**Лекция-5.** **Шифровальная машина М-209 (Хагелин).**

* 1. Инструкция по работе с машиной
	2. Внутренниеиэлементы
		1. Обзор
		2. Пример настройки М-209
		3. Пример шифрования
	3. Производство и использование
	4. Криптостойкость

В [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) **М-209**, так же известная как **CSP-1500** и **C-38** — это портативная механическая шифровальная машина, первоначально использовавшаяся армией США во [Второй мировой войне](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). Она так же активно использовалась и в течение [Корейской войны](https://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D1%80%D0%B5%D0%B9%D1%81%D0%BA%D0%B0%D1%8F_%D0%B2%D0%BE%D0%B9%D0%BD%D0%B0). M-209 — это улучшенная версия шифровальной машины [C-36](https://ru.wikipedia.org/w/index.php?title=C-36_(%D1%88%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%B0%D0%BB%D1%8C%D0%BD%D0%B0%D1%8F_%D0%BC%D0%B0%D1%88%D0%B8%D0%BD%D0%B0)&action=edit&redlink=1).

Линейные размеры М-209: 83×140×178 мм (3,25×5,5×7 [дюймов](https://ru.wikipedia.org/wiki/%D0%94%D1%8E%D0%B9%D0%BC)). Эта машина была отличным решением для неэлектронной технологии. В ней используется колёсная схема, похожая на те, что используются в [машине Лоренца](https://ru.wikipedia.org/wiki/%D0%9C%D0%B0%D1%88%D0%B8%D0%BD%D0%B0_%D0%9B%D0%BE%D1%80%D0%B5%D0%BD%D1%86%D0%B0) и в машине [SFM](https://ru.wikipedia.org/w/index.php?title=Siemens_and_Halske_T52&action=edit&redlink=1).



*Рисунок 1. Хагелин М-209.*

**Инструкция по работе с машиной**

Принцип работы М-209 относительно прямолинеен. В верхней части машины находятся подвижные ***роторы***. Эти роторы имеют дискретное количество положений. Каждому положению соответствует одна буква английского алфавита. Начальное положение роторов определяет **внешний**[**ключ**](https://ru.wikipedia.org/wiki/%D0%9A%D0%BB%D1%8E%D1%87_%28%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%8F%29).

Чтобы зашифровать сообщение, оператор выставляет *кнопку шифрование-расшифрование* в положение *шифрование*. Ставит роторы в некоторое начальное положение. Затем устанавливает *индикаторный диск*, расположенный слева, в положение, соответствующее первой букве сообщения. Поворачивает *рукоятку* в правой части машины, в результате чего зашифрованная буква печатается на бумажной ленте, роторы поворачиваются на одно положение и машина вновь готова к вводу следующей буквы сообщения. Вместо пробела в шифре используется буква «Z». Пока не введена следующая буква *рукоятка* справа блокируется. Повторяя данную процедуру для остальных букв сообщения, получаем [шифротекст](https://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80%D0%BE%D1%82%D0%B5%D0%BA%D1%81%D1%82%22%20%5Co%20%22%D0%A8%D0%B8%D1%84%D1%80%D0%BE%D1%82%D0%B5%D0%BA%D1%81%D1%82), который затем можно передавать. Оператор, принимающий шифр должен знать [ключ](https://ru.wikipedia.org/wiki/%D0%9A%D0%BB%D1%8E%D1%87_%28%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%8F%29) чтобы расшифровать сообщение. К примеру, можно брать каждый день ключи из некоторой книги, которая есть у обеих сторон.

[Шифротекст](https://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80%D0%BE%D1%82%D0%B5%D0%BA%D1%81%D1%82) автоматически печатается группами по пять символов для удобочитаемости. Машина снабжена *счётчиком букв*, который показывает номер текущей буквы, шифруемой или дешифруемой. Он может быть полезен, если оператор сбился при шифровании или дешифровании.

Дешифрование производится почти также, как и шифрование; оператор устанавливает кнопку шифрование-расшифрование в положение «расшифрование» и устанавливает роторы в то же самое начальное положение что и при шифровании. Индикаторный диск устанавливается в положение, соответствующее первой букве [шифротекста](https://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80%D0%BE%D1%82%D0%B5%D0%BA%D1%81%D1%82%22%20%5Co%20%22%D0%A8%D0%B8%D1%84%D1%80%D0%BE%D1%82%D0%B5%D0%BA%D1%81%D1%82). Затем оператор вращает рукоятку, в результате чего поворачиваются роторы и печатается расшифрованная буква. Если в [шифротексте](https://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80%D0%BE%D1%82%D0%B5%D0%BA%D1%81%D1%82%22%20%5Co%20%22%D0%A8%D0%B8%D1%84%D1%80%D0%BE%D1%82%D0%B5%D0%BA%D1%81%D1%82) встречается буква «Z» то печатается [пробел](https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D0%B1%D0%B5%D0%BB). Отсутствующие «Z» расставляются оператором на основе контекста.

