Шифровальные машины СССР 1931-1991 гг.

Шифровальные машины СССР История создания и характеристики В-4, М-100, М-101, К-37, М-105, М-125, М-105, М-205. Ключевые документы шифровальных машин. Обзор 1931- 1991 годы

18 ноября 2020 (обновлено 04.09.2024) · На чтение: 24 мин Комментарии: 8

Содержание

1. Необходимость автоматизации процесса шифрования
2. Начало работ по созданию шифровальных машин в СССР
3. Шифровальная машина М-100 (В-4) «Спектр»
4. Кодировочная машина К-37 «Кристалл»
5. Шифровальная машина М-101 «Изумруд»
6. Советские шифровальные машины послевоенного периода
7. Кодировочная/шифровальная машина М-125 «Фиалка» («Фиалка-3М»)
8. Шифровальная машина М-105 «Агат»
9. Шифровальная машина М-205

1. Необходимость автоматизации процесса шифрования

Внедрение технических средств связи (телеграф, телефон, радио) в конце 19 -начале 20 века, позволило многократно повысить оперативность передачи шифрованных сообщений. В то же время открылись самые широкие возможности для их перехвата. Это потребовало кардинального повышения стойкости шифров, ведущей к их усложнению. Разрыв между скоростью шифрования сообщений и скоростью их передачи еще более увеличился.

В то же время, задержка доведения информации, способна нанести ущерб больший, чем ее перехват и дешифровка противником.

Выход был найден в автоматизации процесса шифрования

После окончания первой мировой войны началось создание первых шифровальных машин, в том виде, в котором мы их знали на протяжении двадцатого столетия. Наиболее часто в них использовались шифраторы, в которых преобразование текста реализовывалось следующими методами:

- Наложение на открытый (или уже преобразованный по несложному алгоритму) текст внешнего шифра, представляющего собой случайную равновероятную гамму.
- Многоразовой заменой знаков открытого текста сдвигаемым по заданному закону алфавитом, с периодом равным модулю шифрования
- Наложением на открытый или преобразованный текст псевдослучайной гаммы, вырабатываемой самой шифровальной машиной.
-

Наиболее значимыми изобретателями шифровальной техники того периода являлись:

Гилберт Вернам (США) — изобрел шифровальную машину с внешним носителем шифра (1919 г.).

Хуго Кох (Нидерланды) — изобрел машину с шифратором, состоящим из 3 подвижных дисков и штепсельного коммутатора (1919 г.).

Арвид Дамм (Швеция) — разработал несколько типов механических шифровальных машин и электромеханическую В-1.

Артур Шербиус (Германия) — изобрел знаменитую «Энигму».

Борис Хагелин (Швеция) — вероятно самый продуктивный из изобретателей шифровальных машин. Среди его разработок и прототип американской М-209.

2. Начало работ по созданию шифровальных машин в СССР

1931 году при 8-ом отделе Штаба РККА было создано 2 отделение —техническая лаборатория.

В 1932 г. в ней были разработаны и изготовлены два образца шифровальной машины «ШМВ-1». Ввиду ее громоздкости и механической ненадежности работы были прекращены.

Однако использованный в ней принцип гаммирования стал основным для советских шифровальных машин на несколько десятилетий.

В этот же период офицеры 8 отдела совместно с сотрудниками Спецотдела НКВД разработали проект технического задания на конструирование отечественной шифровальной машины.

В конце 1933 г. из сотрудников Спецотдела НКВД и командиров РККА была создана совместная группа для выбора предприятия наиболее пригодного для разработки и изготовления отечественной шифровальной машины.

Выбор остановился на заводе № 209 (Завод им. Кулакова, бывший завод Гейслера, построен в 1896 г.)



Завод им. Кулакова (№ 209)

В ноябре 1934 г на завод приехал начальник Второго отделения Восьмого отдела штаба РККА капитан 1 ранга И.П. Волосок. После ознакомления с заводом и разговора с его директором В.И. Голубиным 20 ноября было подписано соглашение, произвольной формы, о создании на заводе специальной группы для конструирования и изготовления шифровальной техники

Была создана первая в СССР научно-техническая и производственная структура по выпуску отечественной документирующей техники предварительного и линейного шифрования.

В июне 1935 г. между заводом и 8 отделом штаба РККА был подписан договор на проведение ОКР под шифром «В-4» и на заводе был открыт заказ № 1001

Для выполнения ОКР была создана, и утверждена Спецотделом ОГПУ, специальная группа. В ее состав вошли: В.М. Демичев, В.Н. Рытов, О.А. Примазова, Е.П. Изотова.

Эти четыре человека положили начало новому направлению в отечественной технике, обеспечивающей скрытое управление войсками.

Выпуск конструкторской документации на шифровальную аппаратуру «В-4» был завершен в 1937 году.

8 февраля 1938 г. был создан Комбинат техники особой секретности.

Маленькая спецлаборатория (4 человека, 30 м2) превратилось в современное предприятие, оснащенное новейшим оборудованием и принадлежностями.

В новом корпусе площадью 800 м2 трудились 18 разработчиков и около 100 рабочих.

В 1940 г. изделия ТОС занимали 5,6% в общем объеме выпуска продукции завода № 209. Руководителем комбината был назначен Г. С. Кукес.

Руководство 8 управления понимало, что такую сложную задачу, как создание отечественной шифровальной техники, можно решить только с привлечением лучших ИТР и рабочих.

