Илья ТИТОВ

ТАЛИБ ПОДКРАЛСЯ НЕЗАМЕТНО

Выводить войска из Афганистана — плохая примета

Год 1919-й. Самая могущественная военная империя мира покидает Афганистан, наполняясь стыдом, который предвещает её будущий крах.

Год 1989-й. Самая могущественная военная империя мира покидает Афганистан, наполняясь печалью, которая предвещает её будущий крах.

Год 2021-й…

ПОПЫТКИ СФОРМУЛИРОВАТЬ книгу правил, по которым должна вестись глобальная политика в XXI веке, заведомо обречены на полный провал — в наше время убогое недогосударство, существующее за счёт базы НАТО и завода шпрот, буднично наносит страшное оскорбление первой по величине экономике мира, а последняя сверхдержава показательно и безуспешно бодается с какой-то трубой в Балтике, что-то лепеча про молекулы свободы. Мир полон абсурда, хаоса и неопределённости. Именно поэтому так велик соблазн отыскать в броуновском движении фракций, экспансии стран и переселениях народов знакомые паттерны, объяснить необъяснимое с помощью уже виденного, попытаться предугадать исход действа, развязка которого не ясна даже его постановщикам. Так произошло с уходом США из Афганистана и переходом многострадальной страны под власть талибов*. Случилось это так стремительно и резко, что языки матёрых корифеев международной политической публицистики в мгновение ока пересохли, а их трепещущие глотки не смогли выдать ничего, кроме пустых сравнений с былым.

Всё случилось почти мгновенно. Поток новостей захлестнул читателей оперативных сводок так же резко и порывисто, как волны "Движения Талибан" захлёстывали Афганистан. В начале августа многомудрые эксперты рассуждали о том, что падение Кабула неизбежно и, по сути, представляет собой вопрос пары-тройки месяцев, но Кабул пал досрочно, к середине августа. Не было ни эпической битвы Добра со Злом за последний бастион свободы и демократии — те, кто мог сопротивляться, давно перешли на сторону будущей власти; ни кровавых расправ в столице: талибы пообещали особо не злодействовать и вроде бы даже выполнили обещание. Быстро, слаженно, чётко — ещё утром они были на подступах к городу, днём вешали свои флаги в его спальных районах, а вечером уже разгуливали по президентскому дворцу, откуда в Таджикистан бежал бывший президент Гани. Следующим утром (по Москве) талибы торжественно заявили о своей победе, что сопровождалось вбросом в инфополе триумфальных видео с визитами в дома сбежавших чиновников павшего режима — стандартная, в общем-то, процедура при насильственном захвате власти в наше время.

Спросите у любого эксперта, и он скажет вам, что для всех скорое падение афганского правительства было очевидно ещё весной, а для него, эксперта, — вообще примерно лет двадцать назад. Основной задачей коалиции под руководством США (не только США, это важно) стало недопущение превращения отступления в бегство. Нужно было создать иллюзию, что всё идёт по плану, — цели достигнуты, задачи выполнены, а уж разборки местных ничуть не касаются Дяди Сэма и его подпевал. Для этого даже назначили дату торжественного вывода войск — 11 сентября. С задачей создания такой видимости западная агитационная промышленность блестяще не справилась. Отчасти тому способствовала уверенность в том, что на эвакуацию из Кабула есть ещё месяц-два, отчасти — бешеная скорость продвижения талибов, а отчасти — хроническая неспособность признавать собственные ошибки. Ещё 8 июля, когда исход был ясен, президент Байден пытался сохранить лицо. На пресс-конференции он ответил на вопрос о сравнении "Талибана" и Вьетконга, заявив, что первые "далеко не так могущественны", как вторые, и что повторения кадров эвакуации с крыши американского посольства можно не ждать. Правительство, говорил Джо, ещё может переломить ситуацию, а посольство никто не будет штурмовать. 15-е августа доказало, что Джо ошибся. В облаках чёрного дыма от горящих секретных документов на крышу кусочка Америки, спроектированного, кажется, специально для таких задач, садится грузовой вертолёт. Посольство, к слову, никто не штурмовал ни в Кабуле, ни в Сайгоне — если не считать толп вьетнамских коллаборантов, которых Штаты обещали эвакуировать, но обманули, а потом их расстреляли из винтовок американские морпехи. Госсекретарь Блинкен в начале августа говорил, что не всё решено, что правительственные войска могут дать достойный отпор, — 15 августа он заявил, что слабость афганской правительственной армии стала причиной триумфа талибов. Борис Джонсон объявил, что Британия "завершает свою двадцатилетнюю миссию в Афганистане", — формально, конечно, не соврал, но широта возможных трактовок слов премьера поражает. Министр иностранных дел Германии пригрозил, что талибы могут не рассчитывать на 400 с лишним миллионов евро помощи от Германии, которая ежегодно шла прозападному правительству. "Какая жалость", — сказали талибы и пошли растить мак. Спикер американской Палаты представителей Пелоси потребовала участия женщин в переговорном процессе. Что она имела в виду — бог весть, но талибы, вероятно, посмеялись.

