Хранители тайны.

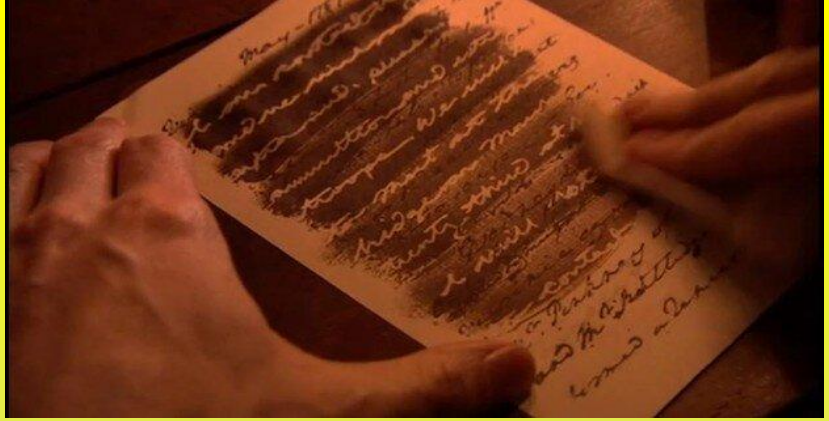
Презентацию подготовила Мещерякова О.В., ОИБО ЦБ БЕН РАН

Свой профессиональный праздник российские шифровальщики отмечают 5 мая.

Именно в этот день в 1921 году согласно Постановлению Совета народных комиссаров РСФСР была создана первая советская служба криптографии и шифрования.

Праздничным он является так же для представителей криптографической службы России, всех, кто связан с шифровкой важной информации, кто имеет отношение к связи и коммуникациям.

Также поздравления 5 мая принимают специалисты, связанные с военной тайной и государственными секретами, работники сферы информационных технологий, ученые – криптографы.



Во все времена люди прятали свои секреты, и именно шифры помогали справляться с этой задачей успешнее всего. Шифровка оказалась самым надежным способом скрыть информацию.

Изначально шифры были примитивными, а порой просто дикими. Например, во времена египетских фараонов для передачи тайного письма выбирался раб, точнее, его голова. Его брили наголо и водостойкой растительной краской наносили текст сообщения. Когда волосы отрастали, раба отправляли к адресату. Там его снова брили и читали нанесенный текст. Для удобства обработки голову предварительно снимали с плеч.

Правда, доставка сообщения таким способом была не очень надежной. Ведь во время путешествия носитель сообщения мог быть убит, заболеть или, наконец, просто сбежать.