Опытный оператор машины М-209 тратил от двух до четырёх секунд на шифрование/расшифрование одной буквы, так машина работала довольно быстро.

После шифрования сообщения, оператор переписывал его на лист из *книги сообщений*.

**Внутренние элементы**

Внутри М-209 возникает гораздо более сложная картина. Каждой букве на каждом роторе соответствует *подвижный штырь*. Эти штыри могут быть в *активном* и *неактивном* положениях. Если они сдвинуты влево — то это *активное*положение, если вправо — то *неактивное*. Позицию подвижных штырей выставляет оператор.



*Рисунок 2. Роторы*

Видно, в каких положениях может находиться управляющий рычаг, в зависимости от того взаимодействует он с активными или не активными штырями.



*Рисунок 3. Взаимодействия роторов и барабана*

Слева управляющий рычаг взаимодействует с активным штырём. Поэтому он не касается насадок на спицах. Справа управляющий рычаг не взаимодействует с активными штырями, поэтому когда вращается барабан, управляющий рычаг может взаимодействовать с насадками на спицах, тем самым сдыигая их(спицы).

Каждое роторное колесо содержит разное количество букв и, соответственно, разное количество штырей. Слева направо роторы имеют:

* 26 букв, от A да Z
* 25 букв, от A до Z, кроме W
* 23 буквы, от A до X, кроме W
* 21 буква, от A до U
* 19 букв, от A до S
* 17 букв, от A до Q

Количества букв выбраны [взаимно простыми](https://ru.wikipedia.org/wiki/%D0%92%D0%B7%D0%B0%D0%B8%D0%BC%D0%BD%D0%BE_%D0%BF%D1%80%D0%BE%D1%81%D1%82%D1%8B%D0%B5_%D1%87%D0%B8%D1%81%D0%BB%D0%B0) чтобы увеличить период комбинаций для внешнего [ключа](https://ru.wikipedia.org/wiki/%D0%9A%D0%BB%D1%8E%D1%87_%28%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%8F%29). Этот период равен 26×25×23×21×19×17 = 101 405 850. Каждый ротор может взаимодействовать с *управляющим рычагом* посредством штырей. На каждый ротор приходится один управляющий рычаг, который может иметь два положение *активное* и *не активное*. Активное — когда он взаимодействует с активным штырём, не активное — с не активным штырём. Состояния штырей являются первой частью внутреннего ключа М-209.

За роторами расположен цилиндрический барабан с горизонтальными *спицами* в количестве 27 штук. На каждой спице закреплены по две *насадки*; каждая насадка может быть расположена в одном из восьми положений: шесть положений соответствуют роторам и два положения — нейтральные. Штыри в эффективном состоянии заставляют соответствующий управляющий рычаг перейти в активное состояние и взаимодействовать со спицами на барабане. Положения насадок являются второй частью внутреннего ключа М-209. Устанавливать внутренний ключ — довольно сложно, поэтому это делалась относительно нечасто, обычной практикой было менять внутренний ключ раз в день.

Когда оператор поворачивает рукоятку, цилиндрический барабан делает полный оборот. Если насадка на какой, либо спице касается управляющего рычага, то спица, на которую насажена эта насадка, сдвигается влево; насадки в нейтральных позициях никогда не взаимодействуют с управляющими рычагами. Спицы, которые были сдвинуты влево образуют образуют [шестерёнку](https://ru.wikipedia.org/wiki/%D0%97%D1%83%D0%B1%D1%87%D0%B0%D1%82%D0%BE%D0%B5_%D0%BA%D0%BE%D0%BB%D0%B5%D1%81%D0%BE) с переменным количеством зубьев. На бумажную ленту печатается буква, сдвинутая по алфавиту именно на это число зубьев.

После того как цилиндрический барабан совершил оборот *рефрактор* возвращает сдвинутые спицы обратно, а *промежуточная передача* поворачивает роторы на одну позицию; затем срабатывает блокирующая защёлка, которая не даёт вращать барабан до введения новой буквы.

В каждой итерации сдвиг буквы разный; без этого шифр бы напоминал [шифр Цезаря](https://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80_%D0%A6%D0%B5%D0%B7%D0%B0%D1%80%D1%8F).

### **Пример настройки М-209**

Перед началом шифрования оператор М-209 должен настроить машину. Настройка заключается в установлении положений штырей на всех шести роторах и в установлении позиций насадок на спицах; обычно эти настройки определялись секретными таблицами, которые давались отправителю и получателю. Начальное положение роторов выбиралось отправителем произвольно и передавалось получателю по секретному каналу связи.