Бегство из Афганистана стало последним прощальным приветом эпохи решения военных конфликтов силовым путём. Несмотря на заверения британского министра обороны в том, что Британия вернётся в Афганистан, посмей тот приютить у себя террористов, кажется, что западные солдаты покинули страну навсегда. Отныне этот островок средневековья станет ареной столкновения НКО, фондов, пропагандистских структур, военных и разведывательных ведомств. И все имеют свой интерес: американцы грезят упущенной прибылью от торговли оружием и наркотиками, турки пускают слюни и носятся со своим Великим Тураном, Иран не хочет лишней головной боли, Китаю позарез нужен настроенный против Индии центр Средней Азии и транзитный пункт на их Шёлковом пути, а России нужно обеспечивать безопасность своего мягкого подбрюшья, что довольно проблематично сделать, когда так близко к нашим границам власть взяла всё ещё считающаяся террористической мощная группировка. Талибы уже дали понять, что любые попытки вмешательства извне будут пресекаться, в частности, обещали перебить турецких солдат в случае, если те к концу августа всё ещё будут оставаться в их стране. Видимо, не всё гладко с Эрдоганом, как это выставляют турецкие СМИ. К слову, в западной пропаганде то там, то сям всё чаще встречается тезис о большой вине России в развязывании афганского кризиса. В этом непонятном лепете явственно одно: чтоб искупить страшную провинность нужно принять беженцев из Афганистана, желательно всех. О необходимости наводнить Россию ещё бóльшим количеством демографического оружия из Средней Азии и с Ближнего Востока уже много лет говорят видные чиновники на всех уровнях американских, европейских и натовских структур, так что в этом никакой новости нет. Важно то, что из исторического события, из доселе невиданного захвата Кабула, из миллионов ярких аспектов, которые, играя отражениями, делают исход этой войны чем-то удивительным и уникальным, каждый влиятельный игрок привычно гнёт свою линию. А как всё начиналось… В 2001-м президент Буш-младший, самый могущественный человек мира, хозяин империи эпохи конца истории, вечного гегемона и неоспоримого авторитета, сказал:

"Талибану" пришёл конец".

* Талибы, "Талибан", "Движение Талибан" — организация, признанная террористической по решению Верховного суда РФ от 14.02.2003 г.

Найди 10 отличий: вехний снимок — 1975 год, американский военный вертолёт садится на крышу посольства США в столице Южного Вьетнама Сайгоне для срочной эвакуации сотрудников посольства, нижний снимок — 2021 год, американский военный вертолёт садится на крышу посольства США в столице Афганистана Кабуле для спешной эвакуации сотрудников посольства