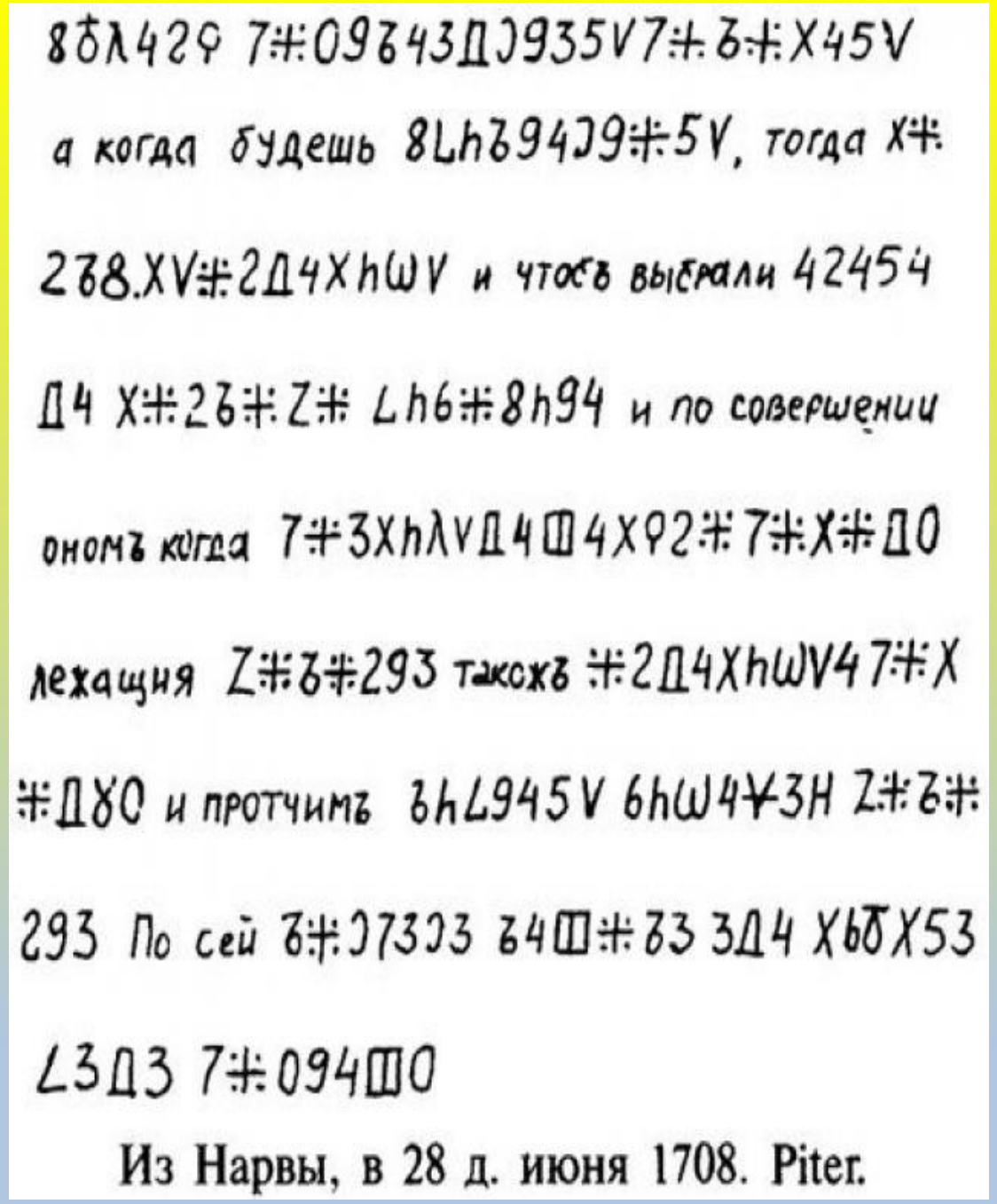
Также хорошо известна система Цезаря, который в тексте каждую букву заменял на последующую в алфавите. Метод действовал только потому, что тогда мало кто умел читать и писать. Известными шифровальщиками древности были Аристотель, Нерон и Пифагор.

Одним из самых популярных способов скрыть послание были симпатические или исчезающие чернила. В Средние века шпионы особенно преуспели в их изготовлении.

Первое упоминание о «тайнописчиках» имеет отношение к созданному в России в 1549 году Посольскому приказу. На службе в этом приказе состояли и разработчики шифров, называвшихся «азбука», «цифирь» и «цифра».

Впрочем, в те стародавние времена дипломаты пользовались довольно бесхитростными способами шифрования. Так, например, русский посол в Грузии просто разбивал текст на слоги и переставлял буквы в каждом слоге.

Первым дошедшим до наших дней русским шифром считается введенный в действие в 1633 году шифр **патриарха Филарета**.



При Петре I шифрование стало гораздо сложнее и изощреннее. Был создан целый шифровальный словарь, и для кодирования сообщений уже не просто заменяли буквы, а использовали новые символы, знаки, буквы и цифры. В дешифратор были добавлены «пустышки» - символы, которые ничего не означали и только запутывали человека, перехватившего послание.