И. П. Волосок

Высочайший уровень секретности требовал исключения/минимизации «текучести кадров». Для решения этих задач в полном объеме были задействованы методы экономического стимулирования.

Финансовые средства перечислялись заказчиком непосредственно на счет лаборатории, минуя бухгалтерию предприятия, что являлось грубейшим нарушением финансовой дисциплины.

Однако такой порядок позволил уже в 1936 г. после вычета затрат на зарплату, электроэнергию и прочие расходы получить прибыль в несколько сотен тысяч рублей, и направить ее на нужды лаборатории.

Уровень зарплаты работников был в 2 — 2,5 раза выше, чем у работников основного производства.

В 1940 г заказчик стал отчислять определенный процент, от суммы оплаченной продукции, непосредственно в фонд оплаты труда комбината, и размер заработной платы еще более увеличился.

Работники комбината уходили в отпуск в основном в летний период. Все желающие получали путевки в санаторий которые, как и билеты в оба конца, оплачивал комбинат. Те, кто не мог или не хотел отдыхать в санатории, получал денежную компенсацию.

Большое внимание уделялось семейному отдыху. Так за счет комбината организовывалось посещение театра им С.М. Кирова (Мариинский) Билеты приобретались на все спектакли сезона.

Рабочий день зачастую заканчивался поздно, дорога домой занимала час-полтора, люди уставали и не могли работать с требуемой отдачей.

Для таких случаев на комбинате была организована «гостиница». Трехразовое питание для работников, находящихся в «гостинице», обеспечивалось за счет комбината.

В цеху проходы были устланы ковровыми дорожками, а в комнате отдыха можно было в любое время отдохнуть и расслабиться.

Такой вот «хозрасчет по-Сталински»

3. Шифровальная машина М-100 (В-4) «Спектр»

В январе 1938 г. шифровальная аппаратура В-4 прошла Госиспытания, и в мае 1938 г. была принята на вооружение. В конце года начались ее поставки в войска. Время на обработку информации сократилось 5-6 раз. Скорость обработки составляла 300 знаком в минуту.

Использование термина «аппаратура» вместо «машина» было полностью обоснованным. «В-4» состояла из 8 оригинальных узлов и немецкой электромеханической пишущей машинки «Мерседес», общим весом 141 кг. Шифровальная машина (аппаратура) В-4 считается первой советской шифровальной машиной

В 1939 г под руководством Главного конструктора Н.М Шарыгина были завершены работы по модернизации аппаратуры «В-4». Модернизированный вариант получил название шифровальная машина М-100 «Спектр».



М-100 «Спектр»

Ее выпуск был начат в 1940 г. параллельно с «В-4». Вес данной машины был снижен до 116 кг.

Однако главным успехом была разработка собственного буквопечатающего устройства, которое позволило впоследствии, отказаться от использования немецкой электромеханической печатной машинки «Мерседес».

Специализированные печатающие устройства стали неотъемлемой частью отечественных машин предварительного шифрования. Это придало им дополнительное качество — способность документирования информации.

Отпечатанный шифровальной машиной текст становился юридически значимым документом.

4. Кодировочная машина К-37 «Кристалл»

В 1937 г под руководством главного конструктора В.Н. Рытова начались работы над малогабаритной дисковой кодировочной машиной.

Прототипом стала разработанная Б. Хагелином, для французской армии (500 шт.), шифровальная машина «В-211». Две такие машины были приобретены в Стокгольме нашим торговым представительством

В 1939 г. кодировочная машина К-37 «Кристалл» была принята на снабжение РККА. Вес машины составлял 19 кг.



Кодировочная машина К-37 «Кристалл»

В процессе эксплуатации выяснилось, что машина имеет низкую надежность, да и ее криптографическая стойкость была не высока. В том числе из-за ряда «упрощений» которые внесли в конструкции наши разработчики.

Часть недостатков была устранена, однако дальнейшее совершенствование остановилась, в том числе и по причине выхода Постановления ГКО № 3596 от 16 июня 1943 г. требующего ускорения поставки кодировочных машин в войска.
В сентябре 1941 года К-37 была захвачена немцами. После ее изучения немецкие криптографы пришли к выводу, что машина «примитивна» и безопасной ее можно считать лишь условно. Это не было секретом и для советских криптографов.
Интересно, что сегодня, многие «эксперты» и авторы, утверждающие, что советская шифровальная техника не попадала в руки немцев, (и все такое прочее) используют для иллюстрации описания К-37 фотографии как раз из немецкого отчета.



Фотография К-37 из немецкого отчета

Было принято решение об использовании кодировочной машины К-37 на Дальнем Востоке.
На советско-германском фронте она не использовалась. Во время допросов немецких криптоаналитиков американцами, те утверждали что трафик этой машины никогда не перехватывался.
Машина в период 1940-1941 гг. выпускалась на заводе № 209, а в период 1942-1945– заводом № 707 в Свердловске.
Эту машину вряд ли можно назвать удачной. В 1946 г она была взломана американцами с помощью специально созданного аналога «Sauterne Mk-I», а в 1947 г. снята со снабжения. Тем не менее эта машина положила начало семейству машин второго поколения, состоявшего из 18 моделей.

5. Шифровальная машина М-101 «Изумруд»

Дальнейшим развитием серии В-4 стала машина М-101 «Изумруд». Машина разрабатывалась конструкторами Шарыгиным и Козловым под общим руководством И. П. Волоска.
Машина состояла из двух узлов и весила 64,5 кг, а ее объем был уменьшен в 6 раз.
В 1942 г. «Изумруд» был введен в эксплуатацию. В 1943 в войска было отправлено свыше 90 комплектов шифровальной машины М-101.



