Информатика в годы Великой Отечественной войны

СТРОГО СЕКРЕТНО
Снятие копий воспрещается

ПОДЛЕЖИТ ВОЗВРАТУ В 48 ЧАС.
(Пост. ПБ от 5 мая 27 г. пр. № 100, п. 5)

Кому послана Молотову, Хатаевичу, Чернову, Сталину

ШИФРОВКА

Из ДНЕПРОПЕТРОВСКА отправлена 28-10 27/У1 1933 г. Поступила в ЦК ВКП
на расшифрование 28/У1 193 3г. ч. 9 м. 40 Вх. № 985/Ш

МОСКВА ЦКВКП(б) тов. СТАЛИНУ.-

Продолжающиеся последние 10 дней беспрерывные дожди сильно оттянули вызревание хлебов и уборку урожая.

В колхозах ряда районов полностью с"еден, досдается весь отпущенный нами хлеб, сильно обострилось продовольственное положение, что в последние дни перед уборкой особенно опасно.

Очень прошу, если возможно дать нам еще 50 тысяч пудов продссуды. ок 12/с

ХАТАЕВИЧ.

Расшифрована 28/У1 1933 г. в ч. 11 м. 25 Напечатано 6 экз. Е.Иванова.-

ИЗВЛЕЧЕНИЕ ИЗ ИНСТРУКЦИИ:

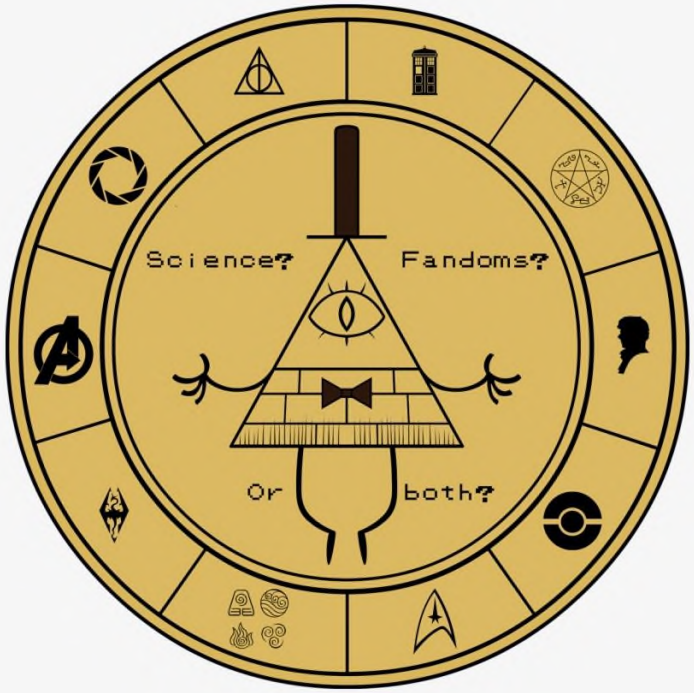
1. Шифротелеграмма должна храниться только в секретных хранилищах.
2. При ссылках на текст шифротелеграмм воспрещается указывать, что цитируемый текст получен шифром, также воспрещается указывать и номера шифроков.
3. Ответ на шифровку посылается также в шифрованном виде, текст передаваемого шифром сообщения составляется коротко и ясно: пишется только в одном экземпляре, который и передается на шифрование.

Выполнил:
Фонов В. М.

2021 г.

За многовековую историю использования шифрования информации человечеством изобретено множество методов шифрования или шифров.

Методом шифрования (шифром) называется совокупность обратимых преобразований открытой информации в закрытую информацию в соответствии с алгоритмом шифрования. Большинство методов шифрования не выдержали проверку временем, а некоторые используются и до сих пор.