Каждой букве на роторе соответствует штырь, который может быть выставлен в активное или неактивное положение. Таблица, описывающая состояния штырей, может выглядеть следующим образом:

|  |  |
| --- | --- |
| **Ротор** | **Состояния штырей** |
| 1 | AB-D---HI-K-MN----ST-VW--- |
| 2 | A--DE-G--JKL--O--RS-U-X-- |
| 3 | AB----GH-J-LMN---RSTU-X |
| 4 | --C-EF-HI---MN-P--STU |
| 5 | -B-DEF-HI---MN-P--S |
| 6 | AB-D---H--K--NO-Q |

*Рисунок 4. Состояния штырей*

Штыри, соответствующие буквам, которые приведены в таблице, выставляются в активное положение, остальные в неактивное.

Цилиндрический барабан имеет 27 спиц, на каждой спице имеется по две *насадки*. Эти насадки могут быть установлены в любое из восьми положений, 6 из которых соответствуют роторам и два нейтральные. Таблица 1 содержащая информацию о положениях может выглядеть следующим образом:

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Спица** | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** |
| **Насадки** | 3-6 | 0-6 | 1-6 | 1-5 | 4-5 | 0-4 | 0-4 | 0-4 | 0-4 |
| **Спица** | **10** | **11** | **12** | **13** | **14** | **15** | **16** | **17** | **18** |
| **Насадки** | 2-0 | 2-0 | 2-0 | 2-0 | 2-0 | 2-0 | 2-0 | 2-0 | 2-0 |
| **Спица** | **19** | **20** | **21** | **22** | **23** | **24** | **25** | **26** | **27** |
| **Насадки** | 2-0 | 2-5 | 2-5 | 0-5 | 0-5 | 0-5 | 0-5 | 0-5 | 0-5 |

*Таблица 1. Положение насадки*

На спице 1 нужно выставить насадки в положения «3» и «6», на спице 2 в положения «0» и «6» и так далее.

Наконец, внешний ключ устанавливается вращением роторов в определённую или произвольную последовательность букв. Для проверки того, что внутренний ключ был установлен правильно, оператор устанавливал роторы в положение «АААААА» и выполнял шифрование сообщения, состоящего только из букв «А», затем сравнивал полученную зашифрованную последовательность с уже имеющейся *проверочной строкой*. Для приведённой выше конфигурации внутреннего ключа проверочная строка выглядит следующим образом:

T N J U W A U Q T K C Z K N U T O T B C W A R M I O

Штыри на роторах вступают в игру, когда соответствующие им буквы проходят через нижнее положение во время вращения; в данном случае, для комбинации роторов «AAAAAA» это буквы «PONMLK», слева направо.

### **Пример шифрования**

После того, как М-209 настроена как показано выше, машина готова к шифрованию. Продолжим пример шифрования *проверочной строки*. Первая буква из сообщения для шифрования — «А». Оператор устанавливает *индикаторный диск* в положение, соответствующее букве «А» и поворачивает *рукоятку*. Комбинация на роторах «AAAAAA», а противоположные им буквы «PONMLK»; из приведённых выше таблиц видно, что штыри около букв «O», «N», «M», «K» — в активном состоянии, а штыри около «P» и «L» — в неактивных состояниях. Следовательно, управляющие рычаги с номерами 2, 3, 4 и 6 будут в активном состоянии. Во время вращения цилиндрического барабана, каждая спица с насадкой в одном из этих позиций будет сдвинута влево. Из таблицы для барабана видно, что сдвинутся влево спицы с номерами 1, 2, 3 и с 5 по 21. То есть всего 20 спиц. В [шестерёнке](https://ru.wikipedia.org/wiki/%D0%97%D1%83%D0%B1%D1%87%D0%B0%D1%82%D0%BE%D0%B5_%D0%BA%D0%BE%D0%BB%D0%B5%D1%81%D0%BE) с переменным количеством зубьев будет ровно 20 зубьев. В шифровании этой буквы будет использоваться сдвиг на 20 букв. M-209 использует частный случай [шифра подстановки](https://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80_%D0%BF%D0%BE%D0%B4%D1%81%D1%82%D0%B0%D0%BD%D0%BE%D0%B2%D0%BA%D0%B8) [шифр Бьюфорта](https://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80_%D0%91%D1%8C%D1%8E%D1%84%D0%BE%D1%80%D1%82%D0%B0). Который сначала отображает алфавит на этот же алфавит, но записанный в обратном порядке:

|  |  |
| --- | --- |
| *Исходный алфавит:* | ABCDEFGHIJKLMNOPQRSTUVWXYZ |
| *Алфавит шифротекста:* | ZYXWVUTSRQPONMLKJIHGFEDCBA |

*Таблица 2. Алфавит*

Если сдвиг равен нулю, то «A» отображается в «Z», «B» в «Y», «C» в «X» и так далее. Если сдвиг не равен нулю, то сдвигаем букву влево на соответствующее число позиций. Сдвиг происходит циклически, то есть достигнув левого края мы переходим на правый. Зашифруем букву «P» со сдвигом 3. «P» отображается в «K», затем сдвигаем на 3 позиции влево, получаем «N». Продолжим наш пример с «A». «A» отображается в «Z» и затем сдвигается влево на 20 позиций. Получаем «T» что и видим в *проверочной строке*.