М-101 «Изумруд» 1942 год

Производство этой машины было освоено в Свердловске, на заводе № 707, который считался филиалом завода № 209.
В июле 1941 г. производство ТОС было эвакуировано из Ленинграда в Свердловск. Двумя эшелонами было вывезено более 150 единиц наиболее ценного оборудования и 300 сотрудники комбината.

Ввиду негативного отношения партийного руководства Ленинграда к эвакуации предприятий, завод № 209 вывезти не успели. Впрочем, такая же судьба постигла и многие другие предприятия колыбели революции

За создание и внедрение шифровальной машины М-101 «Изумруд» И. П. Волоску, П. А. Судакову, В. Н. Рытову была присуждена Сталинская премия 3 степени.

Н. М. Шарыгин, М.С. Козлов, П. И. Строителев и Н. И. Гусев — награждены орденами.

И.П. Волоску также была присвоена ученая степень кандидат технических наук без защиты диссертации и воинское звание генерал-майор войск связи.

Для обеспечения подвижности шифровальных органов и ведения работы в процессе движения в 1939 г. в США были закуплены 100 автобусов «Студебеккер». На заводе № 209 было разработано специализированное рабочее место шифровальщика, размещенное в автобусе. В декабре 1940 г. были сданы заказчику 5 таких автобусов. Однако в условиях войны эта задача решена не была.

6. Советские шифровальные машины послевоенного периода

К началу Великой Отечественной войны было изготовлено немногим более 150 комплектов К-37 и 96 комплектов В-4/М-100.

По состоянию на май 1945 г. на вооружении более 130 шифровальных органов РККА находилось 396 комплектов шифровальной техники.

На середину 1941 года, в Германии было произведено порядка 50 000 шифрмашин «Энигма», а ко времени ее поражения, общее производства этих машин превысило 100 000 шт.

Следует добавить, что «Энигма» не единственный тип подобной техники, производимой в этой стране. В США за период войны было изготовлено около 140 000 ШМ «М-209» и 10 600 значительно более криптостойких «SIGABA», а также 450 000 шифдисков к ним. Производилось до 500 шифровальных машин «М-209» в сутки.

В СССР же основной системой шифрования были коды с перешифровкой.

Количественное превосходство западных стран в шифротехнике, перешло в качество, СУВ было значительно улучшено.



Шифровальная машина М-150 «Рубин»

В условиях разворачивающегося противостояния, в СССР были предприняты все возможные меры направленные, как на разработку новых образцов шифровальной техники, так и на насыщение ею ШО всех уровней и различной ведомственной принадлежности.

В послевоенные годы было разработано несколько десятков типов шифровальной техники. Буквой Т- стали обозначать технику линейного шифрования, а М- технику предварительного шифрования.

Уже в 1945 г. была разработана шифровальная машина М-102 «Малахит», в 1946 М-150 «Рубин», в 1952 освоено производство шифровальных машин М-152 (А и Б) «Гранит», М-103 «Малахит – 2М». В 1955 М-153 «Аметист- А». Далее последовали М-161 «Апатит», М-111 «Мрамор» В 1967 г. под руководством Н.М. Шарыгина была разработана дисковая машина М-120 «Жемчуг».

Свое место в этом ряду заняли СМ-1 «Василек» и СМ-2 «Сирень» имеющие незначительные отличия.



СМ-1 «Василек»



Шифровальная машина СМ-2

Производилась и специализированная шифровальная техника, например шифровальная машина М-130 «Коралл», предназначенная для закрытия метеорологической информации. На клавиатуре этой машины было всего 10 значащих клавиш, соответствующих цифрам от 0 до 9.



Шифровальная машина М-130 «Коралл» с блоком питания



Шифровальная машина М-130 «Коралл» с поднятой верхней крышкой

В 1980 гг.. в ВС СССР стали поступать шифровальные машины 3-го поколения М-200 «Уран», АРМ шифровальщика «Тобол» и другое оборудование.

Войска, в необходимых количествах были обеспечены спецаппаратными на разнообразной транспортной базе.



Спецаппаратная СА-9 шифровального органа

Однако долгие годы, практически до конца существования Советского Союза, основой машинного парка шифровальных служб СССР, государств ОВД и многочисленных друзей являлись: кодировочная машина М- 125 «Фиалка» (и ее модификации серии 3М) и шифровальная М-105 «Агат».

В просторечье получившие названия «цветок» и «камень».

7. Кодировочная/шифровальная машина М-125 «Фиалка» («Фиалка-3М»)

Наиболее полная информация о шифровальной машине М-125-3М «Фиалка-3М». В действительности, машина кодировочная, хотя процедура шифрования и была предусмотрена.

1. Общие сведения о М-125 «Фиалка»

Широко использовалась не только в ВС и силовых ведомствах, но и на предприятиях промышленности, торговом флоте и во многих других случаях.

М-125, одна из 18 дисковых шифровальных машин второго (послевоенного) поколения, разработана в середине пятидесятых годов под руководством Главного конструктора Н. Гырдымова.

Для повышения криптографической стойкости и эксплуатационных характеристик «Фиалка» неоднократно модернизировалась (М-125, М-125М, М-125-3М).

Производились модификации, адаптированные под языки (алфавиты) зарубежных заказчиков.



