Прочти меня, если сможешь

Криптография и криптоаналитика Великой Отечественной войны

Презентация составлена по материалам из открытых источников сети Интернет

Сост.: зав. отделом обслуживания Фундаментальной библиотеки ГАОУ ВО МГПУ в ИЦО Кершенгольц А.Б.

У каждой страны нет ничего более секретного, чем её шифры, поскольку их раскрытие другим государством повлечет за собой утечку многих тысяч секретов, закрываемых этими шифрами…

Пока существуют государства, будет оставаться и необходимость в защите государственных секретов.

Н.Н. Андреев

Война стала не только крупнейшим противостоянием в истории вооруженных конфликтов, но и принципиально изменила подход к передаче информации. Ведь тот, кто владеет информацией, может изменить исход боевых действий.

С развитием языков, письменности, науки и техники вырос и уровень шифрования – вместо символов, тайных жестов, иероглифов и выдуманных языков в ход пошли сложные математические принципы, модуляторы сигналов и шифровальные машины.

Инженеры – конструкторы и криптографы

Иван Павлович Волосок

Владимир Александрович Котельников

Валентин Николаевич Рытов

Офицеры–конструкторы 8-го Управления Генерального Штаба в годы войны занимались не только созданием новых образцов шифртехники.
Внедрение её в войска, обучение работе – было их основным занятием.

Самым распространенным методом шифрования в Красной Армии во время Великой Отечественной войны были коды с перешивкой.

Существовала определенная иерархия их использования:

2-значные коды применялись низшими звеньями вооруженных сил,

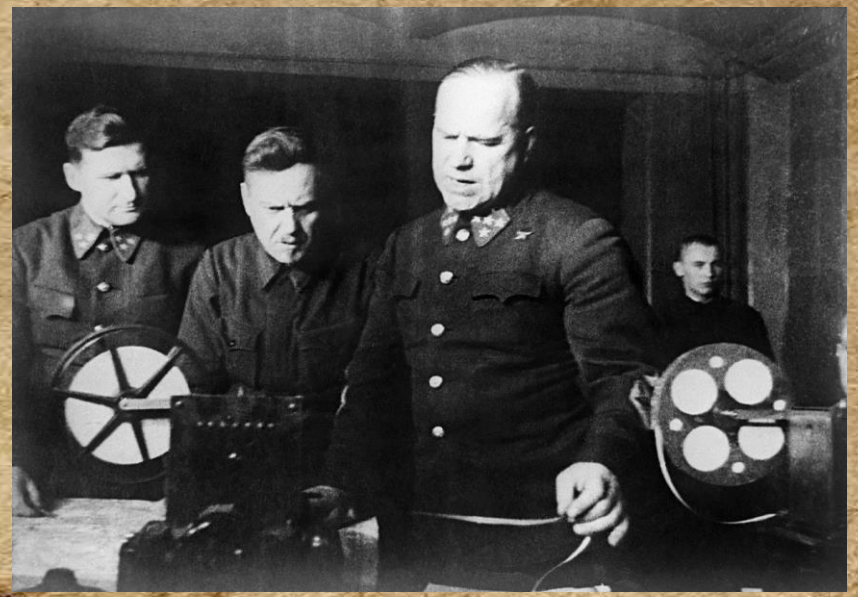
3-значные были в ходу в подразделениях до уровня бригады,

4-значные предназначались для армий и фронтов,

5-значный код использовался только для шифрования стратегической информации самого высокого уровня.

Именно 5-значные коды оказались самыми стойкими – на протяжении всей войны такие шифры не могли читать ни враги, ни нейтралы, ни союзники Советского Союза.

Читать о шифрах подробнее



Криптоаналитики (дешифровальщики)

Борис Алексеевич Аронский

Сергей Семёнович Толстой

Алексей Иванович Копытцев

Заводы, на которых конструировалось и производилось шифровальное оборудование

Завод № 209 им. А.А. Кулакова

История завода в блокаду и войну

Телефонный завод «Красная заря»

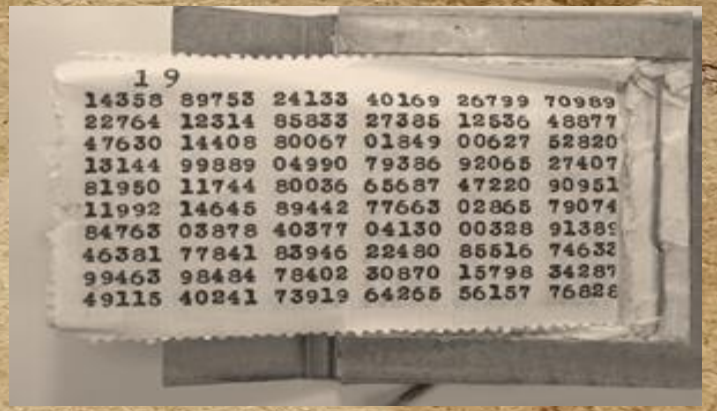
Шифровальная аппаратура

Шифровальная машина М-100 «Спектр»

Шифровальная машина М-101 «Изумруд»

Шифровальная машина К-37 «Кристалл»

Засекречивающая аппаратура С-1 «Соболь-П» КВ-радиотелефонии



Блокнот шифровальщика

Шифровальная техника позволила в 5-6 раз по сравнению с ручным способом повысить скорость обработки телеграмм, сохраняя при этом гарантированную стойкость передаваемых сообщений.