Валерий ВОРОБЬЁВ

ГИБЕЛЬ СТРАЖЕЙ

США: начало самоликвидации

ОСНОВОПОЛАГАЮЩИЙ момент становления байденовской Америки — 6 января, день беспорядков в Вашингтоне. В государстве, считающем себя эталоном демократии, источником легитимности власти стали не выборы, а выражение недовольства, вызванного мутностью и явной нечестностью этих выборов. Беспорядки в американской столице, проход в Капитолий, позирования и кривляния, довольно безвредные (если сравнить с бунтами BLM прошлым летом) выходки — всё это силами государственного аппарата и машины СМИ было превращено в страшную угрозу американской государственности. Участники выступления были объявлены "внутренними террористами" и "мятежниками", посажены по тюрьмам, уволены с работы, вытравлены из интернета и подвергнуты остракизму. Истерика массмедиа раздула немногочисленный прорыв в пустое здание американского парламента до масштабов революции, где десятки тысяч вооружённых до зубов трампистов штурмовали последнюю цитадель демократии, не желая признавать честнейшие выборы в истории. Это мгновенно вытравило из дискурса вопросы о выборах, что дало Байдену легитимность и законность диктатора, пришедшего в самый опасный момент и не размениващегося на формальности. Капитолий ещё долго стоял в окружении высокого забора, заполненный нацгвардией. Любое происшествие неподалёку от центра Вашингтона (а их хватало, ведь в американской столице очень высокий уровень криминала) где-то до середины весны трактовалось как подготовка второго акта неудавшейся революции. Любой критик демократического Сената, Палаты представителей или Белого дома тут же объявлялся трамповским недобитком, что вызывало острую реакцию со стороны прессы. При этом поражает вялая реакция журналистов на самоубийства вашингтонских полицейских, присутствовавших при важнейшем событии всей эпохи Байдена. Офицеры Джеффри Смит и Говард Либенгуд с разницей в два дня покончили с собой вскоре после инцидента на Капитолийском холме.

А сейчас с интервалом в пять дней совершили суицид офицеры Гюнтер Хашида и Кайл ДеФрейтаг. Среди них не было неоперившихся новичков, так что столкновение с жестокой реальностью на улицах этого наполненного неграми города едва ли могло стать причиной добровольного ухода из жизни. В СМИ лишь сухие факты — никакого анализа, никаких предположений, просто краткая биография, пара предложений об участии в подавлении "восстания" и скупая информация о самоубийстве. И только газета The New York Times выпустила в конце июля более-менее подробный материал о Джеффри Смите, умершем ещё в январе. Причиной самоубийства называлась травма головы, полученная в ходе событий в Капитолии — она-де стала причиной депрессии, которая вконец довела опытного офицера. Виновниками гибели Смита без сомнений были сторонники Трампа — говорит NYT, ссылаясь на безутешную вдову. По сути, бессовестно-манипулятивный материал ньюйоркцев стал единственным анализом странной закономерности — по поводу копов-самоубийц молчат даже конспирологи, хотя событие открывает им широкий простор для фантазии. Ни разговоров про то, что такого могли увидеть и рассказать офицеры, ни рассуждений о сходстве этих самоубийств с другими — ничего. Зачистка медиапространства в 2021 году оставила на месте некогда громких праворадикальных медиа выжженную пустыню, где немногие выжившие боятся лишний раз вызвать по отношению к себе злобу и ненависть истеблишмента. Американское государство успешно уничтожает своих внутренних врагов, через борьбу с выдуманной угрозой зачищая дискурс от крамолы и сомнений в правоте линии партии. На полулегальное положение вот-вот скатится даже карманная оппозиция Белого дома. Популярного телеведущего Fox News Такера Карлсона часто называют самым громким голосом консервативной Америки, хотя его взгляды весьма умеренны, а сам он плоть от плоти вашингтонская элита. Эти факторы, однако, никак не помогли ему избежать слежки со стороны АНБ, информация о которой была обнародована. Оказалось, что Агентство получило доступ к переписке влиятельного телеведущего (недавно, кстати, бравшего интервью у венгерского премьера Орбана), после чего анализировало её и сливало самые вкусные куски верным медиапсам режима. Только вдумайтесь: могущественная спецслужба работает в тандеме с конгломератом СМИ, давя на телеведущего с дурацкой причёской. Дело не в самом Карлсоне: его лояльность режиму не вызывает сомнений, несмотря на антидемократическую риторику — просто в условиях полного отсутствия у околоконсервативных сил интересного и харизматичного транслятора идей Такер стал единственным рупором (пусть и довольно сильно искажающим реальные идеи) стремительно вымирающей белой Америки.