Технические характеристики изделия М-125-3М	
Напряжение питания	
Переменный ток	100-250В
Постоянный ток	24В±10%
Частота	50 или 400 Гц
Температура эксплуатации	
при влажности 65±10 %	0...50° С
при влажности 95-98 %	+2...40° С
Размеры ШхВхГ, мм (без упаковки)	
Машина	350x280x215
Блок питания	270x175x190
Вес, кг	
Машина	16
Блок питания	6,4
Рабочая скорость, знак/мин.	
С перфоленты	455
С клавиатуры	500
Вероятность ошибки	2×10^{-5}
Перфолента	17,4 мм, шаг 2,54
Клейкая лента	10 мм

ТТХ машины М-125-3М «Фиалка-3М»

По отношению к данной машине зачастую употребляется выражение «внучка Энигмы», «имеет конструктивное сходство» и т.п. Это так и не так. У «Фиалки» с «Энигмой» общего не больше, чем, например у KL-7 или NEMA. А конструктивное сходство — 4 колеса, имеют и «Мерседес», и «Запорожец». В части распространенности сравнима с американской KL-7 (25 000 штук, по цене чуть ниже 1500 долларов), а может и превосходит ее.

Важнейшим преимуществом данной машины, была возможность используя разовые (вырабатываемые) ключи обшей связи установить кодированную связь практически с любым корреспондентом, имеющим такую же машину и соответствующую ключевую документацию.

Считалось, что в угрожаемый или особый период это будет крайне необходимо. Для этого существовал специальный блокнот (ключевой документ), экземпляры которого имелись практически в каждом шифровальном органе и кодогруппе страны. И комплект шифрдисков на «особый период»

При работе в некоторых режимах машины «Фиалка-М» и «Фиалка-3М» являлись совместимыми

В эксплуатации имела неофициальное название «Цветок», в отличие от «Агата» известного как «Камень»

Будучи сложным электромеханическим устройством М-125 «Фиалка-3М» содержала множество самых разнообразных контактных групп и контактов, требовавших тщательного ухода. А где контакты, там спирт. В этом было одно из главных ее достоинств, с точки зрения эксплуатации.



Пример плотности сборки М-125-3М

Машина (контакты) любила спирт, но довольствоваться приходилось обычным ластиком. Иногда, от отсутствия «медицинского» алкоголя она дурела и начинала «бить звездочки и кресты». В этом случае приходилось идти на компромисс.

Тем не менее машина была вполне надежная, хотя и уступала, в этом отношении, «автомату Калашникова» шифрслужбы — М-105 «Агат»

После перехода на электронные шифраторы, была заменена на кодировочную машину М-465

2. Некоторые конструктивные особенности машины «Фиалка-3М»

Основные органы управления кодировочной (шифровальной) машиной М-125-3М «Фиалка-3М» показаны на рисунке ниже



Органы управления кодировочной/шифровальной машиной М-125-3М «Фиалк-3Ма»

В «Фиалке» ликвидирован один из главных недостатков «Энигмы» — невозможность зашифровки буквы на саму себя. С помощью, действительно оригинальной конструкции, состоящей из 3 транзисторов (2Т603А) и 7 диодов (Д237А) каждая 30 буква кодируется сама в себя.

Необходимо сказать, что в данной статье используются в основном фотографии машин стран ОВД. М-125-3М для советской армии имела некоторые отличия в том числе и по клавиатуре.

Не было латиницы, клавиши имели форму как у М-125М, соответственно и печатающая головка была только под кириллицу и цифры.



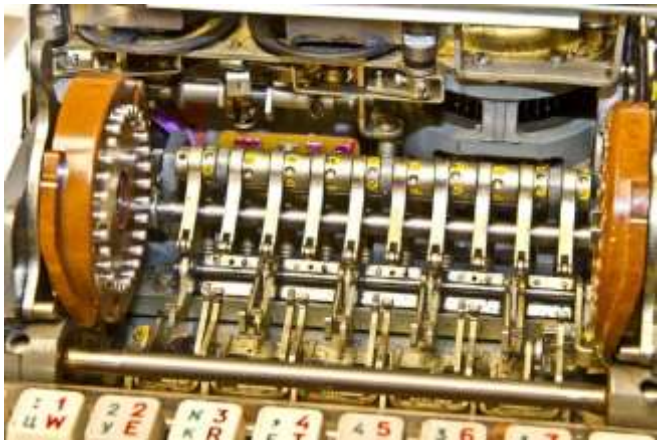
М-125-3М «Фиалка-3М» с русской клавиатурой для СА

В среднем ряду, крайние клавиши ЦФ и БК для переключения между буквенным и цифровым режимом работы.

Справа, н уровне шифрдисков, те самые «три транзистора» которые обеспечивают зашифровку каждой тридцатой буквы на саму себя.

Рядом переключатель режимов: ПФ — перфорация и ПЧ — печать.

Следующий переключатель, отвечает за выбор режимов работы: О — открытый текст, Р — расшифрование и З — зашифрование



Механизм движения шифрдисков машины М-125-3М

Движение каждого шифрдиска независимо от движения других и связь между ними производиться через специальные штифты

При нажатии клавиши, в движение приводятся все шифрдиски, если не стоит блокирующий штифт.

Механизм движения шифрдисков обеспечивал движение двух соседних дисков в противоположных направлениях.