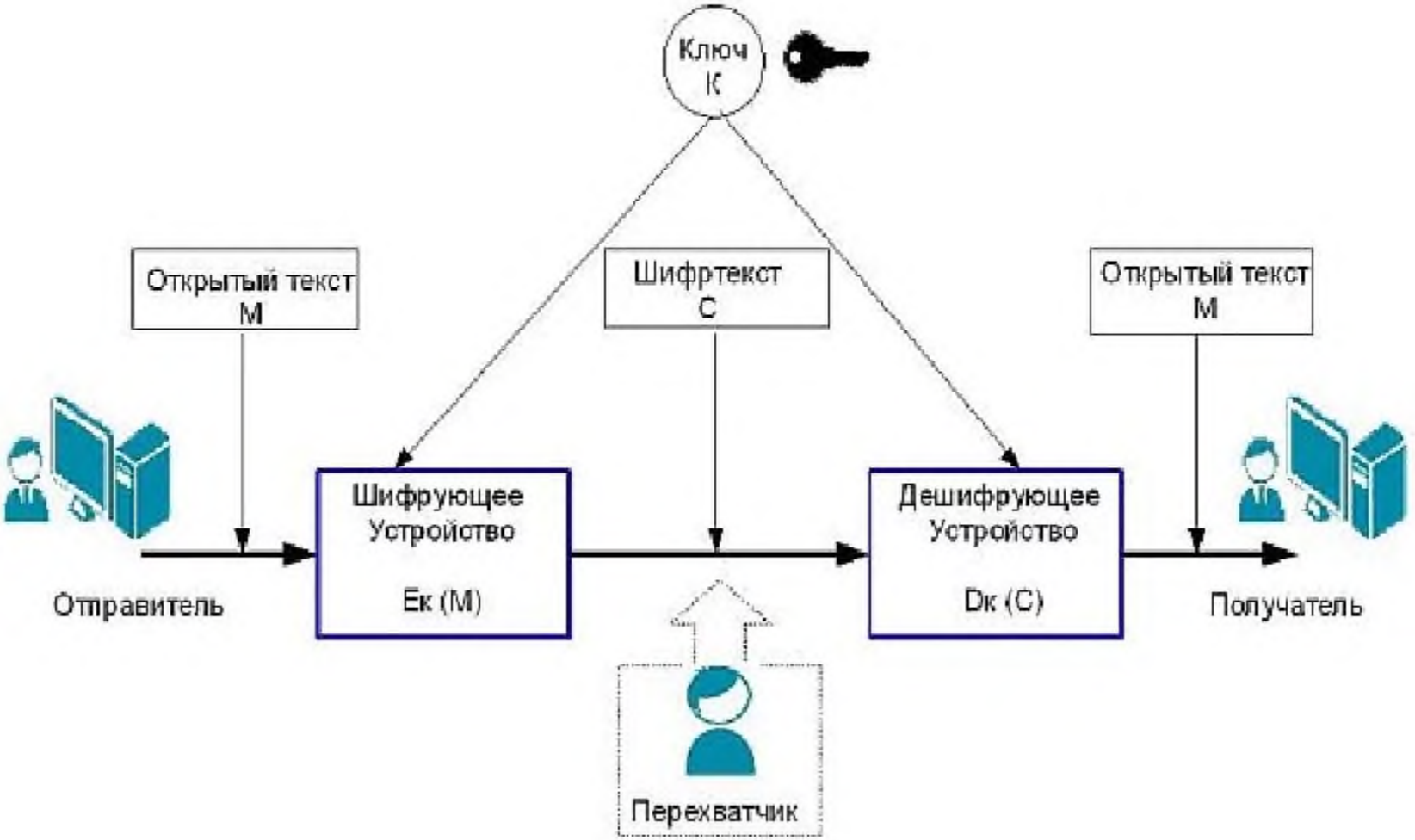


Шифр Марии,
королевы Шотландии

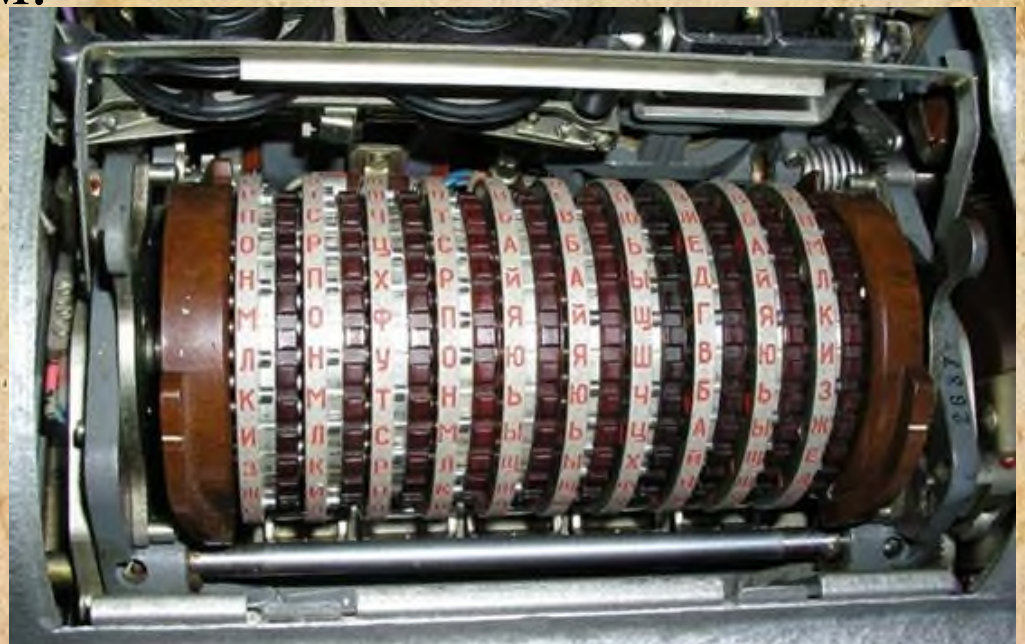
Во время ВОВ сложные технические и криптографические средства зашиты информации стали во многом ключевыми, ведь ценность информации возросла кратно.

