УДК 681.188.000.93
DOI: 10.33099/2707-1383-2021-39-1-97-113

Сергій Вдовенко
доцент кафедри зв'язку та автоматизованих систем, Інститут забезпечення військ (сил) та інформаційних технологій, Національний університет оборони України імені Івана Черняховського (Київ, Україна),
ORCID https://orcid.org/0000-0001-8139-7975
Електронна пошта: vsg64@ukr.net,

Микола Гульков
викладач кафедри зв'язку та автоматизованих систем, Інститут забезпечення військ (сил) та інформаційних технологій, Національний університет оборони України імені Івана Черняховського (Київ, Україна),
ORCID https://orcid.org/0000-0003-1883-4954
Електронна пошта: n.gulkov@gmail.com,

Сергій Сидоров
професор кафедри історії війн і воєнного мистецтва, Інститут державного військового управління, Національний університет оборони України імені Івана Черняховського (Київ, Україна),
ORCID https://orcid.org/0000-0002-1961-4251
Електронна пошта: sydorov@ukr.net,

Володимир Джола
слухач групи 4109, Інститут забезпечення військ (сил) та інформаційних технологій, Національний університет оборони України імені Івана Черняховського (Київ, Україна),
ORCID https://orcid.org/0000-0002-9344-7172
Електронна пошта: voldj@ukr.net

ЗАСОБИ КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ СРСР ПЕРІОДУ ДРУГОЇ СВІТОВОЇ ВІЙНИ

У статті розглядаються шляхи створення й розвитку техніки криптографічного захисту інформації СРСР на передодні та в період Другої Світової Війни та їх вплив на систему управління військами. Теорія «глибокої операції», фактично — воєнна стратегія СРСР того часу, внаслідок технічного прогресу засобів збройної боротьби, зокрема засобів зв'язку, зміни поглядів на організацію військ, їх оперативну побудову, просторово-часові характеристики операцій вимагала докорінних змін в управлінні військами та організації взаємодії міжвидових угруповань. Одним зі шляхів досягнення цієї мети була автоматизація процесів шифрування інформації.

Науково-технічний прогрес у всі часи впливає на форми і способи ведення бойових дій. Розвиток систем зв'язку та інформатизації, технічної розвідки, криптоаналізу вимагають впровадження в сучасних умовах новітніх засобів озброєння та військової техніки, форм і способів їх застосування.

На основі досвіду, набутого Радянським Союзом, досліджуються вимоги, які необхідно врахувати для підвищення скритності та оперативності управління військами під час підготовки та в ході ведення операцій, в т.ч. — операції Об'єднаних сил.

Ключові слова: *конфіденційність, криптографічний захист інформації, оперативність, скрите управління військами, скритність, шифрувальна машина, шифрувальний орган, шифрувальна техніка.*

Постановка проблеми. На початку XX століття необхідність забезпечення секретності інформації про стан збройних сил та дотримання скритності управління військами при підготовці та проведенні операцій, при веденні воєнних (бойових) дій в більшості країн світу призвела до стрімкого розвитку криптографії. Оперативно-технічні умови операцій, виходячи зі стратегій та воєнних доктрин того часу, вимагали одночасного забезпечення секретності й високої оперативності доведення інформації, що циркулює під час управління військами (Вдовенко, С. Г. & Даник, Ю. Г. 2020, с. 32). Основним способом вирішення цього завдання стало впровадження автоматизованих механічних та електромеханічних засобів криптографічного захисту інформації (Сумароков, В. П. 1999, с. 115).

Огляд основних досліджень. Наприкінці XX – початку XXI століття, спочатку в іноземних (Кан, Д. Е.

2000, с. 38–45), а згодом в російських виданнях (Нарышкина, А. В. & Торкунова С. Е. 2015, с. 20–22; Бабиевский, В., Бутырский, Л., Ларин, Д. & Шанкин, Г. 2002), опублікована значна кількість переважно публіцистичних робіт даної тематики. В Україні це питання майже не досліджувалося. За винятком декількох газетних та журнальних публікацій (Вдовенко, С. Г. 2001, с. 22–23). В Ужгороді В. Гребенніковим видана електронна книга «Історія криптології & секретного зв'язку». Причому, унаслідок надвисокої секретності криптографічних питань в СРСР, у ряді джерел (К-37 «Кристалл». Материал из Википедии — свободной энциклопедии 2012; Штеменко, 1987, с. 469) по тексту та/або в ілюстраціях опублікована неправдива або некоректна інформація.