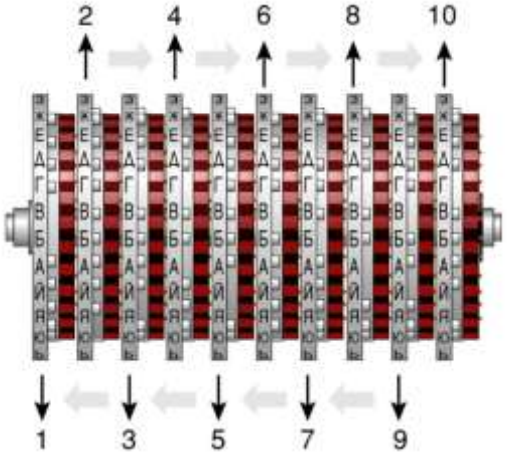


Схема движения шифрдисков кодировочной машины М-125-3М

Звук движения шифрдисков одинаков, что не позволяет использовать для дешифровки средства акустической разведки

В 80-е годы в ВС СССР использовались машины М-125М и М-125-3М. Между ними имелись «некоторые» различия.



М-125-М и М-125-3М (для стран ОВД)

Так на М-125-3М были введены дополнительные знаки на клавиатуре, задействован режим работы открытым тестом, при этом шифрдиски не двигались, введен переключатель модуля шифрования для базовой настройки коммутатора КС, переключатель работы «в линию».

Была предусмотрена работа непосредственно через датчик Морзе П-590А и радиостанцию Р-142. Однако этот режим как правило не применялся. При ошибке оператора, незашифрованный текст сразу мог уйти в эфир, да и каждый оператор имел свой «почерк», что позволяло идентифицировать те или иные части и соединения.



Датчик кода Морзе П-590А подключался к М-125-3М

Первоначально использовался блок питания БП-24 аналогичный блоку питания шифровальной машины М—105 «Агат»

Впоследствии заменен на БПК-125, более современное устройство с защитой от ПЭМИН и системой контроля.



Блоки питания БП-24 и БПК-125

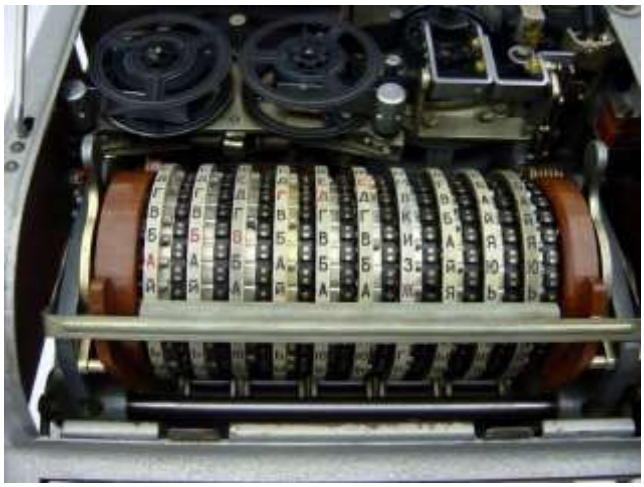
При печати или перфорации применяется 5-битный код. При этом задействуется до 5 соленоидов, в разной комбинации. По изменению потребляемого тока можно определить количество задействованных соленоидов для каждого знака, то есть читать текст. Причем на довольно большом расстоянии.

Для исключения этого в БПК-125 размещено 5 мощных резисторов, используемых в качестве искусственной нагрузки, каждый из которых является эквивалентом соленоида. Включением необходимого количества резисторов достигается постоянство потребляемого тока.

Этот БП в основном использовался в Советской Армии и Войске Польском

3. Криптографическая система машины М-125-3М «Фиалка-3М»

Собственно криптографическая система машины состояла из набора шифрдисков (ротора) и коммутатора КС 30х30



Установленные в «Фиалку» шифрдиски

На фото установленные в кодировочную машину шифрдиски (набор или ротор). Установочная планка опущена. Именно по ней выставлялся разовый ключ. Видны два металлических рычага-фиксатора (зажим/разжим) а так же диск ввода и отражатель (зеленного цвета).
Разборный/настраиваемый шифрдиск «Протон-2». Корпус, с подвижным наружным ободом. Сменный модуль проводки и фиксирующая защелка.



Шифрдиск Протон-2

В этой машине первоначально использовалось 10 шифрдисков с фиксированной внутренней распайкой. 30 входных контактов соединены с 30 выходными в определенном порядки и его смена в полевых условиях невозможна.
С 1978 г. машины комплектовались шифрдисками «Протон-2». Каждый диск имел внешнее регулируемое кольцо с 30 возможными положениями. Внутри диска находился модуль проводки, который так же мог быть зафиксирован в 30 различных положениях. Модуля проводки были взаимозаменяемы и могли использоваться в каждом диске.
Наборы шифрдисков (роторы) изготавливались различных серий с уникальными схемами внутренней распайки. Для Польши-3К, ГДР – 4К и т.д. Существовал комплект 0К используемый для общей связи. Иногда, ошибочно, указывают что для СССР использовалась серия 1К. Это не так. У советских дисков префикс был, как правило, двухзначный (например 68). Вероятно разные серии использовались в разных сетях.
Кроме того существовала и цветовая маркировка (цвет букв и т.п.)



Коммутатор КС 30х30 с перфокартой и тестовой пластиной машины М-125-3М

На фото слева выдвижная панель коммутатора КС-30х30 с установленной перфокартой суточного ключа. Данное устройство является вторым элементом (по сути первым) криптографической системы кодировочной машины М-125-3М. Перфокарта (часть суточного ключа) после извлечения из блокнота устанавливалась в лоток, который задвигался в корпус КМ.
Справа, вместо перфокарты, в коммутатор установлена, треугольная металлическая пластина. Она использовалась в процессе проверки работоспособности и при проведении техобслуживания. В этом случае коммутатор как бы «отключался», соединение цепей происходило «напрямую».
Ниже коммутатора расположен переключатель модуля 10 – 30 (не виден).
Самое верхнее отверстие — выход перфоленты. Чуть ниже и левее – разъем подключения блока питания.
В самом низу, на уровне коммутатора — тестовый электроразъем (заглушен).

