**СРСП 6. Шифровальная машина Фиалка(М-125).**

**Форма и содержание отчета**

Отчет должен содержать:

1. Титульный лист установленного образца.
2. Описание комплексного поиск возможных методов доступа.
3. Сравнительный анализ рассмотренных терминалов защищенной информационной системы.
4. Перечень использованных информационных источников.

Отчет выполняется на листах формата А4 рукописным или печатным способом. При рукописном оформлении отчета текст следует излагать четким почерком чернилами черного цвета.

**Фиалка (М-125)** — шифровальная машина, разработанная в [СССР](https://ru.wikipedia.org/wiki/%D0%A1%D0%BE%D1%8E%D0%B7_%D0%A1%D0%BE%D0%B2%D0%B5%D1%82%D1%81%D0%BA%D0%B8%D1%85_%D0%A1%D0%BE%D1%86%D0%B8%D0%B0%D0%BB%D0%B8%D1%81%D1%82%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%B8%D1%85_%D0%A0%D0%B5%D1%81%D0%BF%D1%83%D0%B1%D0%BB%D0%B8%D0%BA) вскоре после [Второй мировой войны](https://ru.wikipedia.org/wiki/%D0%92%D1%82%D0%BE%D1%80%D0%B0%D1%8F_%D0%BC%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D1%8F_%D0%B2%D0%BE%D0%B9%D0%BD%D0%B0). Использовалась странами [Варшавского договора](https://ru.wikipedia.org/wiki/%D0%9E%D1%80%D0%B3%D0%B0%D0%BD%D0%B8%D0%B7%D0%B0%D1%86%D0%B8%D1%8F_%D0%92%D0%B0%D1%80%D1%88%D0%B0%D0%B2%D1%81%D0%BA%D0%BE%D0%B3%D0%BE_%D0%B4%D0%BE%D0%B3%D0%BE%D0%B2%D0%BE%D1%80%D0%B0) до 1990-х годов. Большая часть машин после распада СССР была разобрана или уничтожена. Несколько экземпляров хранятся в частных коллекциях и музеях. Работающая модель представлена в [Музее компьютерной истории](https://ru.wikipedia.org/wiki/%D0%9C%D1%83%D0%B7%D0%B5%D0%B9_%D0%BA%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D0%BE%D0%B9_%D0%B8%D1%81%D1%82%D0%BE%D1%80%D0%B8%D0%B8) (Computer History Museum) в США и [Блетчли-Парке](https://ru.wikipedia.org/wiki/%D0%91%D0%BB%D0%B5%D1%82%D1%87%D0%BB%D0%B8-%D0%9F%D0%B0%D1%80%D0%BA) (Bletchley Park) в Великобритании. В истории [криптографии](https://ru.wikipedia.org/wiki/%D0%9A%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%8F) мало что известно о Фиалке, до 2005 года вся информация об устройстве держалась в секрете. Правильное определение "Фиалки" — кодировочная машина, поскольку она обладала более слабой криптостойкостью, чем шифровальные машины.

Фиалка содержит устройство считывания с бумажной [перфоленты](https://ru.wikipedia.org/wiki/%D0%9F%D0%B5%D1%80%D1%84%D0%BE%D0%BB%D0%B5%D0%BD%D1%82%D0%B0_%28%D0%BD%D0%BE%D1%81%D0%B8%D1%82%D0%B5%D0%BB%D1%8C_%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%B8%29) справа, если смотреть спереди машины, а сверху — устройство для печати и для перфорирования ленты. Устройство вставки перфоленты для ввода ключа находится слева. Фиалка питается от источника постоянного тока напряжением 24 В, а через отдельный блок питания — от сети переменного тока 100…250 В, 50 или 400 Гц

## **Механизм шифрования**

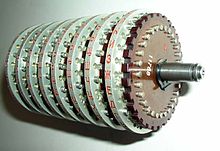
Как и другие роторные машины, Фиалка состояла из комбинации механических и электрических подсистем. Механическая часть включала в себя клавиатуру, набор вращающихся дисков — роторов, — которые были расположены вдоль вала и прилегали к нему, и ступенчатого механизма, двигающего один или несколько роторов при каждом нажатии на клавишу. Движение роторов приводит к различным криптографическим преобразованиям при каждом следующем нажатии на клавишу на клавиатуре. Механические части двигались, замыкая контакты и образуя меняющийся электрический контур (то есть, фактически, сам процесс шифрования букв реализовывался электрически). При нажатии на клавишу [клавиатуры](https://ru.wikipedia.org/wiki/%D0%9A%D0%BB%D0%B0%D0%B2%D0%B8%D0%B0%D1%82%D1%83%D1%80%D0%B0) контур замыкался, ток проходил через различные цепи и в результате получалась искомая буква кода.

Сам по себе ротор производил очень простой тип шифрования: элементарный [шифр замены](https://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80_%D0%B7%D0%B0%D0%BC%D0%B5%D0%BD%D1%8B). Например, контакт, отвечающий за букву E, мог быть соединён с контактом буквы T на другой стороне ротора. Но при использовании нескольких роторов в связке за счёт их постоянного движения получается более надёжный [шифр](https://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80).[[3]](https://ru.wikipedia.org/wiki/%D0%A4%D0%B8%D0%B0%D0%BB%D0%BA%D0%B0_%D0%9C-125#cite_note-second-3) Так же шифрование происходило в электронном блоке под названием "комутатор", который имел 30х30 контактов. код в комутаторе набирался путём вставки перфокарты. Согласно отверстиям в перфокарте замыкались контакты и производилась замена символа по аналогии с шифродисками (ротор).