К июню 1941, когда немецкие армии вторглись на территорию СССР, наша система защиты государственной тайны была практически полностью сформирована. Она успешно выполняла целый ряд поставленных перед ней задач. От любых иностранных разведок надежно защищались все информационные ресурсы: мобилизационные, технические, военные, политические, идеологические и природные.

Криптографические средства защиты информации

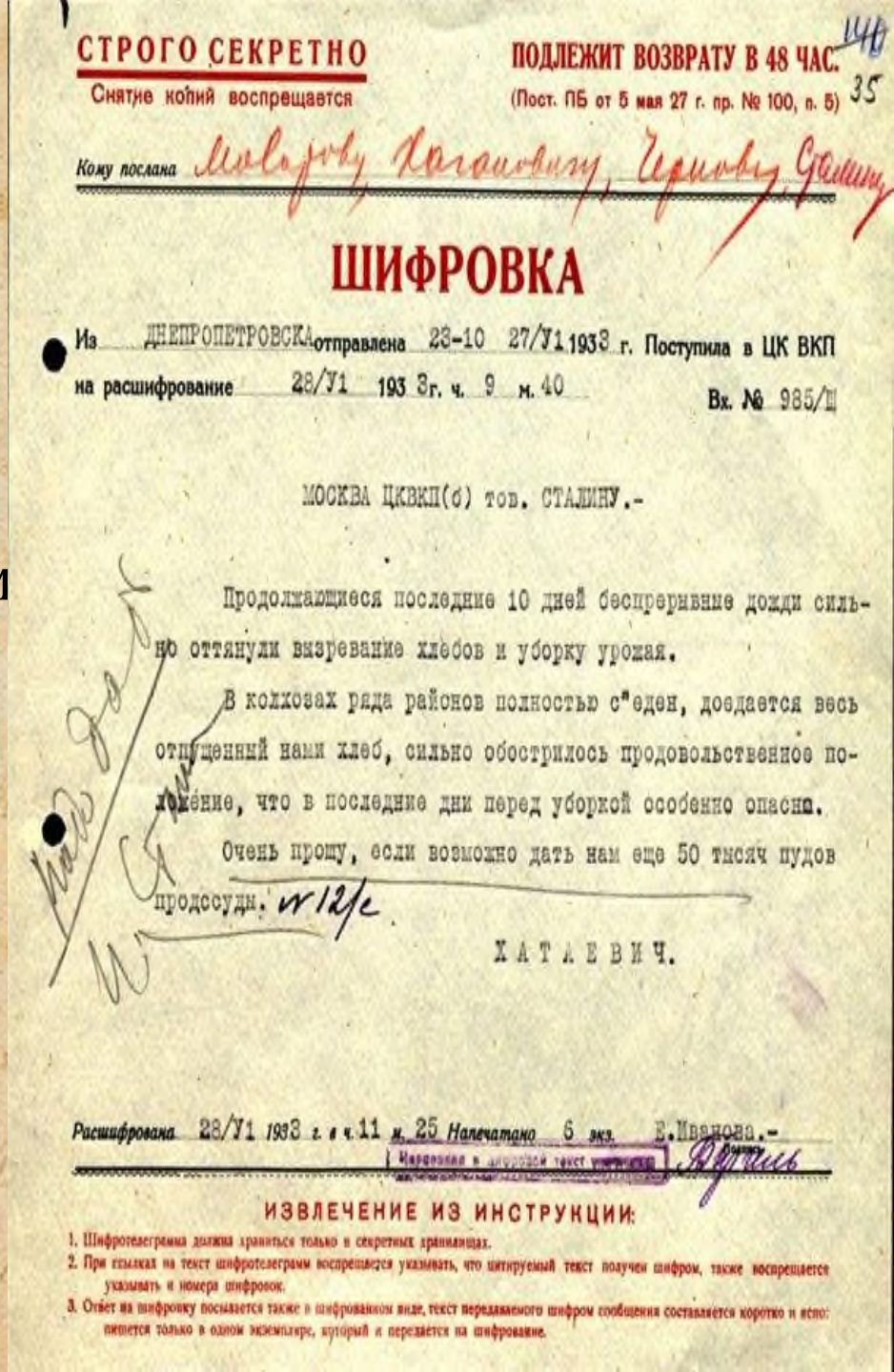


В 1937 году в Ленинграде на заводе «209», был образован комбинат техники особой секретности. Его основной задачей стало создание шифровальной техники для скрытого управления войсками: в 1939 году была создана шифровальная машина, которая получила название М-100. Основным недостатком этой машины был их огромный вес. Устройство весило 141 килограмм.



В годы войны на машинную шифросвязь легли огромные нагрузки. Только шифровальной службой РККА (8-й отдел) за период войны было отработано 1,5 миллиона шифротелеграмм и кодограмм.