Письмо, зашифрованное на картинке слева, читается следующим образом:

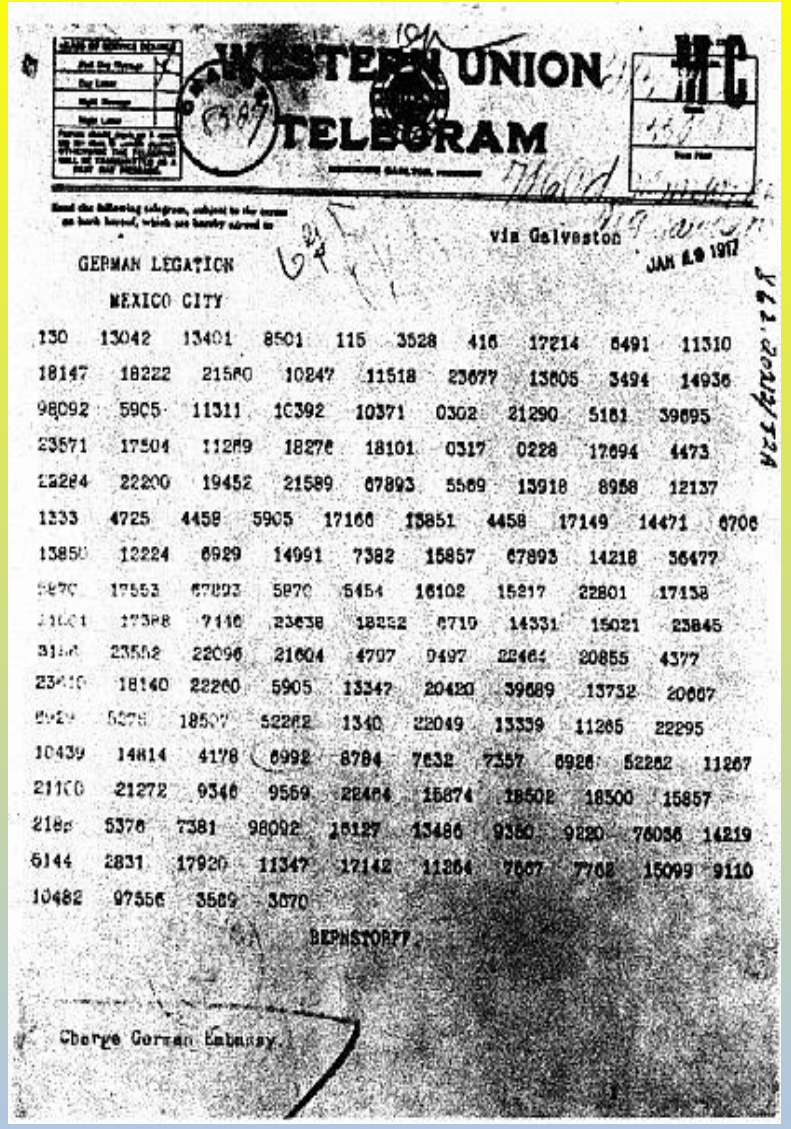
«***Поди къ Черкаскому и, сослався з губернаторомъ азовскимъ, чини немедленно съ Божіею помощію промыслъ надъ тьми ворами, и которые изъ нихъ есть поиманы, тъхъ вели вѣшать по украинскимъ городамъ. А когда будешь в Черкаскомъ, тогда добрыхъ обнадежь и чтобъ выбрали атамана доброго человека; и по совершении ономъ, когда пойдешь назадъ, то по Дону лежащие городки такожъ обнадежь, а по Донцу и протчим речкамъ лежащие городки по сей росписи разори и над людми чини по указу***».

К началу XX века Россия пришла с довольно слабым криптографическим багажом. Кодирование секретных сообщений происходило с помощью шифра простой замены (одного символа на другой), без какого-либо усложнения.

Впрочем, простейшими шифрами пользовались в то время и в Западной Европе, Японии, США. Уже осенью 1914 года часть русских военных шифров была расшифрована австрийцами.

В 1916 году в русской армии ввели новый тип шифра со множеством шифровальных групп, но и это не помогло обеспечить полную секретность. По сравнению с армией флотские специалисты добились куда больших успехов.

На поврежденном в Балтийском море германском крейсере «Магдебург» нашли папку кодов, а вторую, выброшенную немцами, достали со дна водолазы. Для перехвата германских радиосообщений в Балтийском море и в Севастополе построили специальные подслушивающие станции. Несколько раз немцы и пользующиеся немецкими шифрами турки меняли коды, но все они были разгаданы русскими дешифровщиками.



