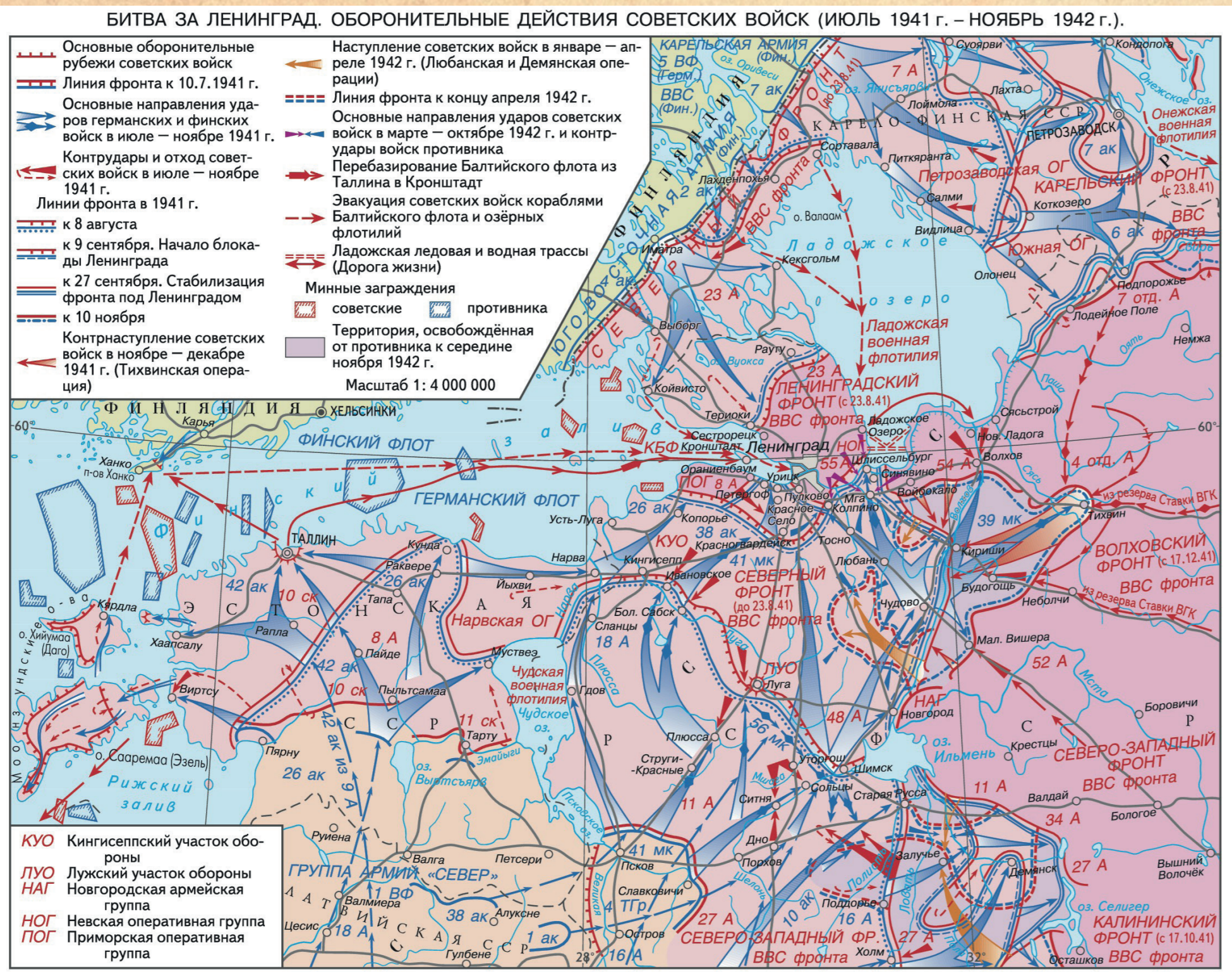




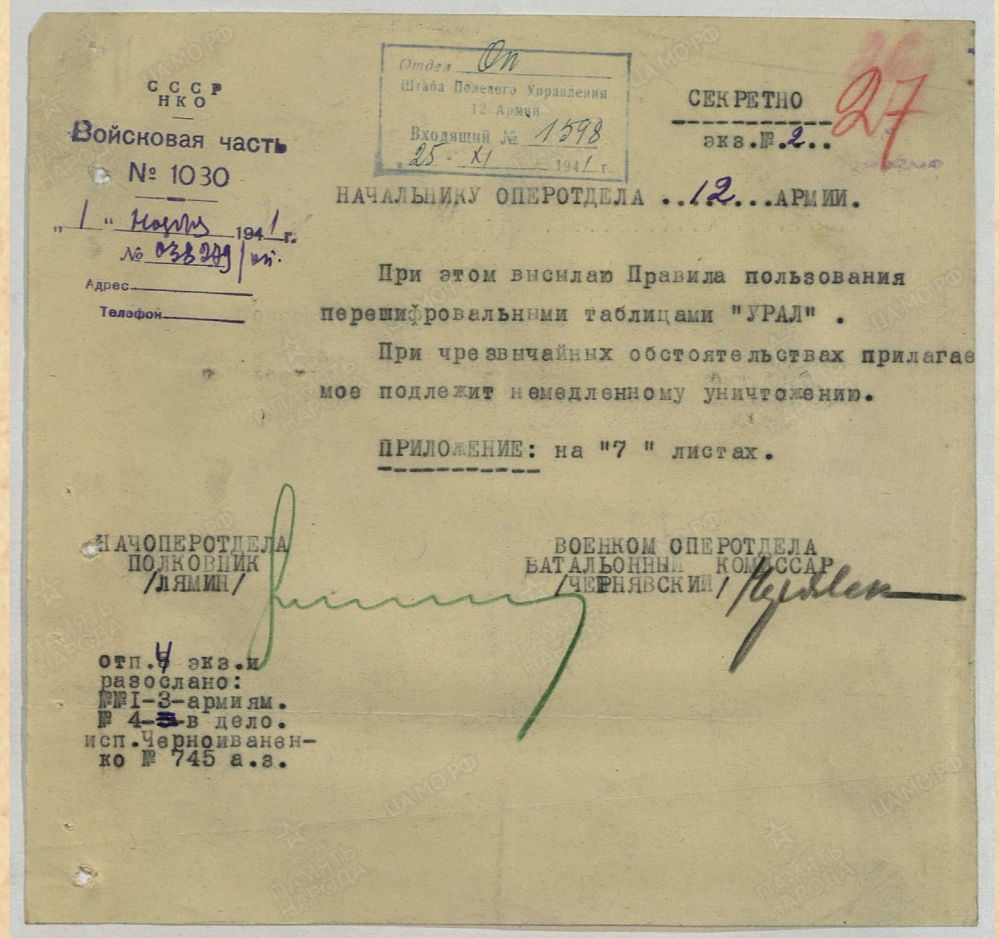
КРИПТОГРАФИЧЕСКИЙ ФРОНТ ВЕЛИКОЙ ОТЕЧЕСТВЕННОЙ

ШИФРЫ ВЕЛИКОЙ ОТЕЧЕСТВЕННОЙ ВОЙНЫ

Правила пользования перешифрованными таблицами «Урал»



В период проведения войсковых операций особую роль играли такие естественные рубежи, как реки, озёра и болота. Гидрологи регулярно составляли сводки их фактического состояния, а также разрабатывали краткосрочные и долгосрочные гидрологические прогнозы. В основном требовалось предсказание хода уровней рек, степени обводненности болот, дат замерзания рек и озёр, толщин льда в конкретный момент времени, характера ледовых образований, вскрытия рек и разрушения льда.



Для защиты при передаче по радио такого рода информации применялись перешифровальные таблицы «Урал».

Table 1: A grid of numbers used for encryption, with instructions on how to select a group of five digits.

Гидрологическая информация заранее кодировалась по схеме кода ежедневного информационного гидрологического радиобюллетеня. В результате получались группы пятизначных чисел. Секретное перешифрование заключалось в следующем. Из таблицы выбиралась любая пятизначная группа. Цифры выбранной группы и последующие за ней вправо по строке прибавлялись к цифрам перешифруемых гидрологических сведений по модулю 10.

Table 2: A grid of numbers used for deciphering, with instructions on how to subtract the key group from the ciphertext.

Table 3: A grid of numbers used for deciphering, with instructions on how to subtract the key group from the ciphertext.



Расшифрование производилось в порядке обратном изложенному, т.е. по показателям обозначительной группы в перешифровальной таблице находится цифрованная группа, с которой было начато перешифрование. Начиная с найденной и переходя на следующие группы таблицы, производится вычитание цифр таблицы из цифр шифрограммы.