4. Ключевая система кодировочной (шифровальной) машины М-125-3М «Фиалка-3М»

Для установки суточных ключей использовались блокноты ОСБ, ОСВ и некоторые другие.



Блокнот суточных ключей ОСВ-25 для машины «Фиалка-3М»

Каждый блокнот содержал 31 перфокарту (для коммутатора КС 30х30) и 31 таблицу настройки шифрдисков.

В таблице отметок делались записи о дате вскрытия блокнота, извлечении каждой ключевой таблицы и перфокарты.

Блокнот вскрывался в строго определенных местах, длина разрезов была регламентирована. При нарушении правил вскрытия составлялся соответствующий акт. Такой порядок был обусловлен требованиями безопасности.

Ключевая таблица (суточного ключа) имела следующий вид.

И Д Ж З А	В К Г Б Е	I4
О С А Н Е	Р Т Ь Б Ы	
Б Д В И А	Г Е З К Ж	
2 I I 2 2	I 2 2 I 2	
К У Л К Ю	Ы Х В У Г	

Таблица суточного ключа для М-125-3М «Фиалка-3М»

где:

- 14 – число месяца, на которое действовала таблица (и соответствующая перфокарта)
- 1 строка – определяет порядок шифрдисков на оси.
- 2 строка – установку подвижных колес-ободов.
- 3 строка – какие модули проводки с какими дисками использовать.
- 4 строка (цифровая) – какой стороной укладывать модуль.
- 5 строка – положение модуля относительно диска.

Таким образом для первого шифрдиска (первый столбец). Берем диск «И», устанавливаем его обод в положение «О». Модуль Б устанавливаем стороной 2 (мы видим эту цифру) в положение «К». Вторым будет диск «Д» и т.д.

В некоторых типах блокнотов суточных ключей была и шестая строка из 10 букв. Для первоначальной установки шифрдисков при выработке ключей общей связи. Однако были и другие алгоритмы их выработки.

Для установки разового ключа использовались блокноты индивидуальной или циркулярной связи.

Блокнот ЦЗ-25 для входящих циркулярных телеграмм (для исходящих циркулярных всегда использовался экземпляр 1). Тип УП-5С, экземпляр 10, номер 119327, год выпуска 1979, гриф секретности «Совершенно секретно».



Блокнот циркулярной связи ЦЗ-25М

Из блокнота извлечены (использованы) 5 ключевых таблиц. Следующая – шестая имеет опознавательную группу ТРВБР. Собственно разовый ключ (установка шифрдисков при расшифровке): БЩЕББ АВАРВ.

В блокнотах такого типа, было как правило 40 ключей, необходимый выбирался по опознавательной групп

В конце 80-х годов, в документах ОВД, криптографическая стойкость «Фиалки» определялась сроком в 24 часа (в начале 80-х — трое суток). Определенных успехов в дешифровке закрытой этой машиной информации добилась и Австрия.

Однако по сравнению с ЗАС Т-217 «Эльбрус» или например, Т-219 «Яхта», которые читались в режиме реального времени, это было относительно не плохо.

В заключении, можно отметить, что М-125 «Фиалка-3М» добротная кодировочная машина. Ничуть не хуже, если не лучше, чем соответствующие образцы техники противника. Естественно, предназначенная для передачи сведений соответствующего грифа (степени) секретности

8. Шифровальная машина М-105 «Агат»

М-125-3М «Фиалка-3М», часто называемая шифровальной машиной, такой не являлась. «Фиалка» машина кодировочная, с большими ограничениями по степени секретности передаваемы сведений, ввиду недостаточной криптографической стойкости.

Основной шифровальной машиной, как Вооруженных Сил, так и других министерств и ведомств являлась М-105 «Агат», позволяющая обрабатывать информацию с грифом «Совершенно секретно».



Общий вид шифровальной машины М-105 «Агат»

Машина М-105 «Агат» была разработана во второй половине 60-х годов для замены во многом идентичной М-104 «Аметист». Тем не менее «Аметист» продолжал эксплуатироваться в некоторых сетях (например РВСН) еще довольно продолжительное время.