После революции защитой государственных и военных тайн озаботились уже большевики. В шифровальном отделении, организованном приказом Реввоенсовета в ноябре 1918 года, работало поначалу всего 14 человек.

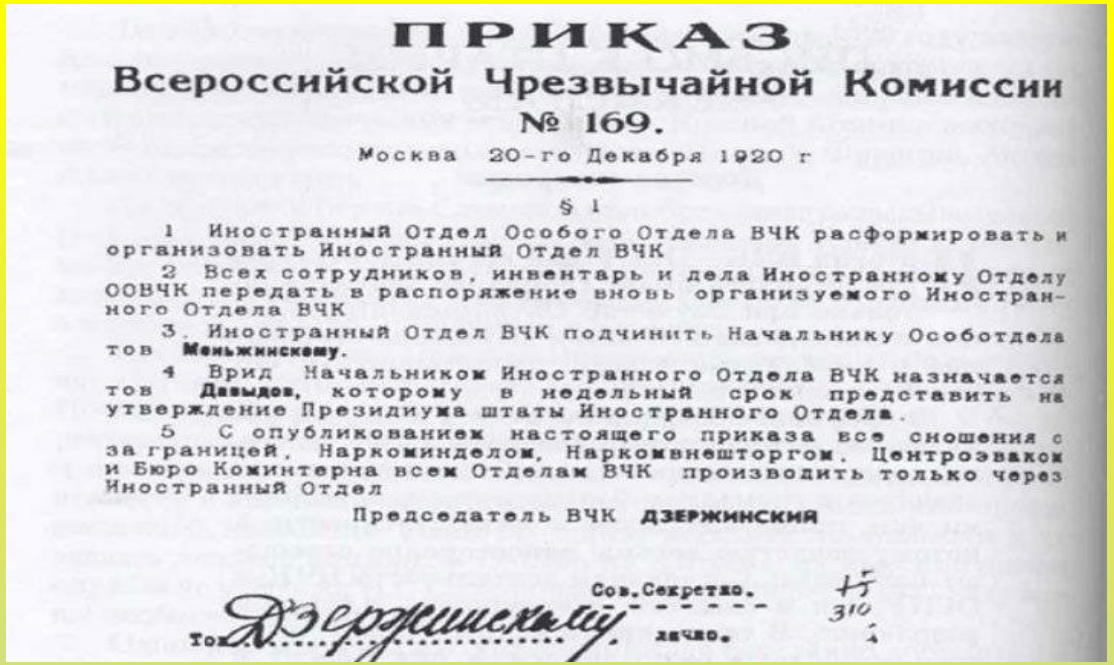
Уровень защиты ценнейшей информации молодой советской республики оказался в те времена весьма посредственным. Нередко для экономии времени шифровались только отдельные участки секретных сообщений, а остальная их часть передавалась открытым текстом. Плюс советские шифры повторяли старые ошибки: все они представляли собой простейшие замены слов на цифровые группы.

Осенью 1919 года польские дешифровальщики смогли взломать шифры РККА и до конца 1920 года перехватили несколько тысяч радиограмм, подписанных **Троцким**, **Тухачевским**, **Якиром** и другими. На основе этих сообщений командование польской армии смогло принять верные стратегические решения и одержать победу в Варшавском сражении и во всей польско-советской войне.

Немалый урон наносили и случаи прямого предательства со стороны шифровальщиков Красной армии.

Так, в 1919 году в руки противника попало более 20 шифров, в 1920 — около 30. Специалисты армии Врангеля буквально через час после перехвата читали все телеграммы красного комфронта Фрунзе.

Советские дипломатические шифры также успешно взламывались почти всеми дешифровальными отделами европейских стран.