Вымирание американских белых ещё недавно считалось мифом и опасным заблуждением праворадикальных конспирологов. Газеты картинно посмеивались над рассказами про демографический перелом и тревогами о печальном будущем белого населения. Лишь несколько лет назад в крупных СМИ стали появляться подтверждения того, что доля цветного населения в США действительно растёт (хотя это видели все). Американские статистики опубликовали результаты прошлогодней переписи населения. Оказалось, что цветных не просто становится больше — белых становится меньше. За десять лет страна где-то потеряла аж 5 миллионов европеоидов, так что там их теперь меньше 58%. Нет ни единой причины предполагать, что хоть кто-то из участников процесса заинтересован в остановке и повороте вспять этой опасной тенденции. Белые накачаны пропагандой, озабочены карьерой и загнаны в глушь, им не до размножения. Цветное население преисполнено выращенной ненависти, взбешено десятилетиями социальной напряжённости и жаждет обрести лёгкий способ избавления от всех бед. Власти же проводят последовательную политику по превращению Соединённых Штатов в страну белого меньшинства. Когда потомки строителей этой страны добровольно сделаются меньшинством, с ними никто не станет церемониться. Не будет ни квот в оскароносных фильмах, ни упрощённой процедуры поступления в вузы, ни постоянных восхвалений через все медиаканалы.

Константин БАТАНОВ

ХАКЕРЫ БЫВАЮТ РАЗНЫЕ

…чёрные, белые, красные

"Китайские хакеры взломали сервер Пентагона. Каждый из них попробовал один пароль. Каждый второй пароль был "Мао Цзэдун". На 74357181-й попытке сервер согласился, что у него пароль "Мао Цзэдун"

Анекдот

СОЕДИНЁННЫЕ ШТАТЫ и присоединившиеся к ним Европейский Союз, НАТО, Великобритания, Канада, Австралия, Новая Зеландия и Япония сообща отреагировали на взлом программы для обмена сообщениями Microsoft Exchange Server, которой активно пользуются американские ведомства, учреждения и предприятия. В блоге Microsoft сообщается: "В ходе атак злоумышленники использовали уязвимости, чтобы получить доступ к учётным записям электронной почты и установить вредоносные программы для получения постоянного доступа к среде. Microsoft Threat Intelligence Center (MSTIC) с высокой степенью уверенности считает, что атаки проводятся группой HAFNIUM, деятельность которой финансируется правительством Китая".

Взлом был обнаружен в марте. Совместное осуждение его западными странами прозвучало 19 июля. Отмечается, что он затронул по меньшей мере 30 тыс. американских организаций.

Госсекретарь США Блинкен обвинил Китай в создании "экосистемы хакеров-контрактников, которые осуществляют как спонсируемую государством деятельность, так и киберпреступления для собственной финансовой выгоды" и заявил, что это является частью "модели безответственного, разрушительного и дестабилизирующего поведения в киберпространстве, представляющего серьёзную угрозу нашей экономической и национальной безопасности".

Представители НАТО призвали Китай "выполнять свои международные обязательства… в том числе в киберпространстве".

По мнению американских экспертов, целью хакеров являются получение информации о корпорациях, правоохранительных органах, политических деятелях, правительственных чиновниках, политических активистах и диссидентских группировках, представляющих интерес для правительства Китая. Хакеры также могут наносить непосредственный ущерб, например, отключать или нарушать работу сетей.

Американцы отметили, что китайские хакеры были "сложно обнаруживаемыми и адаптивными", то есть успешно уклонялись от предпринимаемых американскими специалистами ответных действий. Было замечено, что одна из групп скрывала своё вредоносное программное обеспечение в папках корзин для удалённых файлов. Другая группа маскировала шпионские программы под антивирусное программное обеспечение и южнокорейский мультимедийный плеер под названием "PotPlayer".

"Китайское правительство должно положить конец этому систематическому кибер-саботажу и может рассчитывать на привлечение к ответственности, если оно этого не сделает", — говорится в заявлении министра иностранных дел Великобритании Доминика Рааба.

В ответ представитель Министерства иностранных дел Китая Чжао Лицзянь ответил, что обвинения в причастности Китая к атакам являются "сфабрикованными" и представляют собой "клевету". Представитель также обвинил ЦРУ в проведении кибератак на объекты аэрокосмических исследований Китая, нефтяную промышленность, интернет-компании и правительственные учреждения. "Китай в очередной раз решительно требует, чтобы Соединённые Штаты и их союзники прекратили кибератаки против Китая и перестали поливать Китай грязью в вопросах кибербезопасности".

