8)
9. www.fondiv.ru [↑](#footnote-ref-9)