ПРИКАЗ
Всероссийской Чрезвычайной Комиссии
№ 169.
Москва 20-го Декабря 1920 г

§ 1

1 Иностранный Отдел Особого Отдела ВЧК расформировать и организовать Иностранный Отдел ВЧК

2 Всех сотрудников, инвентарь и дела Иностранному Отделу ОООВЧК передать в распоряжение вновь организуемого Иностранного Отдела ВЧК

3. Иностранный Отдел ВЧК подчинить Начальнику Особотдела тов **Меньжинскому.**

4 Врид Начальником Иностранного Отдела ВЧК назначается тов **Давыдов,** которому в недельный срок представить на утверждение Президиума штаты Иностранного Отдела.

5 С опубликованием настоящего приказа все сношения с за границей, Наркоминделом, Наркомвнешторгом, Центроэваком и Бюро Коминтерна всем Отделам ВЧК производить только через Иностранный Отдел

Председатель ВЧК **ДЗЕРЖИНСКИЙ**

Сов.Секретно.
Тов. Дзержинскому. лично.

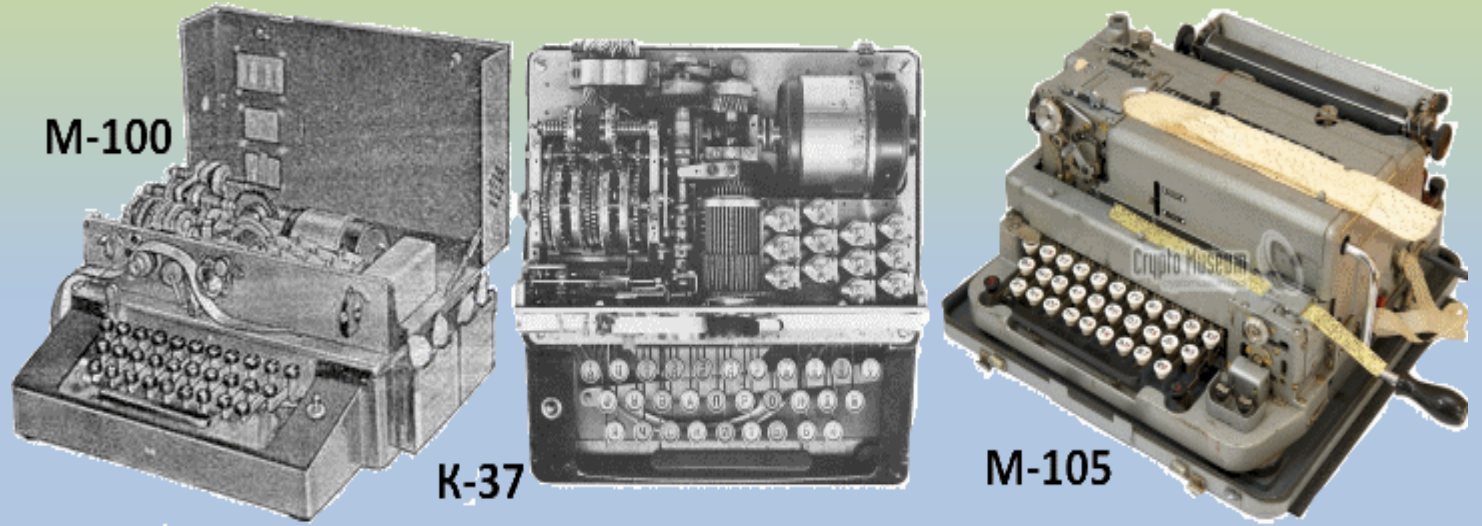
Ситуация начала меняться только в 1920 году, когда в Политбюро ЦК РКП(б) обсудили меры по повышению уровня защиты секретных сообщений.

В апреле следующего года был создан центральный шифровальный отдел штаба РККА, а 5 мая 1921 года декретом Совнаркома был учрежден спецотдел ВЧК, занимающийся «наблюдением за всеми государственными учреждениями, партийными и общественными организациями по сохранению государственной тайны».

Впоследствии сотрудники спецотдела смогли дешифровать телеграммы иностранных шпионов, работавших в советской России под прикрытием, раскрыть немецкий дипломатический код, взломать шифры разведотдела польского Генштаба.

В 1927 году наши умельцы начали читать японскую шифропереписку, а в 1930 — американскую.