Согласно отчёту китайского Национального центра по чрезвычайным ситуациям в Интернете, американские хакеры обычно используют широкий спектр методов атаки для сканирования сетевых и системных уязвимостей с применением высокочастотных средств взлома. В 2020 году около 52 тыс. иностранных серверов управления компьютерными вредоносными программами атаковали около 5,31 млн компьютеров в Китае.

Были определены три группы американских хакеров, действующие наиболее дерзко и масштабно.

Первая группа была обнаружена в октябре 2020 года. Она использовала 1065 компьютеров, расположенных в Соединённых Штатах, и атаковала 2426 компьютеров в Китае. Её целями были партийные и правительственные органы, предприятия автомобильной и металлургической промышленности.

Вторая группа также была выявлена в октябре 2020 года — с помощью 24 компьютеров она атаковала 993 компьютера, находящихся в университетах провинций Шаньси, Гуанси и Гуандун.

Третья группа попала в поле зрения китайцев ещё в августе 2020 года — она использовала 5 компьютеров для атаки на 119 компьютеров в университетах Пекина и провинции Гуандун.

Надо сказать, что тут очевидны попытки промышленного и научного шпионажа со стороны американских хакеров. Обычно в этом обвиняют китайцев, но здесь мы видим обратный процесс. Дело в том, что во многих китайских вузах действуют серьёзные научно-исследовательские центры, результаты работы которых находят применение в промышленном производстве.

В этой связи в Китае всё чаще звучат призывы создать кибервойска, которые должны защищать интересы Китая от посягательств иностранных интернет-врагов. Естественно, что кибер-воины, несущие эту почётную обязанность, сами по сути являются хакерами.

Первое компьютерное преступление в Китае произошло 16 июня 1998 года. Сотрудники одной шанхайской информационной сети во время плановой проверки обнаружили, что их сеть подверглась атаке незваных гостей. 13 июля того же года подозреваемый был арестован. Выяснилось, что преступник последовательно взломал 8 серверов сети, расшифровав учётные записи и пароли не только сотрудников, но и более 500 внешних пользователей. Этот первый китайский хакер был арестован по обвинению в "уничтожении компьютерных информационных систем".

Китайские хакеры делятся на три вида в зависимости от своих целей и методов заработка.

САМО СЛОВО "ХАКЕР" звучит на китайском как "хэйкэ" и записывается двумя иероглифами — "чёрный" и "гость". Первый вид — это обычные хакеры в классическом понимании этого слова, то есть те, кто совершают противозаконные действия с целью наживы. Они похищают данные для дальнейшей перепродажи, разрабатывают вирусы для шантажа пользователей (требуют перевести им деньги, иначе угрожают стереть важную информацию на компьютере), наносят вред физическим лицам и предприятиям.

Таких "чёрных" хакеров становится меньше по нескольким причинам. Во-первых, в Китае ужесточается законодательство в сфере борьбы с киберпреступностью — в зависимости от суммы ущерба хакера может ожидать наказание в виде тюремного заключения от трёх лет до пожизненного, с конфискацией имущества. Во-вторых, в Китае действует интернет-полиция, она отслеживает действия пользователей, поэтому всё тайное в китайском сегменте Интернета при необходимости может довольно легко стать явным, то есть злоумышленника могут быстро вычислить и арестовать. В-третьих, доходы "чёрных" нестабильны. Иногда им удаётся "увести" крупную сумму денег, но чаще случаются длительные периоды простоя, или им приходится довольствоваться небольшими "заработанными" суммами.

ВТОРОЙ ВИД ХАКЕРОВ — "хункэ", "красный гость". Это хакеры-патриоты, которые нападают на сети и компьютеры недружественных Китаю стран. Кроме того, они отражают хакерские атаки иностранцев на китайские сети, то есть защищают государственные интересы, поэтому являются "хорошими" хакерами и выглядят в глазах китайских обывателей национальными героями. У них есть своя идеология, которая выражается в лозунгах: "Охраняйте единство Родины и защищайте национальный суверенитет", "Боритесь со всеми враждебными нашей стране элементами".