Очень часто сотрудникам управления приходилось обрабатывать до 1500 шифрограмм в день, тогда как суточная норма составляла всего 400 шифрограмм. За все время войны 8-е управление Генштаба разослало нижестоящим подразделениям и войскам почти 3,3 миллиона комплектов шифров.



СТРОГО СЕКРЕТНО
Снятие копий воспрещается

ПОДЛЕЖИТ ВОЗВРАТУ В 48 ЧАС.
(Пост. ПБ от 5 мая 27 г. пр. № 100, п. 5)

Кому послана Молотову, Хатаевичу, Чернову, Сталину

ШИФРОВКА

Из ДНЕПРОПЕТРОВСКА отправлена 23-10 27/VI 1933 г. Поступила в ЦК ВКП
на расшифрование 28/VI 1933 г. ч. 9 м. 40 Вх. № 985/Ш

МОСКВА ЦКВКП(б) тов. СТАЛИНУ.-

Продолжающиеся последние 10 дней беспрерывные дожди сильно оттянули вызревание хлебов и уборку урожая.

В колхозах ряда районов полностью с"еден, доедается весь отпущенный нами хлеб, сильно обострилось продовольственное положение, что в последние дни перед уборкой особенно опасно.

Очень прошу, если возможно дать нам еще 50 тысяч пудов продссуды. 12/с

ХАТАЕВИЧ.

Расшифрована 28/VI 1933 г. в ч. 11 м. 25 Напечатано 6 экз. Е.Иванова.-

ИЗВЛЕЧЕНИЕ ИЗ ИНСТРУКЦИИ:

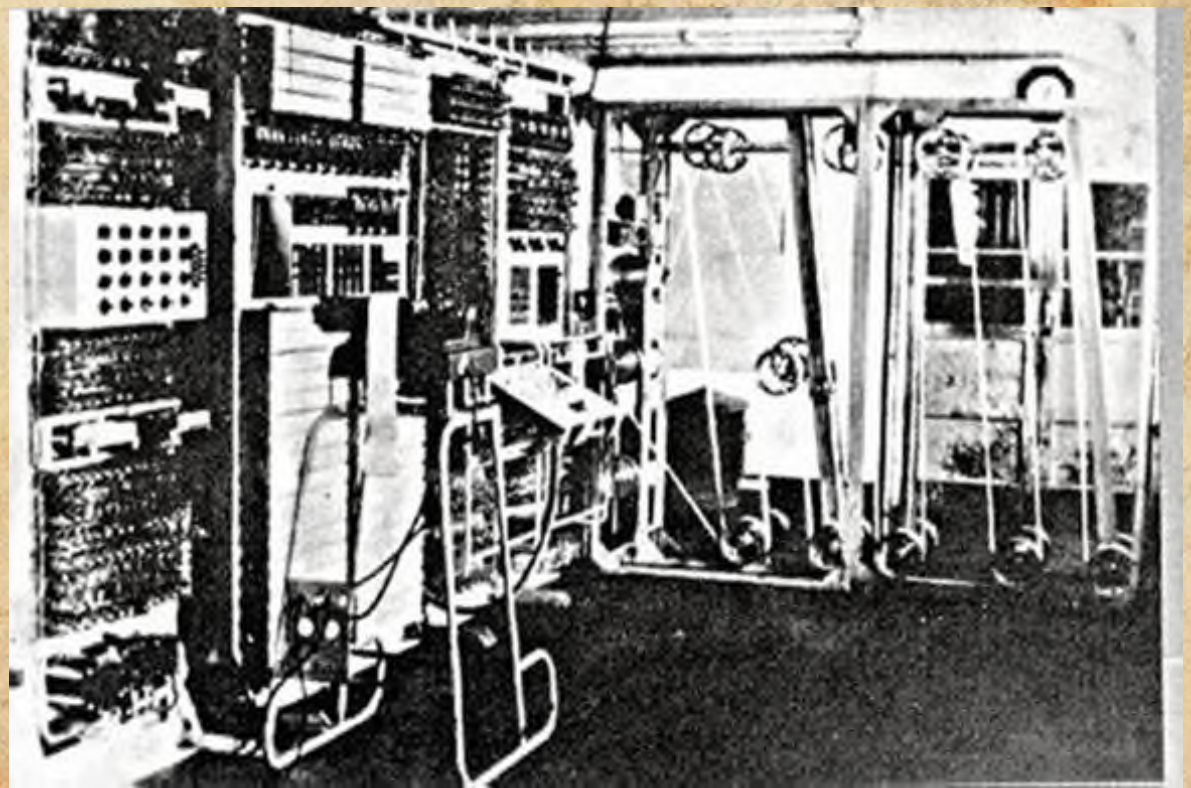
1. Шифротелеграмма должна храниться только в секретных хранилищах.
2. При ссылках на текст шифротелеграмм воспрещается указывать, что цитируемый текст получен шифром, также воспрещается указывать и номера шифровок.
3. Ответ на шифровку посылается также в шифрованном виде, текст передаваемого шифром сообщения составляется коротко и ясно: пишется только в одном экземпляре, который и передается на шифрование.

В конце первой мировой войны и в первые годы после нее возникает несколько изобретений, созданных любителями, для которых это было своеобразным хобби.

По мнению англо-американских историков, если бы не это хобби, война длилась бы на два года дольше.

Одним из этих изобретений является шифровальная машина под названием «Энигма». Для широкой публики слово «Энигма» (по-гречески – загадка) является синонимом понятий «шифровальная машина» и «взлом кода»

Поражение летом 1940 года не было предотвращено, усилия разведслужб Польши, Франции и Великобритании не пропали даром, а сослужили службу в ходе дальнейших военных действий. В Блетчли-Парке Тьюринг закончил создание "Колосса" — счетно-вычислительной машины, способной намного ускорить расшифровку шифров "Энигмы", теперь до 24 часов.



Немцы постоянно совершенствовали «Энигму». Операторов натаскивали на ее уничтожение в случае опасности. Ключи во время войны меняли каждые 8 часов. Шифродокументы растворялись в воде.

Правы были и создатели «Загадки»: расшифровать ее сообщения вручную невозможно в принципе. А что, если противник противопоставит этой машине свою? А ведь он так и поступил: захватывая новые экземпляры техники, совершенствовал свою «антиЭнигму».

Широко использовалось и ручное шифрование. Телеграммы отправлялись с помощью легких, весом в три килограмма радиостанций «Север» (Б. П. Асеев - инженер-конструктор, изобретатель, учёный), или «Северок», как их ласково называли военные связисты.

На машинную шифросвязь в годы войны легла основная нагрузка при передаче секретных телеграмм: громоздкие М-100 заменили на более компактные М-101 («Изумруд»).

Радисты с радиостанцией “Север” обеспечивали успех боевых операций знаменитых партизанских соединений А. С. Ковпака, А. Ф. Федорова, И. Н. Банова и подавляющего большинства более мелких партизанских отрядов и разведывательных групп, действовавших в тылу немецко-фашистских войск.