Кардинально изменило ситуацию изобретение Ивана Волоска. Он сконструировал первый действующий экземпляр шифровальной машины, который сильно отличался от зарубежных. ШМВ-1 (Шифровальная машина Волоска — 1), так назывался этот аппарат, создавал нечитаемые криптограммы с высокой стойкостью. Позже стала выпускаться новая модель М-100. Она обрабатывала шифрованные телеграммы в пять раз быстрее ручного способа, сохраняя при этом стойкость передаваемых радиотелеграмм. Главным недостатком этой машины был большой вес. Устройство весило 141 килограмм. Ей на смену пришла шифровальная машина К-37 "Кристалл", которая весила всего 19 килограммов.



К началу войны на вооружение шифровальных органов СССР было принято свыше 150 комплектов К-37.

За годы войны шифровальные машины обрабатывали полторы тысячи телеграмм в день, тогда как суточная норма составляла всего 400. Это лишило противника возможности читать секретные депеши и документы и тем самым спасло множество жизней.

По мнению историков, если бы не работа службы криптографии и шифрования, Вторая мировая война длилась бы на два года дольше.

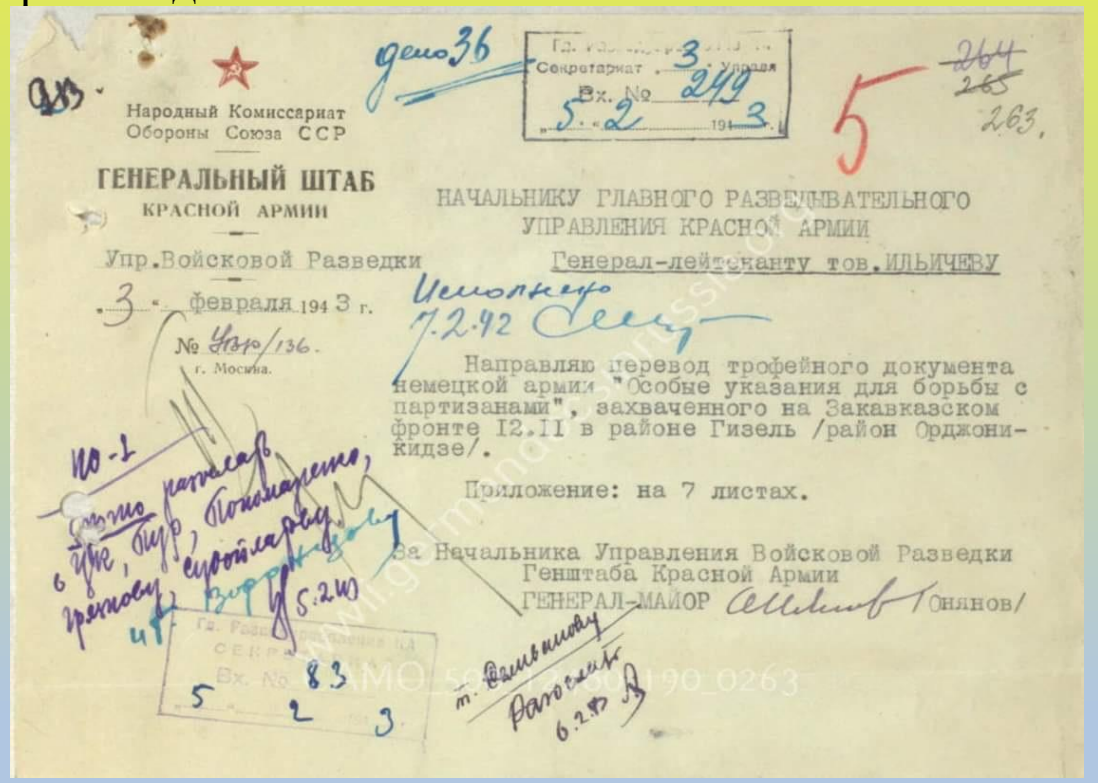
Во время Великой Отечественной войны дешифровальщики противника не смогли прочесть ни одной перехваченной советской криптограммы, обработанной машинными шифрами.