7 мая 1999 года во время войны НАТО против Сербии пятью высокоточными бомбами было уничтожено посольство Китая в Белграде. В результате погибли три журналиста из агентства "Синьхуа" и газеты "Жэньминь жибао", также были ранены 10 человек. Представители НАТО утверждали, что это было сделано не специально, а в результате ошибки. США выплатили компенсации семьям погибших. Однако это событие всё равно вызвало волну справедливого негодования китайцев, что выразилось в демонстрациях, массовых пикетах у посольства и генконсульств США, других стран НАТО в Китае.

Китайские хакеры не могли оставаться в стороне. За одну ночь был создан "Центр экстренной конференции китайских хакеров", что стало началом движения "хункэ". Собравшиеся выразили "готовность сражаться и осмелиться стащить американского императора с лошади". Через несколько дней они взломали сайт американского Белого дома и "вывесили" на нём флаг КНР. Такая же судьба постигла ещё несколько сайтов правительственных и военных ведомств США. На сайте одного из подразделений американских ВВС они разместили рукописное письмо отца одной из жертв бомбардировки Посольства.

В Китае говорят: "новорождённые телята не боятся тигров". "Хункэ" в основном представляют собой молодых людей в возрасте от 15 до 30 лет, которые не боятся крушить авторитеты и готовы бросить вызов любым иностранным специалистам по компьютерной безопасности.

С тех пор "красные хакеры" регулярно напоминают о себе. Например, в 2011 году они успешно вторглись в сетевую систему Аль-Каиды*, уничтожили там многие данные и нанесли этой одиозной организации чувствительное киберпоражение.

В 2013 году японские хакеры атаковали китайские интернет-предприятия, причинив им серьёзный ущерб. Это ранило национальные чувства китайцев, так как вызвало ассоциации с нападением Японии на Китай во время Второй мировой войны, в результате чего японцами было убито около 40 млн китайцев. В ответ на японские кибератаки "хункэ" скоординировались и за полчаса взломали 70% японских сетей. Японцам потребовалась неделя, чтобы их восстановить, всё это время китайский пятизвёздный красный флаг висел на сайтах самых известных СМИ Японии.

В разное время "хункэ" отмечались на сайтах правительственных учреждений западных стран, Индии, Австралии (то есть тех, кто, по их мнению, проводит враждебную по отношению к Китаю политику), а также на сайтах политической оппозиции в странах, имеющих хорошие отношения с Китаем. Например, однажды их жертвой стала одна из политических партий Камбоджи, которую они заподозрили в прозападных настроениях.

ТРЕТИЙ ВИД ХАКЕРОВ — "баймао", "белошапочники". Они занимаются тем, что ищут уязвимости китайского ПО и компьютер-ных сетей. Это происходит двумя путями.

Первый путь — они взламывают чью-то сеть или сайт, оставляют небольшой след (например, могут заменить одно слово или цифру), при этом не наносят никакого ущерба. После этого хакеры вступают в контакт с владельцами и сообщают им, что они обнаружили слабые места в их продукте и готовы помочь их исправить в обмен на денежное вознаграждение. Очевидно, что здесь "белошапочники" ходят по грани, потому что сначала взламывают сайты и сети, как обычные хакеры, то есть хозяева этих сетей имеют достаточно оснований, чтобы заявить на них в полицию.

Второй путь — разработчики нанимают их сами. Как вариант, между ними устраивается соревнование по взлому, и победителю полагается приз. В Китае существует специальная платформа под названием "Бутянь", на которую выгружаются программные продукты, где "баймао" их тестируют и пытаются найти слабые места. Пользователи (то есть "белошапочники") должны там зарегистрироваться и заполнить анкету, чтобы получить доступ к тестируемым продуктам. Поэтому данная часть хакерского сообщества является относительно прозрачной. Более того, они сами в этом заинтересованы, чтобы их могли найти клиенты.

В настоящее время на платформе зарегистрировано 11 770 "баймао". Самому младшему из них 12 лет, а самому пожилому — 78. 68% из них — люди, родившиеся после 1990 года. 23% из них живут в провинциях Хэнань (одна из самых густонаселённых в Китае), Шаньдун и Гуандун (развитые приморские провинции). Почти 5% "баймао" — женщины и девушки.