Кибернетика – это наука об общих закономерностях процессов управления и передачи информации в различных системах, будь то машины, живые организмы или общество. Мы решили кратко рассказать только о восьми советских учёных-кибернетиках, кто в годы Великой Отечественной внёс научный, знаниевый вклад в дело освобождения Родины и победы над фашистами.

Вклад информатиков в ВОВ

Выполнили :
обучающие группы 11м:
Минаева Ангелина,
Терехова Марина
Преподаватель:
Глебкин А.Ю.

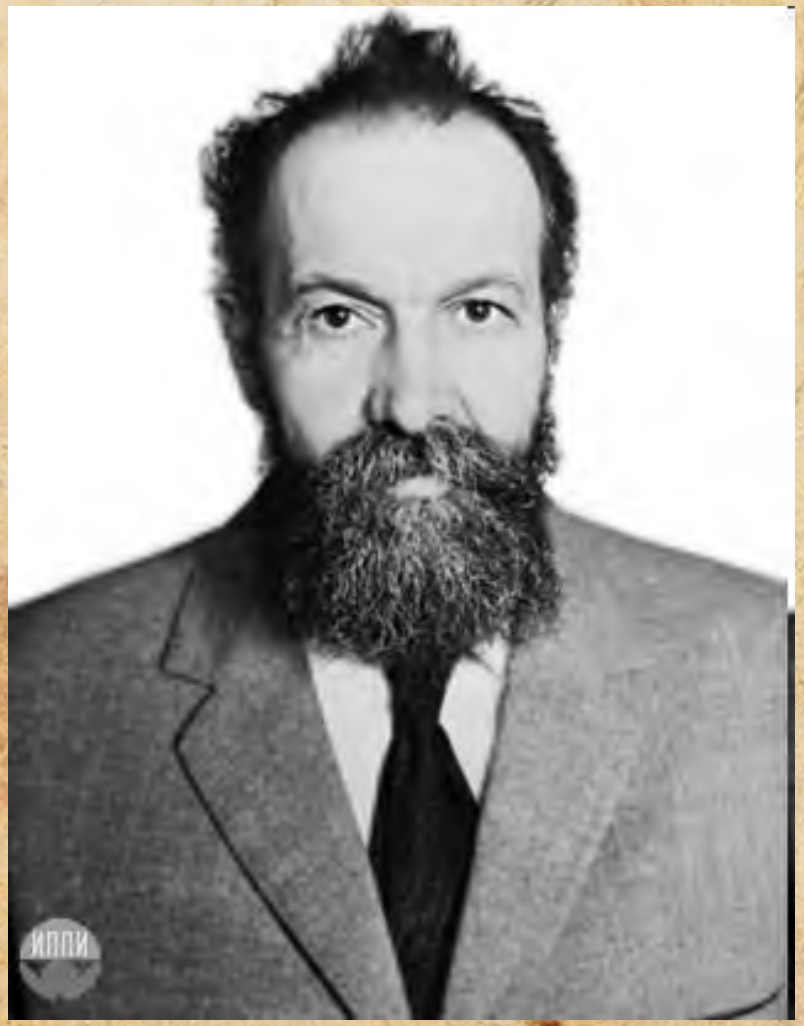
2020 г.

Пионеры компьютерной техники

Ляпунов Алексей Андреевич — разработал теорию операторных методов для абстрактного программирования и основал советскую кибернетику и программирование

Лебедев Сергей Алексеевич — разработал и построил первый советский компьютер (МЭСМ) и основал советскую компьютерную промышленность

Ляпунов А.А (1911-1973)



С 1961 года Алексей Андреевич работал в Институте математики Сибирского отделения АН СССР, где фактически создал отделение кибернетики. В Новосибирске он также основал кафедру теоретической кибернетики Новосибирского университета и лабораторию кибернетики Института гидродинамики СО АН СССР, которыми руководил до конца своей жизни.

Лебедев С.А.(1902-1974)

В 1945 г. С.А. Лебедев создал первую в стране электронную аналоговую вычислительную машину для решения систем обыкновенных дифференциальных уравнений, которые часто встречаются в задачах, связанных с энергетикой.

Гаврилов М.А. (1903-1979)

В 1926-1928 гг. им была предложена одна из первых систем телеуправления, вошедшая в эксплуатацию._1939—1941 гг. был руководителем работ по созданию системы телемеханики для управления городским освещением в Москве.