## Роторы

[](https://commons.wikimedia.org/wiki/File:FIALKA-rotors-in-machine.jpg?uselang=ru)

10 роторов

[](https://commons.wikimedia.org/wiki/File:FIALKA-rotors-closeup-on-shaft.jpg?uselang=ru)

набор роторов, показаны 30 контактов

В центре каждой машины Фиалка 10 различных кодировочных колес (роторов), помеченных буквой русского алфавита именно:

А(1) Б(2) В(3) Г(4) Д(5) Е(6) Ж(7) З(8) И(9) К(10)

Каждый ротор представлял собой диск примерно 10 см в диаметре, сделанный из эбонита или бакелита, с 30 пружинными штыревыми контактами на одной стороне ротора, расположенными по окружности. На другой стороне находилось соответствующее количество плоских электрических контактов. Штыревые и плоские контакты соответствовали буквам в алфавите. Не учитывались буквы "Ё", "Й" и "Ъ". При соприкосновении контакты соседних роторов замыкали электрическую цепь.

Коллекцию из этих 10 уникальных колес иногда называют «Протон». Есть два различных типа колеса: фиксированные и регулируемые. Фиксированные колеса были введены ранее для М-125-хх модели, в то время как регулируемые колеса были введены для M-125-3xx модели в 1978 году. В регулируемых наборах можно менять настройки внешнего кольца, тем самым получая 30 возможных позиций. Существенное отличие Фиалки от других роторных машин - каждый из роторов вращается в направлении противоположном соседним.

Различные наборы колес были выпущены для разных стран Варшавского договора. Известно значение нескольких префиксов:

3K: Польша

4K: Восточная Германия

6K: Чехословакия

0K: Общие проводки для всех стран в случае войны

1K: СССР

На крышке устройства находился запасной ротор.[[1]](https://ru.wikipedia.org/wiki/%D0%A4%D0%B8%D0%B0%D0%BB%D0%BA%D0%B0_%D0%9C-125#cite_note-first-1)[[3]](https://ru.wikipedia.org/wiki/%D0%A4%D0%B8%D0%B0%D0%BB%D0%BA%D0%B0_%D0%9C-125#cite_note-second-3)

### Рефлектор

Как и в [Энигме](https://ru.wikipedia.org/wiki/%D0%AD%D0%BD%D0%B8%D0%B3%D0%BC%D0%B0), в Фиалке использовался рефлектор, соединяющий пары проводов вместе. Наличие рефлектора гарантировало, что осуществляемое преобразование есть [инволюция](https://ru.wikipedia.org/wiki/%D0%98%D0%BD%D0%B2%D0%BE%D0%BB%D1%8E%D1%86%D0%B8%D1%8F_%28%D0%BC%D0%B0%D1%82%D0%B5%D0%BC%D0%B0%D1%82%D0%B8%D0%BA%D0%B0%29), то есть дешифрование представляет собой то же самое, что и [шифрование](https://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5). Однако в Энигме наличие рефлектора делает невозможным шифрование какой-либо буквы через саму себя. В Фиалке этот недостаток устранен.

Из 30 контактов, 26 соединены друг с другом в парах, но есть 4 «специальных» провода. Один провод используется для замены зашифрованной буквы на оригинальную. Это приводит к тому, что в 1 из 30 случаев буква закодирована сама в себя. Другие 3 провода подключены к транзисторной схеме (так называемый Magic Circuit) и образуют вращающийся переключатель. В режиме кодирования контакт "x" подается на выход через "y", "y" через "z", "z" через "х". В режиме декодирования контакты "z" и "y" меняются местами.[[3]](https://ru.wikipedia.org/wiki/%D0%A4%D0%B8%D0%B0%D0%BB%D0%BA%D0%B0_%D0%9C-125#cite_note-second-3)

### Ключ-карта

Для усиления криптографической стойкости машины, у Фиалки применялась специальная общая суточная карточка в виде [перфокарты](https://ru.wikipedia.org/wiki/%D0%9F%D0%B5%D1%80%D1%84%D0%BE%D0%BA%D0%B0%D1%80%D1%82%D0%B0). Каждая перфокарта имела 30 отверстий — ровно одно отверстие в строке и в столбце, и тем самым определяла перестановку для 30 роторных линий контакта. Использовалась в определенный день, указанный в левом верхнем ряду. Немного оригинальных перфокарт выжили, так как — в соответствии с протоколом — все они уничтожались по окончании текущих суток.

Карточки были созданы СССР для всех стран Варшавского договора и ежедневно менялись. Каждая страна имела свою собственную уникальную колоду карт, каждая сроком на один месяц. Вместо перфокарты можно было использовать металлический треугольник. Треугольная пластина определяла нулевую перестановку, часто использовалась для проверки работоспособности машины.

Так же на каждый день была своя ключевая таблица. Для фиксированных роторных систем, ключевые таблицы определяют порядок роторов на оси и параметры начального ротора, которые будут использоваться для расшифровки сообщения. Для регулируемых роторов, в таблице также определяется электрическую вставку для каждого ротора. Вот пример для машины M-125-3NM для использования на 14-е число месяца:

ИДЖЗА ВКБГЕ 14

OCAHE PTБВЕ

БДВИА ГЕЗКЖ

2II22 I22I2

КУЛКЮ ЫХВУГ

Ключ не использовался более одних суток и обновлялся в 00:01 часов