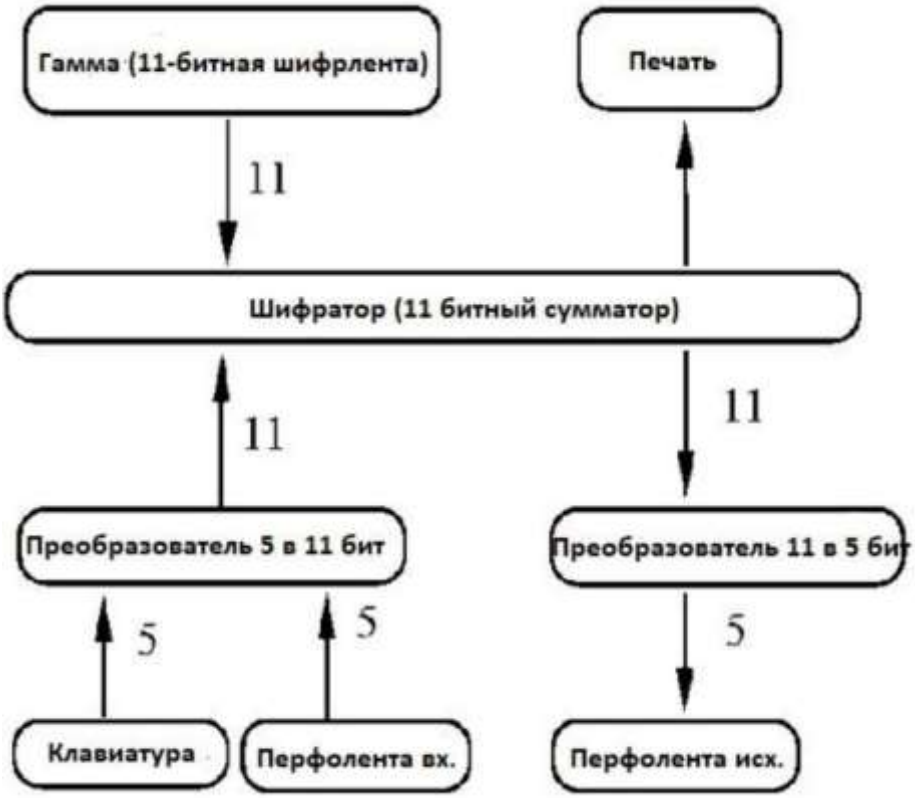


Шифровальная машина М-154-4М «Аметист»

Если бы потребовалось охарактеризовать «Агат» в двух словах, то наиболее подходящим выражением оказалось бы: «автомат Калашникова».

Можно услышать утверждение что М-105 «Агат» похожа на М-125 «Фиалка». Это абсолютно не так. Общее у них только покрытие молотковой эмалью.

Конструктивно М-105 представляет собой сумматор знаков открытого текста со знаками внешней гаммы, носителями которой являлись шифрленты.



Блок-схема шифровальной машины М-105 «Агат»

В криптографическом отношении «Агат» машинным путем реализовывает шифр Вернама (шифр гаммирования, шифр одноразовых блокнотов).

При соблюдении требований к гамме и правил работы обеспечивается гарантированная стойкость



Переключатель режима работы Установлен на З то есть зашифрование

Машина имеет три режима работы:

- «О» — открытый текст
- «З» — зашифрование
- «Р» — расшифрование.

Текст может вводиться как с клавиатуры, так и с перфоленты. Таким же образом осуществлялся вывод информации из машины (печать на бумагу или перфолента).

Электропитание осуществлялось через блок питания БП-24. Изготавливался вариант шифровальной машины с питанием от сети 110 вольт, в этом случае электродвигатель СЛ-369 заменялся на СЛ-369М.



М-105 М-105 «Агат» без верхней крышки. Ручной режим, вращение кривошипом

Была предусмотрена возможность работы без электропитания. На снимке видна ручка ручного привода. На передней стенке, в прорези переключатель «мотор-ручн.»

Справа от клавиатуры — трансмиттер перфоленты и клавиши «Пуск» и «Стоп». Две черные клавиши по краям нижнего ряда букв клавиатуры «Возврат каретки» и «Шаг каретки» предназначены для форматирования при работе открытым текстом и в процессе шифрования не участвуют.

Для исключения одновременного нажатия клавиш предусмотрен легатный механизм.

Предусмотрен только буквенный режим работы. Цифры и знаки препинания на клавиатуре отсутствуют. При необходимости, числа и знаки препинания набираются прописью.

На некоторых «зарубежных» модификациях, ввиду разницы между латинским (26 букв) и кириллическим (в данном случае 30 букв) алфавитами, вводились 4 дополнительных знака, как правило наиболее употребляемые цифры: 2, 5, 7, 8.

На фото машина находиться в режиме «З» зашифрование — клавиша «Й» (крайняя слева, в верхнем ряду) закрыта пластиной, следовательно «пробел» разблокирован. В режиме «Р» расшифрование все наоборот.



Переключатель ввода/вывода П, ПК, К шифровальной машины М-105

В режиме открытого текста «О» и «Й» и «пробел» доступны.

Трансмиттер шифратора предназначен для ввода внешней гаммы в шифратор/сумматор.

На передней стенке виден рычажок переключения режима ввода/вывода:

- «П» — перфолента
- «ПК» — перфолента/каретка
- «К» только каретка (печать).

«Колесико» на передней стенке предназначено для ручного (пошагового) продвижения шифрленты.

На верхней поверхности машины видна линейка. Такое же «колесико» и линейка имеются и у трансмиттера перфоленты. Назначение этих устройств – поиск «сбоев» при расшифровании.



Шифрлента заправлена в трансмиттер шифратора М-105

Для печати используется координатная головка матричного типа на 30 букв. Координаты задаются в 11 битном коде, 5 столбцов и 6 строк.

	0	1	2	3	4
0	Ю	Ы	Щ	А	Ч
1	Ь	И	О	С	М
2	Н	Е	Ф	Ш	В
3	З	Я	Г	Х	Ц
4	Б	Й	Р	К	Ж
5	Д	У	Л	Т	П

Схема печатной матрицы машины М-105

Таким образом буква «Я» будет иметь следующее значение 01000 000100

Пятидорожечная перфолента имеет возможность задать 32 значащие комбинации. Две из них 10001 и 00000 имеют значение «пробел» и «стоп»

Для исключения случаев двойного использования гаммы, в результате ошибки оператора, предусмотрено контрольно-блокировочное устройство. При переходе в режим «З» на шифрленте пробивалось контрольное отверстие.