Мета статті — аналіз та описання реального стану розвитку засобів шифрованого зв'язку Робітничо-Селянської Червоної Армії (далі — РСЧА) і Робітничо-Селянського Червоного Флоту (далі — РСЧФ) в період Другої світової війни, його впливу на хід воєнних дій з одночасним зазначенням помилок інших джерел.

Виклад основного матеріалу. На передодні і під час війни основним засобом шифрування застосовували в основному ручні коди і шифри такі, як «УП Третій» (*рис. 1*), «АРО Перший» та інші. Швидкість шифрування за допомогою ручних шифрів була надзвичайно низька. Принцип шифрування полягав у криптографічному перетворенні по певному закону цифрових груп коду, що відповідали, відповідним чином, словам або буквам шифркоду. Навіть при високому рівні підготовки шифрувальника, час зашифрування тексту наказу або розпорядження обсягом 1,5–2 сторінки, займав до 4–5 годин. Стільки ж часу витрачалося на розшифрування. Внаслідок помилок під час шифрування через громіздкість і незручність використання шифрблокнотів, а також поганих каналів телеграфного чи радіозв'язку, час на шифрування і розшифрування тексту збільшувався вже вдвічі (Нарышкина, А. В. & Торкунова С. Е. 2015, с. 20). В ході війни обсяг листування у порівнянні з мирним часом зріс в десятки разів. Тільки 8-м управлінням Генштабу РСЧА за роки війни було оброблено понад 1,6 млн. шифртелеграм і кодограм (до 1 500 повідомлень на добу). Середній обсяг шифрованого листування досягав: у фронтовій ланці — 400 шифртелеграм на добу, в корпусах — більш ніж 60. В період війни машинна обробка шифрованої інформації склала: в Генеральному штабі РСЧА — 50%; в штабах фронтів (армій) — 35–60%.

Історія автоматизації шифрувальної служби починається з листа начальника ГШ РСЧА Б. М. Шапошнікова, поданого на адресу НКО СРСР К. Є. Ворошилова в 1930 р., в якому обґрунтовувалася необхідність підвищення оперативності шляхом механізації процесу шифрування. Теоретичну основу створення шифрувальної техніки, що докорінно відрізнялася від західних зразків, вперше запропонував на засіданні наукової ради РСЧА 29 червня 1930 року інженер-конструктор Іван Волосок (*рис. 2*). Його ідея полягала в тому, щоб використовувати принцип накладення комбінацій так званої гами нескінченного ключа на комбінації знаків відкритого тексту, що забезпечувало необхідну гарантовану стійкість шифрування будь-яких повідомлень. В якості носія знаків гами шифру використовувалася перфострічка (*рис. 3*), яка виготовлялася за допомогою пристрою «Х».

Рис. 1. Шифркод

Рис. 2. І. Волосок

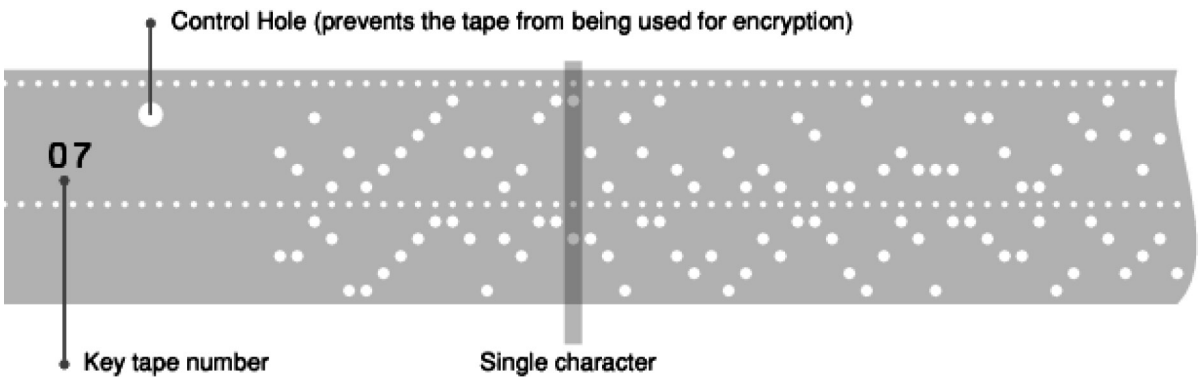

Рис. 3. Стрічка з шифргамою для радянських шифраторів

Ці шифрострічки за розмірами та способом розміщення знаків гами (отворів) відрізнялися від перфострічок стандартного розміру (*рис. 4*), які обмежено використовувалися у США.