Такая система шифрования могла быть уязвима только в одном случае: при наличии самой техники и ключей к ней. Недаром по инструкции советских шифровальщиков обеспечивали надежной охраной, но, помимо этого, они обычно ставили перед собой канистру с бензином и держали под рукой несколько гранат, чтобы при приближении врага уничтожить документы, технику и себя.

Приказ **Гитлера** по вермахту от августа 1942 года, который так и не был выполнен, гласил:

«... кто возьмет в плен русского шифровальщика либо захватит русскую шифровальную технику, будет награжден Железным крестом, отпуском на родину и обеспечен работой в Берлине, а после окончания войны — поместьем в Крыму».

В военные годы на машинную шифросвязь легла огромная нагрузка по передаче секретных телеграмм. В штабах армии ежедневно получали до 60 телеграмм, в штабах фронтов нормальной считалась нагрузка до 400 телеграмм в день.



Народный Комиссариат Обороны Союза ССР

ГЕНЕРАЛЬНЫЙ ШТАБ КРАСНОЙ АРМИИ

Упр. Войсковой Разведки

3 февраля 1943 г.

№ Упр/136.

г. Москва.

НАЧАЛЬНИКУ ГЛАВНОГО РАЗВЕДЫВАТЕЛЬНОГО УПРАВЛЕНИЯ КРАСНОЙ АРМИИ

Генерал-лейтенанту тов. ИЛЬИЧЕВУ

Направляю перевод трофейного документа немецкой армии "Особые указания для борьбы с партизанами", захваченного на Закавказском фронте 12.II в районе Гизель /район Орджоникидзе/.

Приложение: на 7 листах.

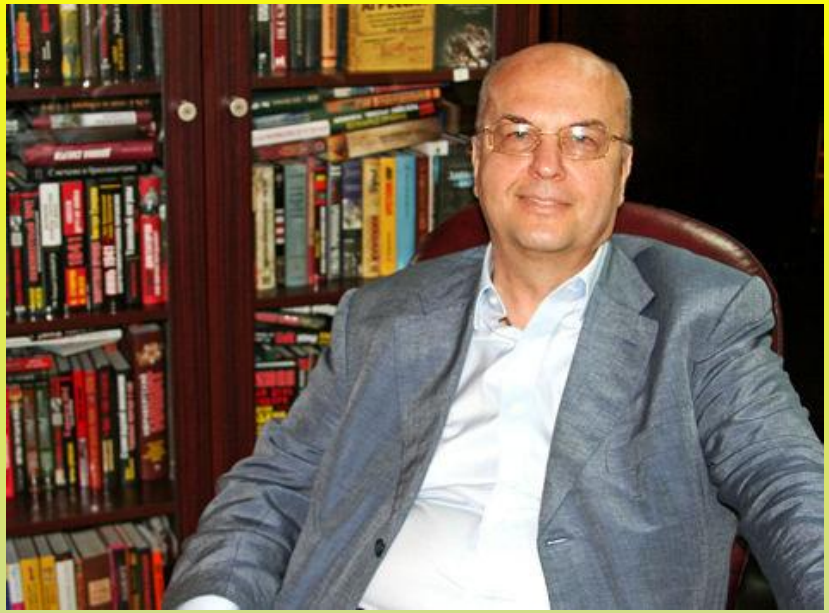
За Начальника Управления Войсковой Разведки Генштаба Красной Армии

ГЕНЕРАЛ-МАЙОР /Онянов/

С 1970-х годов криптография стала компьютерной, что обеспечило большую скорость шифрования и максимально высокую устойчивость к взлому.

Экскурс в прошлое.

(Из интервью «МК» учёного-криптографа Анатолия Викторовича Клепова).