**Производство и использование**

В 1938 году фирма Бориса Хагелина выпустила шифровальную машину, которая называлась [C-38](https://ru.wikipedia.org/w/index.php?title=C-38&action=edit&redlink=1). Она предназначалась для использования швейцарской армией, но не получила широкого распространения. В 1940 году Хагелин тайно переправил несколько экземпляров в США. Там машину слегка модифицировали, переименовали в М-209 и пустили в массовое производство. Один экземпляр стоил порядка 64 долларов. (см.[[2]](http://derekbruff.com/site/fywscrypto/files/2010/11/Rice-Essay-2.pdf))

В течение Второй мировой войны разными компаниями было произведено более 140000 экземпляров М-209. Так же выпускались модификации: М-209-А, М-209-В, CSP-1500 (версия для флота). Во время [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) немецкий криптограф [Фриц Менцер](https://ru.wikipedia.org/w/index.php?title=%D0%9C%D0%B5%D0%BD%D1%86%D0%B5%D1%80,_%D0%A4%D1%80%D0%B8%D1%86&action=edit&redlink=1) построил шифровальную машину на основе М-209. Машина называлась [SG-41](https://ru.wikipedia.org/w/index.php?title=SG-41&action=edit&redlink=1) ([*нем.*](https://de.wikipedia.org/wiki/Schl%C3%BCsselger%C3%A4t_41)), она была чисто механической, внутри организована как М-209, но была больше и имела клавиатуру.

После войны Хагелин разработал улучшенную версию М-209; она известна под названием [С-52](https://ru.wikipedia.org/w/index.php?title=%D0%A1-52&action=edit&redlink=1). Её особенностями были: период 2,756,205,443, роторы можно было удалять и переставлять в любом порядке.

**Криптостойкость. Шифра и возможности восстоновление ключа.**

М-209 была хороша для своего времени, но отнюдь не совершенна. К началу 1943 года немецкие криптоаналитики уже умели читать сообщения, зашифрованные машиной М-209 (см. [[1]](http://www.heise.de/tp/r4/html/result.xhtml?url=/tp/r4/artikel/18/18371/1.html&words=M%20209)). Но ввиду того, что машина не требовала электрической энергии и имела малый вес, она хорошо подходила для тактического применения. Впоследствии она так же использовалась армией США в [Корейской войне](https://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D1%80%D0%B5%D0%B9%D1%81%D0%BA%D0%B0%D1%8F_%D0%B2%D0%BE%D0%B9%D0%BD%D0%B0).

В 1970-х годах американский исследователь [Деннис Ритчи](https://ru.wikipedia.org/wiki/%D0%A0%D0%B8%D1%82%D1%87%D0%B8%2C_%D0%94%D0%B5%D0%BD%D0%BD%D0%B8%D1%81%22%20%5Co%20%22%D0%A0%D0%B8%D1%82%D1%87%D0%B8%2C%20%D0%94%D0%B5%D0%BD%D0%BD%D0%B8%D1%81) совместно с [Робертом Моррисом](https://ru.wikipedia.org/wiki/%D0%9C%D0%BE%D1%80%D1%80%D0%B8%D1%81%2C_%D0%A0%D0%BE%D0%B1%D0%B5%D1%80%D1%82) и [Джимом Ридсом](https://ru.wikipedia.org/w/index.php?title=%D0%A0%D0%B8%D0%B4%D1%81,_%D0%94%D0%B6%D0%B8%D0%BC&action=edit&redlink=1) описал атаку на [шифротекст](https://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80%D0%BE%D1%82%D0%B5%D0%BA%D1%81%D1%82%22%20%5Co%20%22%D0%A8%D0%B8%D1%84%D1%80%D0%BE%D1%82%D0%B5%D0%BA%D1%81%D1%82) М-209, которая позволяла дешифровать сообщения длинной около 2000—2500 символов. Ритчи рассказывает, что после дискуссии с [АНБ](https://ru.wikipedia.org/wiki/%D0%90%D0%B3%D0%B5%D0%BD%D1%82%D1%81%D1%82%D0%B2%D0%BE_%D0%BD%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%B0%D0%BB%D1%8C%D0%BD%D0%BE%D0%B9_%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D0%B8), авторы решили не публиковать работу, так как машина всё ещё использовалась иностранными государствами.