Читать подробнее о шифровальной аппаратуре

В конце 1945 года были подведены итоги эксплуатации шифровально-кодировочной техники в действующей армии.

В это же время проводится исследовательская работа по дальнейшему повышению криптостойкости применяемой техники, и намечаются пути и направления по созданию новых образцов аппаратуры с гарантированной стойкостью.

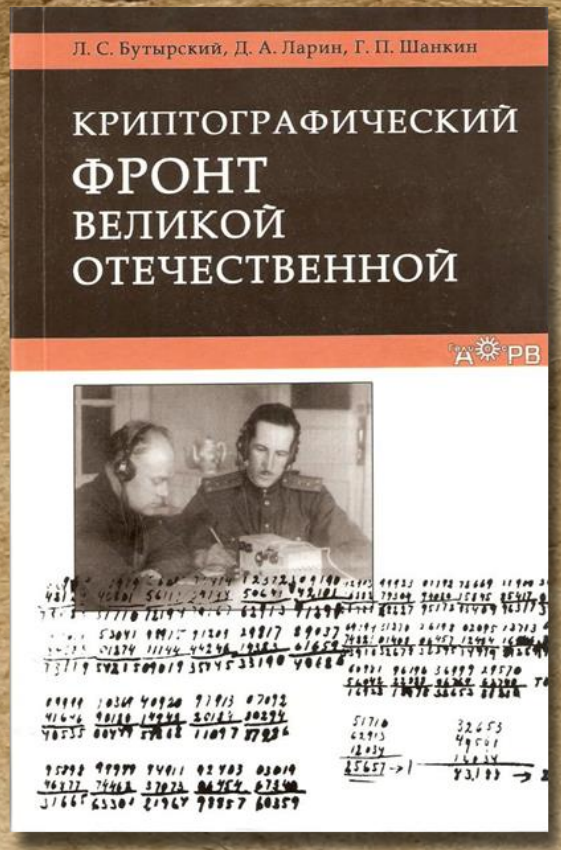
Наряду с шифром гаммирования все большее применение находит шифр колонной замены, техническая реализация которого была заложена еще в 30-е годы в дисковой кодировочной машине К-37.

Приказ Гитлера по вермахту от августа 1942 года, который так и не был выполнен, гласил: «... кто возьмет 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».

Согласно инструкции, советские шифровальщики были обеспечены надежной охраной. Кроме того, они обычно ставили рядом канистру с бензином и держали под рукой гранату, чтобы при приближении противника уничтожить документы, оборудование и самих себя.

Читать подробнее о вкладе военных связистов и криптографов в Великую Победу

Интересное по теме:



Бутырский Л.С. Криптографический фронт Великой Отечественной / Бутырский Л.С., Ларин Д.А., Шанкин Г.П. ; Предисл. д-ра ист. н., проф., засл. деят н. Р. Г. Пихоя. – М. : Гелиос АРВ, 2012. – 688 с. : ил.

Книга в захватывающей и доступной форме рассказывает об одной из самых малоизвестных страниц Великой отечественной войны – противостоянию криптографических служб СССР, союзников и Германии. Начав с увлекательного обзора истории криптографии, авторы последовательно рассказывают о всех направлениях деятельности криптографических служб: ручных шифрах, роторных шифрмашинах, методах и средствах шифрования речевых сообщений. Приводятся интереснейшие данные о деятельности советской шифровальной и дешифровальной службы, использовании криптографических средств в деятельности советской разведки и партизанском движении. Отдельные главы посвящены организации агентурной радиосвязи и использовании стеганографии.

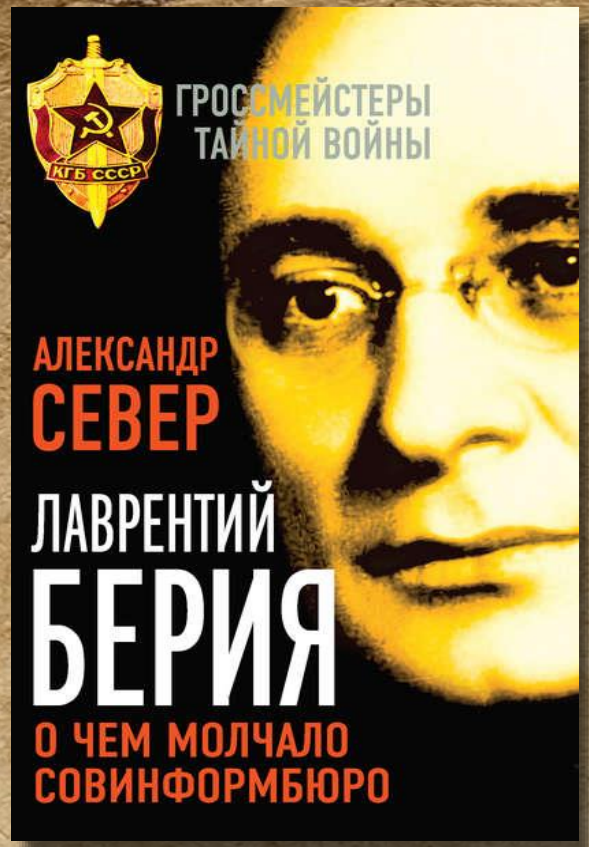
Для всех, кому интересны малоизвестные страницы великого интеллектуального противостояния на криптографическом фронте, где, как и на полях сражений, потом и кровью его участников ковалась великая Победа.