«…Если мы проанализируем историю России XX - XXI веков, то увидим, что **практически все крупнейшие кризисы** сначала Российской Империи, затем СССР, а потом Российской Федерации **вызваны поражениями в информационных войнах.**

Противники были разные. Первая Мировая война. Армия Самсонова, фактически нанеся поражение немецким войскам, потерпела поражение. Почему это произошло? Из-за того, что в армии неправильно были розданы ключи к шифрованию. Ошибки привели к тому, что немцы перехватывали разговоры по радиосвязи между русскими армиями и знали все о передвижении противника. Что и **привело впоследствии к разгрому царской армии**. Если бы не утечка информации, русские войска в 1914 году вполне могли оказаться в Берлине и выиграть Первую Мировую войну. Могло это изменить историю? Думаю, да. Не было бы причин для недовольства в обществе, ставших катализатором Октябрьской революции.

Следующий этап истории нашей страны - 1917 год. Император России Николай Второй отрезан от закрытой связи со своей ставкой и Царским Селом. **Результат — революция**.

1941 год, самые первые дни Великой Отечественной войны. Большое количество шифровальной техники, ручных документов кодирования, а самое главное ключи к ним попали в руки гитлеровцев. Шифрованная связь Советской армии, воевавшей с немецкими захватчиками, была скомпрометирована и фактически перестала существовать. Повторились обстоятельства 1914 года. Советской армии приходилось взаимодействовать по открытой связи. **Итог - громадные человеческие потери в начале войны**.

1979-й год — Афганская война. Я могу написать отдельную книгу о том, как «правильно» использовали советскую шифровальную технику и ручные документы кодирования и к чему это привело. Наши солдаты и офицеры в ротах, батальонах, полках, а порой и более крупных войсковых соединениях не имели надежную шифровальную связь. **Результат – неоправданно высокие потери личного состава**.

Разрушение Советского Союза в 1991 году. Президент СССР, как и Император России в 1917 году, был оторван от закрытой связи...

Чеченские войны. Хочу привести цитату из книги генерала Г.Н. Трошева «Моя война»: «**Скупой платит дважды. Мы платили кровью из-за отсутствия шифровальной техники**»...

Получается, **годы, столетия недостаточного внимания к информационной безопасности страны обернулись гибелью лучших сынов России, финансовым и материальным разорением нашей страны**. И это при том, что Россия всегда считалась крупнейшей криптографической державой».

О высочайшем уровне преступников, с которыми приходилось иметь дело свидетельствовал такой факт. В результате проверки **мы обнаружили не только фальшивые РКЦ, но и многочисленные фальшивые телетайпы**!

Преступники обрезали связь удаленных от Москвы расчетных центров, вклинивали в линию свой телеграф и, **имитируя работу РКЦ Центрального Банка, рассылали, фальшивые авизо**. Против России велась настоящая информационная война. И как во время реальных войн, преступники часто использовали подмену подлинной информации фальшивой. На языке профессионалов это называется «радиоигрaми». Нам противостоял не просто «криминал». Пришлось иметь дело с противниками высочайшего класса, прекрасно знавшими все тайны банковской системы. Кроме того, по используемым ими приемам **было понятно, что за спиной у них и немалый опыт ведения электронной разведки**.

Хищения начались, когда готовился выпуск ваучеров, а пик краж совпал с принятием законов о приватизации. Приватизационных ваучеров выпустили на три триллиона рублей, а денежных хищений по фальшивым авизо зарегистрировано — на четыре триллиона. Фактически **сумма украденных средств превышала стоимостью всех промышленных предприятий России**.

Но основная проблема была даже не в количестве. **Требовалось разработать уникальный криптографический алгоритм для подтверждения достоверности кода каждой платежки**.

Ему тоже двадцать лет. Он стал частью разработанной нами уникальной системы, до сих пор используемой Центральным Банком России.

Знаете, почему количество цифр на платежке - именно двадцать? Когда, руководство ЦБ связалось со мной и поинтересовалось, какой максимальный ряд цифр может обеспечить наш шифратор, я сказал: «Двадцать». Поэтому на каждой российской платежке теперь - двадцатизначный счет».

Сегодня криптографическая служба РФ занимает лидирующие позиции в мире. Ее специалисты обеспечивают защиту информации в телекоммуникационных системах и системах специальной связи в России и ее учреждениях за рубежом.