**СРСП 4.** Аналоги шифровальных машин Энигмы.

**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.

О легендарной шифровальной машине Тьюринга и немецкой "Энигма" знают все, кто хоть немного увлекается военной техникой или, как я, смотрел фильм «Игра в имитацию».  Сложно представить, что в СССР были аналоги этих машин, тем не менее «Кристалл» К-37, «Спектр» М-100 и «Фиалка» М-125 были незаменимой техникой,  позволившей в 5-6 раз по сравнению с ручным способом повысить скорость обработки зашифрованных телеграмм.



К началу 1930-х годов стало ясно, что имеющиеся ручные системы шифрования и кодирования текстов, сколько их ни модернизируй, не справляются с постоянно возрастающим потоком информации. К примеру, для шифрования приказа или распоряжение объёмом в 1, 5 страницы уходило 3-4 часа, для его расшифровки ровно столько же. Понятно, что низкая скорость обработки информации «тормозила» работу советской власти и военных подразделений. Первым электромеханическим шифратором в СССР стала аппаратура засекречивания телефонных переговоров, выпущенная в 1927–28 годы. Но это достижение не облегчило работу государственным служащим, поэтому вопрос о создании подобной отечественной техники вновь был поднят шифровальщиками-моряками.



В 1931 году в технической лаборатории шифровальной службы под руководством И.П. Волоска были разработаны и изготовлены 2 образца советской шифровальной машины. Автор дал ей прозрачное наименование ШМВ-1 (Шифровальная машина Волоска – 1). Но громоздкая и механически ненадёжная шифрмашина в серию не пошла. Зато на заводе № 209 (впоследствии имени А.А. Кулакова) была создана научно-производственная структура по разработке и выпуску техники особой секретности. Весь 1936 год ушёл на разработку конструкции будущего устройства, а через год подготовлена вся документация на шифровальную машину В-4. Эта  техника была проста в использовании и имела минимальный набор органов управления. Поэтому вскоре была модернизирована,  получив название **М-100 «Спектр»** и стала выпускаться одновременно с машиной В-4 (начиная с 1940 года).

Конструкция шифровальной техники СССР имела мало общего с распространёнными зарубежными аналогами, которые работали по принципу механически программируемых шифраторов (называемые роторными или дисковыми). Шифровальная машина **М-100** состояла из 3 основных узлов – клавиатуры с контактными группами, лентопротяжного механизма с трансмиттером и приспособления, устанавливаемого на клавиатуру пишущей машинки. Общий вес комплекта из семи упаковок достигал 116 кг. Аккумуляторы для автономного питания электрической части машины весили 32 кг. Тем не менее, данная техника выпускалась серийно и была успешно испытана в боевых условиях во время гражданской войны в Испании, на озере Хасан, на Халхин-Голе и во время советско-финской войны. Шифртехника первого поколения предназначалась для штабов высшего управления вооружёнными силами и обильно использовалась во время Второй мировой войны. Там, где циркулировала оперативно-стратегическая информация, без этой техники обойтись было трудно. Машина позволяла [шифровать](http://www.kv.by/content/330810-shifrovat-smartfon-pod-android-uvolte) буквенные телеграммы со скоростью до 300 знаков в минуту.

Но советские криптографы на этом достижении не остановились. Работа над улучшением шифровальной техники продолжалась. В 1939 году после войсковых испытаний была принята на вооружение новая шифрмашина с роторным шифратором **К-37 «Кристалл».** Это малогабаритное устройство весом в 19 килограммов работало на шифре многоалфавитной замены (использование двух и более алфавитов для шифрования). К-37 применялась в армейских сетях связи (за год произведено 100 комплектов). Во втором квартале 1939 года были изготовлены опытные образцы шифровальных приборов-приставок для засекречивания телеграфных сообщений. C-306 – для телеграфных аппаратов Морзе с питанием от сети и С-307 – для журналистов с питанием от аккумуляторов. В 1942 году была введена в эксплуатацию М-101, которая состояла из 2 агрегатов общим весом 64,5 кг. Машина получила название **М-101 «Изумруд»** и стала производиться параллельно с В-4 и М-100.

С самого начала войны фашистские дешифровальщики пытались прочесть перехваченные советские криптограммы, зашифрованные машинными шифрами. Но все их попытки были напрасны - наши криптограммы, зашифрованные машинными шифрами, не читались. Было ясно, что уникальная система машинного шифрования русских может быть уязвима только при наличии самой шифртехники и ключей к ней.  Приказ Гитлера по вермахту от августа 1942 года гласил: «Кто возьмёт 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 1962 году появилась целая серия преемников К-37 – роторные шифровальные машины. Одной из самых известных была 10-роторная **М-125 «Фиалка»,** которую СССР поставляло союзникам. И в 2011 году три модели «Фиалки» демонстрировались на выставке американского разведывательного агентства ВВС США в Сан-Антонио. Важным историческим фактом является то, что имеющиеся на Западе Фиалки не из СССР, а из стран Восточной Европы, прежде всего из ГДР.

Большая часть шифровальных машин была разобрана или уничтожена после распада СССР. Некоторые экземпляры хранятся в частных коллекциях и музеях в США (Computer History Museum) и Великобритании (Bletchley Park).