Полетаев И.А.(1915- 1983)

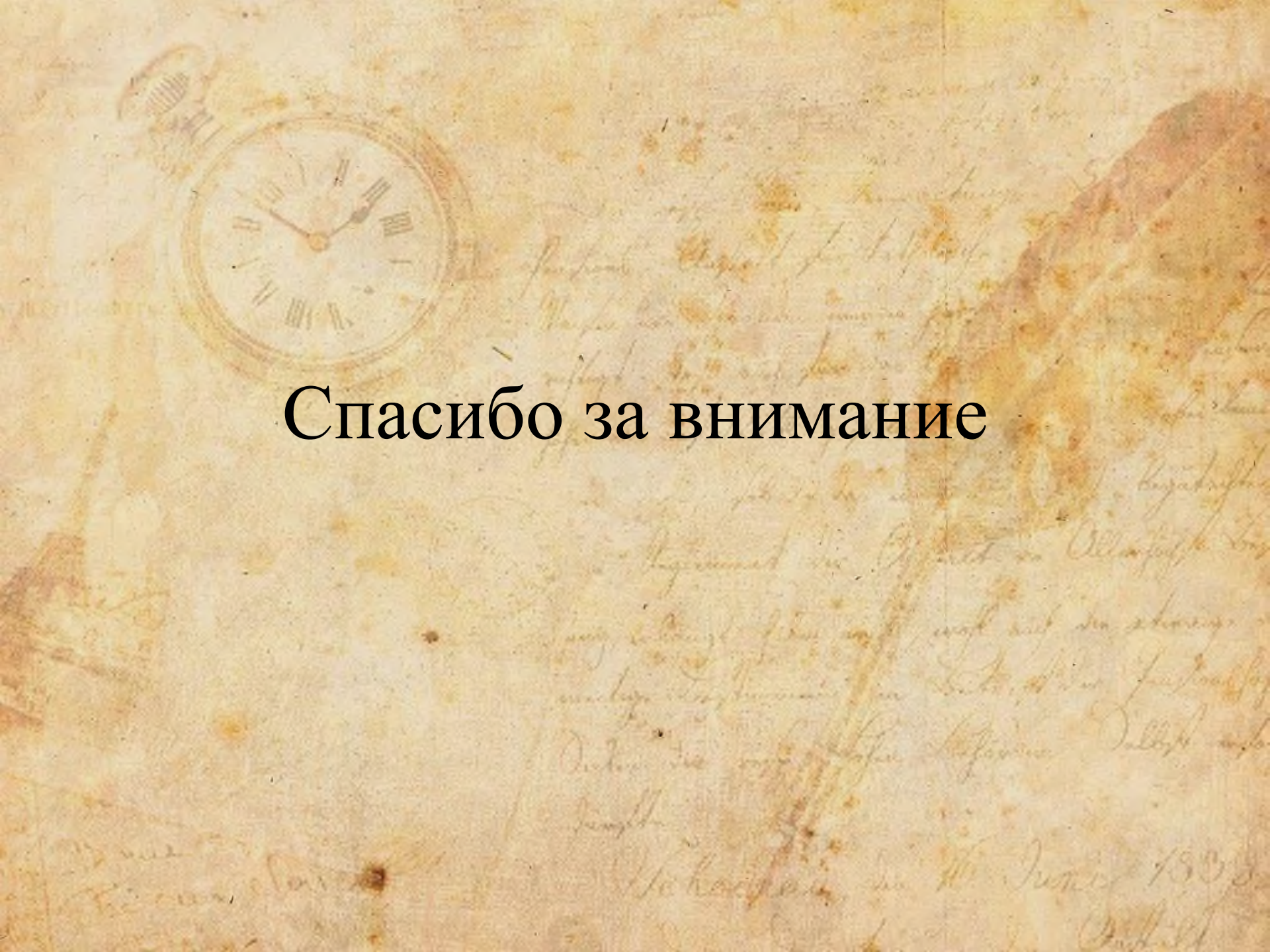
Полетаев И.А. - один из первых отечественных кибернетиков, ученик А.А. Ляпунова, автор первой в нашей стране монографии о кибернетике - "Сигнал".

Цетлин М.Л.(1924-1966)

Начиная с 1961г. и до конца жизни М.Л. Цетлин занимался проблемами целесообразного поведения автоматов.

БЭСМ

Большая электронная счетная машина (БЭСМ) с памятью на ферритовых сердечниках емкостью 2048 слов.


Спасибо за внимание