В плане доходов между членами сообщества существует большой разрыв. Средний доход, который они получают, — 7 тыс. юаней (около 80 тыс. руб.) в месяц. Но есть те, кто получает совсем немного, а есть чемпионы, которые получают почти полмиллиона юаней в месяц. Также есть те, кто имеет неофициальные доходы. Например, некоторые занимаются "крышеванием" сайтов и сетей — за скромную сумму в 20 тыс. юаней (стандартный общепринятый тариф, примерно 227 тыс. руб.) в месяц обещают не атаковать и защищать сайт от нападений других хакеров.

"Баймао" тратят в среднем около двух часов в день на свою деятельность, часто рассматривая её как хобби или подработку. 36,3% "белошапочников" работают в компаниях, предоставляющих услуги по компьютерной безопасности, 34,9% являются студентами, а 7,1% — госслужащие.

55,8% из них не имеют дипломов или сертификатов о профессиональных навыках. Это объясняется тем, что часть из них — "самоучки", а часть — студенты, ещё не окончившие учебное заведение.

При этом, в силу особенностей культуры и менталитета, китайские власти стремятся к систематизации и упорядочению "хакерских ресурсов". Недавно Министерство промышленности и информационных технологий КНР, Управление сетевой информации Китая и Министерство общественной безопасности КНР совместно издали "Положение об управлении уязвимостями безопасности в сетевых продуктах" с целью стандартизировать поведение при обнаружении уязвимостей и предоставлении отчётов, а также с целью уточнения обязанностей организаций и лиц, занимающихся обнаружением уязвимостей.

В настоящее время разрабатывается система сертификации "баймао", в соответствии с их квалификацией. После прохождения испытаний (и в случае необходимости соответствующего обучения) специалистов делят на три категории — базовую, продвинутую и высокую — состоящие из 14 разрядов. Специалист каждого разряда должен обладать определённым набором навыков. Общее число таких навыков — 85.

Желающие могут пройти обучение в школах компьютерной безопасности. Их также называют хакерскими школами, так как очевидно, что для того, чтобы уметь эффективно что-то защищать, надо также уметь на это что-то не менее эффективно нападать. В школах могут обучаться все желающие, оплата за обучение относительно невелика. Если верить китайским сайтам по подбору персонала, доходы специалистов по сетевой безопасности значительно превышают зарплату специалистов по разработке программного обеспечения. Поэтому такие школы пользуются большим успехом. Они ставят своей задачей научить слушателей всесторонне использовать различные технические и нетехнические средства для проведения динамической реальной боевой атаки и защиты в реальной бизнес-системе. На занятиях проводятся настоящие "военные" учения.

11 августа в Пекинском национальном конференц-центре прошла Конференция "белошапочников". Такие конференции может посетить любой желающий. Рассматриваемые темы: веб-безопасность, безопасность мобильных устройств, системная безопасность, безопасность Интернета вещей, безопасность промышленного контроля, технология выявления бинарных уязвимостей, технология обратного программного обеспечения, защита критически важной информационной инфраструктуры и тенденции развития технологий безопасности.

Исходя из вышеизложенного можно сделать несколько выводов.

С учётом роста цифровизации современного общества хакерская деятельность и противодействие ей навсегда войдут в актуальную повестку современной жизни. Этому будет способствовать своего рода "демократизация" хакерства. Дело в том, что инструменты хакерских атак становятся всё дешевле. При этом эффективность новых "дешёвых" инструментов растёт, а время, необходимое для проведения атаки, сокращается. То есть себестоимость хакерской "работы" снижается, а средства становятся доступными всё более широким слоям населения. Это означает, что ряды хакеров будут пополняться. Китайское руководство стремится вывести их из тени и создать условия для того, чтобы они приносили пользу обществу и государству. Российским учреждениям, курирующим вопросы информационной безопасности, имеет смысл установить отношения сотрудничества со своими китайскими коллегами, чтобы обмениваться опытом и трезво оценивать возможности китайских хакеров, для того чтобы в случае необходимости уметь им противостоять (вспомним китайскую пословицу: "В мире нет вечных друзей и нет вечных врагов"), а также для того, чтобы совместно бороться с хакерами из стран НАТО.

* Аль-Каида — запрещённая в РФ террористическая организация