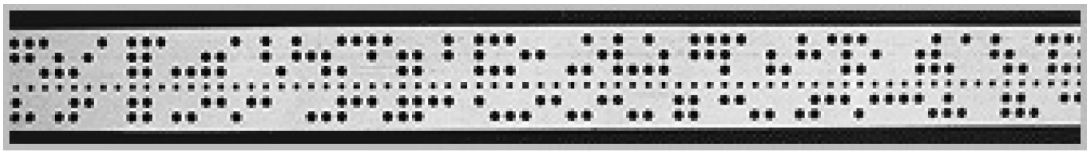

Рис. 4. Стрічка з шифргамою для американських шифраторів

Це було практичне конструктивне рішення, яке математично було розв'язане пізніше в так званій теоремі Віттакера—Найквіста—Шеннона—Котельникова (Нарышкина, А. В. & Торкунова, С. Е. 2015, с. 20–22; Бабиевский, В., Бутырский, Л., Ларин, Д. & Шанкин, Г. 2002). Пристрій використовувався для вироблення стрічок шифруючої гами для шифрувальних машин та механічних шифраторів-приставок для телеграфних апаратів, також розроблених під керівництвом І. Волоска. За винахід, конструкторські рішення та прийняття на озброєння шифратора, що реалізує криптоалгоритм, який теоретично неможливо дешифрувати, генерал-майору військ зв'язку І. Волоску було присвоєно науковий ступень кандидата технічних наук без захисту дисертації.

Перевагою такого алгоритму шифрування є абсолютна недешифруємість криптограм, за умов непорушення правил роботи шифрувальником. Однак його недоліком є велика витрата симетричних ключів та доволі низька швидкість обробки інформації. Внаслідок цього суттєвого недоліку подібна апаратура М-134А виробництва США застосовувалася лише під час Другої світової війни та тільки для забезпечення шифрованим зв'язком на напрямку президент США — прем'єр-міністр Великої Британії. Зазначений принцип шифрування використовувався в Радянському Союзі та державах так званого соцтабору до 80-х років XX століття, хоча у світі, у союзників та протиборчої сторони широко застосовувався принцип лінійного шифрування з використанням дискових шифраторів.

У 1932 р. в технічній лабораторії при 8-му відділі ГШ РСЧА під керівництвом І. Волоска було створено перший дослідний зразок шифрувальної машини ШМВ–1, яка пізніше стала йменуватися В-4. «Акт про прийняття на озброєння електромеханічної шифрувальної машини В-4» затверджено начальником ГШ РСЧА у січні 1934 р. Саме з цього зразка розпочався відлік історії створення серії машин, що забезпечували гарантовану стійкість шифрповідомлень. В-4 через громіздкість та механічну ненадійність

в серійне виробництво не потрапила, але стала прототипом нових, більш досконалих зразків. Протягом 1937–1938 рр. були проведені державні випробування розроблених на її основі дослідних зразків і вже у травні 1938 р. наказом НКО СРСР була прийнята на озброєння шифрувальна машина М-100 «Спектр» (*рис. 5*). До початку Другої світової війни промисловістю було виготовлено 96 комплектів М–100, які застосовувалися в ланці ГШ — штаби військових округів (фронтів) (Вдовенко, С. Г. 2001, с. 13; Вдовенко, С. Г. 2008, с. 22).

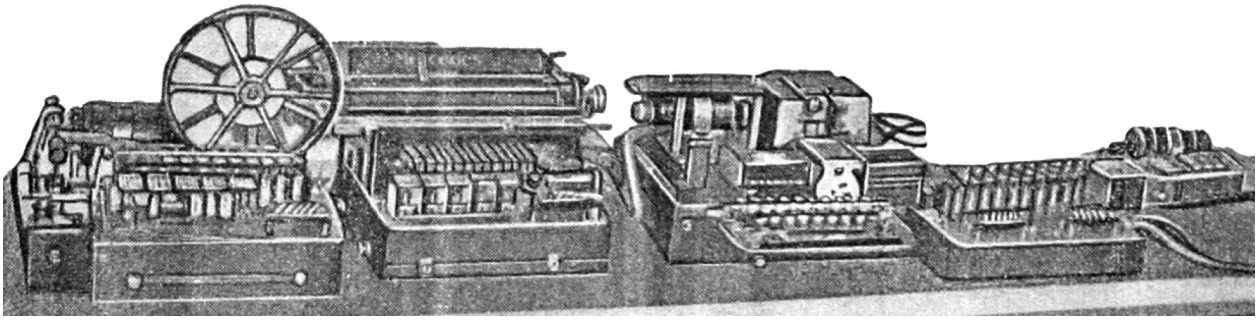

Рис. 5. Шифрувальна машина М-100 «Спектр»

