ПЕРВАЯ МЕЖДУНАРОДНАЯ КОНФЕРЕНЦИЯ

«РУСКРИПТО – 99»
22-24 декабря 1999 г. Моск.обл. «Непецино»

Т.А.Соболева

К вопросу об изучении истории криптографической службы России.

В секретных инструкциях государственных органов России всегда подчеркивалось, что все документы, касающиеся деятельности криптографической службы составляют государственную тайну, подлежат особому хранению и при определенных условиях уничтожаются. Эти правила российская криптографическая служба строго соблюдала всегда. К разряду секретных до последнего времени относились и материалы, связанные с историей самой этой службы. В силу этих и некоторых иных причин в исторической науке почти полностью отсутствуют работы по истории русской криптографии, истории криптографической службы России.

В то же время мировая историческая наука вопросы истории криптографической службы различных государств исследовала весьма основательно, естественно, без ущерба для современных государственных интересов заинтересованных сторон. Сегодня, на пороге третьего тысячелетия, политическая история крупнейших мировых держав, а история криптографической службы является ее неотъемлемой составной частью, привлекает особой внимание. Ее знание и глубокое осмысление позволяет лучше понять настоящее, в определенной степени предвидеть будущее. Наиболее фундаментальными исследованиями на эту тему являются труды Дэвида Кана и в первую очередь его книга «Взломщики кодов» (David Kahn. The Codebreakers. – N. Y. 1967). Однако история криптографической службы России до последнего времени оставалась белым пятном. Наши исследования, проводившиеся на протяжении последних двадцати лет, ставили своей целью восполнить этот пробел.

Мы впервые в отечественной исторической науке провели масштабное изучение различных государственных архивов России и бывшего СССР с целью выявления документов по интересующей нас проблематике. Необходимые материалы были обнаружены и изучены в следующих архивах: Архив внешней политики России (Москва), Центральный государственный архив Российской Федерации (Москва), Российский центр хранения и изучения документов новейшей истории (Москва), Центральный архив ФСБ РФ (Москва), региональные архивы КГБ СССР (Ленинград, Рига, Ташкент), Центральный партийный архив КПСС, областные партийные архивы, Российский военный государственный архив, Центральный государственных архив литературы и искусства и др.

Большая научно-исследовательская работа проводилась автором в период службы в КГБ СССР - ФСБ России. Нами были опубликованы десятки статей, как

определенный этап следует выделить период работы над книгой о жизни и деятельности организатора и первого руководителя криптографической службы России советского периода Глеба Бокия («Доверено защищать революцию», М., Политиздат, 1987). В 1994 году нами была опубликована книга «Тайнопись в истории России». (История криптографической службы России ХУШ – начала ХХ в.).

В этой книге автор впервые в отечественной исторической науке сделал попытку воссоздать, возможно, более полную картину становления и развития криптографической службы России, критически осмыслить накопленный исторический опыт, рассмотреть роль специальной службы в политической истории государства в целом, познакомить читателя с ранее не известными историческими фактами, событиями именами. Здесь уместно привести некоторые выводы и обобщения, к которым мы приходим в нашей работе.

Начало развития криптографии как необходимого и достаточно надежного средства сохранения государственных секретов в России, по существу, относится к эпохе Петра I. Этот период и весь ХУШ век характеризуется широким использованием шифр переписки, организацией первых шифровальных служб, появлением первых наметок анализа шифров, созданием шифров с последующим их усложнением. Разработка шифров, их доставка на места эксплуатации были четко организованы и подчинялись действию определенной системы. Постоянно разрабатывались шифры для индивидуальной, циркулярной связи и для расширявшихся систем общей связи. Создатели шифров правильно понимали значение лингвистических, статистических характеристик шифрованных и открытых текстов для использования их при де шифровании. Русские шифры обладали своеобразием: активно использовались пустышки, многоязычные шифры, специальные усложнения, что повышало их криптографическую стойкость.

40-е годы ХУШ столетия, а точнее, 1742 год можно с полным правом считать временем создания де шифровальной службы России. К этому периоду сложилась определенная система дешифровальной деятельности: была создана служба перехвата и перлюстрации секретной шифр переписки иностранных корреспондентов, организованы ее дешифрование, перевод, докладывание сообщений в высшие инстанции. Была осознана необходимость организации криптографической службы как единой слаженной системы, придания ей научной базы. Важный вклад в дешифровальную аналитическую работу внес известный математик И.-Х. Гольдбах, дело которого продолжали У.Эпинус и другие ученые. Научный подход и активное заинтересованное внимание руководителей государства к специальной службе позволили России добиться быстрых и важных успехов в дешифровании корреспонденции Франции, Англии, Германии.