Отверстие делало невозможным повторное использование данной шифрленты в режиме зашифрования.

Шифрленты предназначенные только для расшифровки (например, при циркулярной связи) имели контрольное отверстие, пробитое при изготовлении.
Это дает возможность проверить расшифровкой, зашифрованный текст перед отправкой.
В принципе, каждый оператор знает, как обойти это КБУ, однако оно защищает от случайной ошибки, а не преднамеренного нарушения.



Шифрлента (носитель гаммы) для шифровальной машины М-105 «Агат»

Шифрлента имеет 11 дорожек (+2 ведущие).
Первые пять (снизу, до первой ведущей дорожки) соответствуют столбцам.
Шесть дорожек (между ведущими дорожками) соответствуют строкам. Необходимая шифрлента, выбирается по показательной группе (в таблице) и соответствующему номеру.
Шифрленты находятся в блокнотах по 20 штук.
Основные типы блокнотов:

- ТИ — для индивидуальной связи
- ТЦ — для связи циркулярной
- Т-КПУ-М — проверочный блокнот

Шифровальная машина М-105 «Агат» сложнейшее электромеханическое устройством, с массой самых разнообразных регулировок.
Тщательная конструкторская проработка и отработанная технология сделали ее, вероятно самой надежной в ВС СССР.

9. Шифровальная машина М-205

К середине 60-х годов прошлого века в связи с развитием компьютерных технологий стало ясно что электромеханические машины уже в обозримом будущем не смогут обеспечить необходимую степень защиты передаваемой информации.



Шифровальная машина М-205 «Уран-2М» Исполнение D для ГДР

Внедрение АСУВ разного уровня увеличивало потоки информации, подлежащей закрытию. Происходил постоянный рост количества шифровальных органов, что только усугубляло и без того не простую задачу обеспечения корреспондентов ключевой документацией.
Одним из путей решения возникших проблем явилось создание шифровальной/кодировочной техники с электронным шифратором.
В конце 70-х/начале 80-годов был разработан ряд образцов специальной техники третьего поколения (М-200, М-201, М-204, М-464 и др.). Были созданы и стали производится АРМ шифровальщика, вплоть до полкового звена.
В качестве основной шифровальной машины, призванной заменить М-105 «Агат», была выбрана М-205, впервые представленная «широкой публике» в 1983 году.



Шифровальная машина М-205D «Уран-2М» с поднятой крышкой

В открытом доступе информации про нее практически нет, а имеющаяся относится к исполнению М-205D, предназначенному для Германской Демократической Республики.

Интересно, что на фото выше видно, что узел печати был изменен и вместо матрицы использовано шаровое печатающее устройство.

Ввиду высокой стоимости М-205D – 175 тыс. марок (около 70 000 руб.) МИД ГДР отказался от ее использования в зарубежных представительствах.

Другим фактором, повлиявшим на принятие данного решения, стало то, что скорость обработки увеличилась всего на 25%.

Технические характеристики изделия М-205D	
Напряжение питания, В	
БП УД-16 (встроенный)	220
БП УД-17 (внешний)	22,8-29,7
Выходное напряжение	5, 15, 27
Вес без упаковки, кг	
Машина	28,5
БП УД-17	8,0
Температура эксплуатации, ^{0}C	
При влажности 65±15%	0...+50 (до -10)
При влажности 98%	до +35
Температура хранения	-50...+65^{0}C
Вибрации	до частоты 60 Гц
Скорость обработки	600 знак/мин.

ТТХ шифровальной машины М-205D «Уран-2М»

С 1986 г. эта шифровальная машина стала использоваться для автоматизированного обмена с ПК ЕС 1835F2 являющегося частью системы шифрования и кодирования данных Т-330 «KENDO». Данная система обладала достаточно высокой скоростью шифрования — более 1 Мбит/сек.

Шифровальная машина М-205D имела развитую ключевую систему.

Разовые (сеансовые) ключи – кассеты (шифрблокноты) УМИ и УМЦ для индивидуальной и циркулярной связи соответственно.

Суточные ключи – кассеты УМС.



Кассета (шифрблокнот) для шифровальной техники третьего поколения



Ключевая лента

Ключевая кассета (блокнот) и ключ для М-205 «Уран-2М»

Долговременные ключи — для настройки коммутаторов блокноты УМД, для КС-А типа УКД.

Для обеспечения общей связи использовался ключ-маркант. Как правило, маркант необходим для обеспечения одноразовости (уникальности) гаммы, вырабатываемой при каждом шифровании. Другими словами, для гарантии отсутствия ее перекрытия.

Длина суточного ключа составляла 125 бит, такую же длину имел и долговременный ключ,

Длина ключа-марканта 50 бит.

В машине использовался электронный шифратор А-10. Обеспечивалась возможность поддержания сети на 500 абонентов

Шифровальная машина М-205D и ключевая документация к ней, были скомпрометированы во время аннексии ГДР Федеративной Республикой.

Кроме того, практически все образцы советской шифровальной техники были вывезены сотрудниками ЦРУ и АНБ из Чехословакии.

В заключение, можно упомянуть еще об одном простом электронном шифраторе, который разрабатывался для нарядов пограничных войск на базе программируемого калькулятора «Электроника-85».



Простейший шифратор «Электроника-85С» на базе калькулятора

Разработчики утверждают, что именно он спас ЦБ от разорения, а страну от коллапса., во время эпидемии т.н. «чеченских» авизо.