Великая Победа : интернет-проект. Радиофронт VII. Криптографы вступают в бой / Под общ. ред. С.Е. Нарышкина, А.В. Торкунова ; Ред. совет: А.Н. Артизов и др. ; Московский гос. ин-т международных отношений (Ун-т) МИД России ; Российское военно-историческое о-во. – 2015. – URL : https://histrf.ru/uploads/media/artworks_object/0001/25/0d0945718c36be3438bb3b6afe9c314cbec548b7.pdf (дата обращения: 27.02.2020).

Ларин Д.А. Защита информации советских партизан и подпольщиков в годы Великой Отечественной войны / Д.А. Ларин // Безопасность информационных технологий. – 2011. – Т. 18, № 3. – С. 91–101. – URL : https://bit.mephi.ru/index.php/bit/article/view/625/630 (дата обращения: 26.02.2020).

Ларин Д.А. Советская шифровальная служба в годы Великой Отечественной войны / Д.А. Ларин // Известия Уральского государственного университета. Серия 1: Проблемы образования, науки и культуры. – 2011. – Т. 86, № 1. – С. 69–80. – URL : https://www.elibrary.ru/download/elibrary_15665372_85920693.pdf (дата обращения: 26.02.2020).

Прочти меня, если сможешь. Советские «тьюринги» и криптография времен Великой Отечественной Войны // Бессмертный полк. Москва: электронная кн. памяти. – URL : https://www.polkmoskva.ru/articles/machines/prochti-menya-esli-smozhesh/ (дата обращения: 26.02.2020).



Север А. Лаврентий Берия. О чем молчало Совинформбюро / А. Север. – М. : Алисторус, 2015. – 410 с. : ил. – (Гроссмейстеры тайной войны).

Когда в ноябре 1938 года Лаврентий Берия был назначен руководителем НКВД СССР, то доставшееся ему от предыдущего наркома внутренних дел Николая Ежова «наследство» сложно было назвать «богатым». Многие сотрудники внешней разведки и контрразведки были репрессированы, а оставшиеся на своих местах не соответствовали задачам времени. Все понимали, что Вторая мировая война неизбежна. И Советский Союз был к ней не готов.

За 2,5 предвоенных года Лаврентию Берии удалось почти невозможное – значительно повысить уровень боеспособности органов разведки и контрразведки. Благодаря этому, например, перед началом Великой Отечественной войны Германия так и не смогла установить точную численность и места дислокации частей и соединений Красной армии. А во время самой войны советские разведчики и контрразведчики одержали серию блистательных побед над спецслужбами не только Германии и Японии, но и стран, ставших противниками СССР в годы «холодной войны», – США и Великобритании.

Столпаков Б. Криптографический фронт Великой Отечественной войны : лекция / Б. Столпаков. – URL : https://www.youtube.com/watch?v=JxKfj5dhbLE (дата обращения: 26.02.2020).

Историк отечественной криптографии в специальной лекции расскажет о работе героев незримого фронта и их вкладе в великую победу.

Они одолели своих немецких соперников в интеллектуальном противостоянии. Разработали и внедрили новые технологии засекречивания. Изобрели методы, которые определили дальнейшее развитие криптографии во всем мире.

Кто они - безвестные герои Великой Отечественной? Каковы заслуги непобедимых бойцов скрытого от глаз криптографического фронта? Ответы на эти вопросы - в лекции историка отечественной криптографии Бориса Столпакова.

Столпаков Б.В. «Чтоб было в тех землях не знатно...». Исторические свидетельства о начале и становлении российской криптографии (XVI - XVII века) / Б.В. Столпаков, В.Г. Никонов. – М. : Авангард, 2016. – 254 с.

Эта книга посвящена истории становления криптографии в Российском государстве. Авторы старались систематизировать имеющиеся документальные свидетельства этого периода. В монографии отражены результаты архивных изысканий и исследований авторов по начальной истории криптографической службы России, проведенных при поддержке Академии криптографии РФ.

При написании книги авторы ориентировались на широкий круг читателей, интересующихся отечественной историей, дипломатией и криптографией. Вместе с тем, книга может быть использована при преподавании истории дипломатической службы и истории криптографии

Сколько битв выиграли криптоаналитики? // Север А. Лаврентий Берия. О чем молчало Совинформбюро. – М. : Алисторус, 2015. – 410 с. : ил. – (Гроссмейстеры тайной войны). – URL : https://military.wikireading.ru/14036 (дата обращения: 26.02.2020).

Памятники воинам-связистам Великой Отечественной войны