В XIX веке в России, как и в других передовых государствах Европы, в области применения шифров начинает постепенно входить и развиваться принцип иерархии. Для каждого уровня корреспондентов, как правило, свои системы шифров или свои правила пользования ими: от простых в эксплуатации, но менее стойких к сложным и более стойким.

Сравнивая шифры России с шифрами других развивающихся государств того времени, следует сделать вывод, что, по крайней мере, по криптографической стойкости, а также по ряду других критериев, включая (в определенной мере) и критерии, характеризующие эксплуатационные качества, отечественные шифры не уступали шифрам таких передовых стран, как Англия, Франция, Италия. По-видимому, можно сделать вывод о том, что если Россия в чем-то и отставала от стран Западной Европы, то это все-таки относится к вопросам углубленной механизации и автоматизации процессов шифрования и дешифрования. К этому можно добавить вопросы организации широкой подготовки кадров криптографов и разработки теории криптографического анализа шифров и опубликования результатов этой разработки в фундаментальных трудах, оказавших большое влияние на последующее развитие криптографической мысли.

В истории России XIX – начала XX века нельзя назвать ни одного имени крупного математика или группы молодых специалистов, впоследствии выросших в крупных ученых, которые бы профессионально занимались теорией криптографии, анализом шифров и разработкой методов дешифрования. П.Л.Шиллинг в этом плане представлял собой скорее исключение, чем правило, но и он был инженером-электротехником и не имел каких-либо трудов в области математики. В то время в странах Западной Европы многие математики занимались вопросами криптографии, что, в конечном счете, не могло не сказаться в дальнейшем на быстром развитии этой прикладной области исследования.

Опыт русско-турецкой и других войн показал, что используемые коды мало пригодны для целей шифрования в военных условиях. Эти шифры оказались громоздкими, ненадежными из-за большого числа ошибок, допускавшихся в процессах шифрования и расшифрования. Из этого опыта следовало делать правильные выводы и вести интенсивную работу по созданию новых стойких шифров, надежных в эксплуатации, поддающихся механизации и автоматизации.

К сожалению, в этих вопросах Россия постепенно стала отставать от Европы, что в конечном итоге сказалось уже в первой половине XX столетия – в первой мировой и Великой Отечественной войнах. Общее отставание России в промышленном отношении от стран Запада не могло не сказаться на отставании в развитии средств и методов связи (телеграфной, радиосвязи), а, следовательно, и на развитии шифр связи, что также проявилось в первую мировую войну и в значительной мере повлияло на исход крупных сражений.

В период гражданской войны значительная часть арсенала сил и средств, кадрового состава криптографической службы царской России была унаследована белой гвардией и затем оказалась за границей. Несмотря на то, что советская сторона частично располагала старыми кадрами специалистов-криптографов, имела в своем распоряжении системы шифров и кодов, применявшихся белой гвардией, из-за слабого оснащения станций радиоперехвата, отсутствия квалифицированных кадров в необходимом количестве линии шифрованной связи белых практически не контролировались. В 20-х годах в Советской России началось критическое осмысление состояния безопасности отечественных линий связи и определение организационных форм будущей шифровальной службы страны. В начальный период этой деятельности руководители страны уделяли

этой службе должное внимание. В результате был создан Специальный отдел при ВЧК как единый центр криптографической службы страны. Структура отдела, кадровый состав, задачи и методы его работы во многом продолжали традиции специальной службы России. В этом было как положительное, так и отрицательное начало. Успехи советской специальной службы в создании систем ручных шифров, системы радиоперехвата в подготовке кадров специалистов-криптографов свидетельствуют о большой, целенаправленной и продуманной работе, которая велась в стране в области развития криптографической службы. С другой стороны подход к криптографии как к виду деятельности узкого круга специалистов, оторванность от достижений мировой криптографической мысли, отсутствие криптографов-математиков, обладающих широкими и фундаментальными аналитическими познаниями, привели к значительному отставанию от стран Запада.

События 30-х годов, фактическое вхождение криптографической службы в систему органов безопасности, сталинский террор нанесли ей существенный урон. Однако, служба продолжала работать в определенной степени выполняя свои задачи. В предвоенное время, то есть к концу 30-х годов, работа советских криптографов определялась значительной активизацией шифрованной переписки иностранных государств и увеличением ее перехвата. При этом работа усложнялась тем, что заметно повысилась стойкость наиболее важных иностранных шифров, некоторые государства стали применять на военных и дипломатических линиях связи шифровальные машины. Кроме того, работа над иностранными шифрами требовала большого количества квалифицированных работников, которыми советская криптографическая служба в то время еще не располагала.

Следует признать, что в этот период в советской криптографической службе наблюдалось постепенное отставание уровня научных исследований и криптографии, замерли поиски и разработка принципиально новых идей и методов дешифрования, новых шифр систем. Если указанное обстоятельство отрицательно повлияло на методы дешифрования применявшихся в то время ручных шифров и кодов с различными усложнениями, то оно сказалось просто катастрофически на разработке теории и практики дешифрования уже появлявшихся в то время электромеханических шифраторов, и в первую очередь «Энигмы». При этом еще первая мировая война дала сильный импульс развитию криптографии почти во всех передовых капиталистических странах, и в первую очередь развитию методов криптоанализа, методов машинного синтеза.

Проведенное нами исследование позволяет выделить те необходимые направления, те компоненты работы, которые были упущены советской криптографической службой в 20-е и 30-е годы.

1. Правильный прогноз развития шифр средств. Внимание этому виду анализа.
   Справедливо было подмечено, что шифр блочной гаммы одноразового использования, несмотря на его абсолютную криптографическую стойкость, не является перспективным. Он требует слишком большого времени для зашифрования и очень громоздок, чтобы применять его в сколько-нибудь широком масштабе. Поэтому англичане пришли к

правильному выводу о том, что наиболее вероятно обращение криптографов Германии к машинным шифрам, которые уже в 20-е годы получили реальные очертания и обладали такими важнейшими качествами, как быстродействие, легкость в обращении при шифровании и рас шифровании.

2. Продуманные оперативные мероприятия.

Так, англичане своевременно давали своим агентам задание вести целенаправленный поиск такой шифровальной машинной системы. Подобные задачи перед советской разведкой, по-видимому, в тот период не ставились. Во всяком случае, возможность купить документы, связанные с машинным шифрованием, или даже сами машины была. Вне поля зрения советской разведки оказалась и работа центра в Блечли.

3. Привлечение к работе научных специалистов, практиков-аналитиков и талантливых организаторов.

В Блечли были привлечены к работе несколько самых выдающихся математиков Англии: Александер, Беббут, Барри, Уэлгмет. Все они обладали помимо математических способностей даром глубокого анализа, расчета многочисленных возможностей вариантов. Вместе с ними трудились молодые специалисты-криптографы Нокс, Тилтмен, Стреги – незаурядные люди, создавшие электронную быстродействующую систему для дешифрования «Энигмы». Эти люди в кратчайшие сроки разработали и усовершенствовали методы дешифрования, построили электронную специализированную вычислительную машину «Бронзовая богиня». Вся эта работа привела к тому, что уже в феврале 1940 года начались массовая передача зашифрованных радиограмм по линиям радиосвязи и их массовое дешифрование.

В Советском Союзе математики высокого класса были привлечены в криптографическую службу лишь в конце 40-х годов, когда уроки войны заставили правительство в корне пересмотреть свое отношение к этой службе.

Таким образом, криптография в России в рассматриваемый период проявила себя скорее как практическая деятельность, а не как наука.

Отечественная криптографическая служба всегда являлась составной частью государственной машины, точнее – разведки и контрразведки, начиная с начала XУIII века и до новейшего времени. На структурах, методы, размах деятельности криптографической службы постоянно влияли два фактора: внешнеполитический, который порождался потребностями России, ее менявшимся положением в системе других государств, и внутриполитический, определявший уровень экономики, науки, культуры по сравнению с другими государствами.

По мере развития методов и средств шифрования и дешифрования, увеличения криптографической стойкости шифров обеспечение безопасности связи криптографическими методами становится задачей все более комплексной, решение ее может быть эффективным с применением

и других методов – инженерно-технических, организационных и иных. История, в особенности XX века, четко показала, что ни в коей мере нельзя оставлять без внимания крупные теоретические исследования, направленные на перспективу. Именно крупные исследования время от времени содержат такие выводы, которые рождают принципиально новые направления криптографии и оказывают революционизирующее воздействие на всю последующею криптографическую деятельность. Такие открытия и повороты в криптографии по своей значимости и конечной пользе не раз перекрывали все затраты на фундаментальные исследования, делая их «рентабельными» в долгосрочном плане.