Цей виріб також виявився громіздким. Складався із трьох основних вузлів: клавіатури з контактними групами, стрічкопротяжного механізму з трансмітером і пристрою, що встановлювався на клавіатуру друкарської машинки. Додатково в комплект входили ще сім складових. Загальна вага комплекту сягала 141 кг. Лише акумулятори для автономного живлення важили 32 кг. Швидкість набору знаків на клавіатурі складала 230–250 знаків/год. Незважаючи на це, М–100 випускалася серійно і була успішно випробувана в бойових умовах на Хасані, Халхин-Голі, в Іспанії та під час фінської війни (Нарышкина, А. В. & Торкунова, С. Е. 2015, с. 20–22; Бабиевский, В., Бутырский, Л., Ларин, Д. & Шанкин, Г. 2002; Вдовенко, С. Г. 2008, с. 22).

В окремих джерелах (Гребенніков, В. 2009) на фотоілюстрації під назвою М–100 «Спектр» насправді зображена малогабаритна дискова кодувальна машина К-37 «Кристалл» (*рис. 7*), про яку мова піде нижче.

В 1939 р. почата розробка більш досконалого виробу, дослідний зразок якого був створений в 1940 р., а серійне виробництво розпочато в 1942 р. Виріб був введений в експлуатацію на початку 1943 р. під індексом М-101, умовна назва «Ізумруд» (*рис. 6*).

Дана апаратура шифрування складалася з двох основних вузлів, за вагою була меншою за «М-100» вдвічі, а за габаритами — в шість разів. Дещо була підвищена швидкість роботи з 250 до 280 знаків на годину. Автоматизована обробка шифртелеграм прискорювала роботу в 4–6 разів.

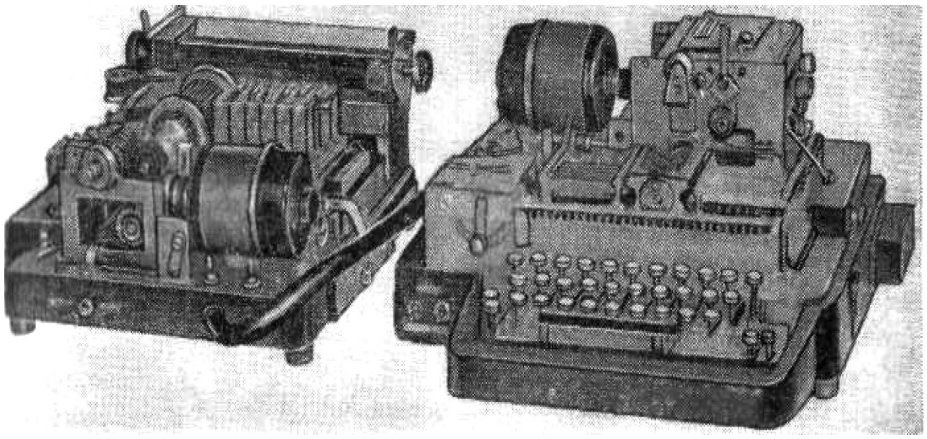

Рис. 6. Шифрувальна машина М-101 «Ізумруд»

В окремих джерелах (Нарышкина, А. В. & Торкунова С. Е. 2015, с. 20–22; Бабиевский, В., Бутырский, Л., Ларин, Д. & Шанкин, Г. 2002) фотоілюстрації під назвою М-101 «Ізумруд» на справді зображена малогабаритна дискова кодувальна машина К-37 «Кристалл» (*рис. 7*), а в (Гребенніков, В. 2000) дійсне фото післявоєнного виробу М-105 «Агат» підписане, як М-105 «Ізумруд».

Рис. 7. Кодувальна машина К-37

В оперативній ланці (армія — корпус — дивізія) успішно експлуатувалася малогабаритна дискова кодувальна машина К-37 «Кристал» (*рис. 7*), що замінювала документи ручного кодування. Тільки за 1940 р. промисловість випустила 100 комплектів К-37, а загалом до початку війни - 150. Це був достатньо компактний автоматизований пристрій вагою 19 кг, що складався з однієї упаковки. Друк здійснювався на паперову телеграфну стрічку.

Д. Кан (Кан, Д. Е. 2000, с. 74) висловлює думку про використання поставлених до СРСР по ленд-лізу виробів М-209 (*рис. 8*) для створення радянських шифрувальних машин. Виходячи з того, що з криптографічних пристроїв лише зразок К-37 був дисковим, саме його порівняємо з М-209. Крім того, слід враховувати, що поставки кораблів, які комплектувалися шифрмашиною CSP-1500 (назва виробу М-209 для ВМС) від США до СРСР були здійснені лише у 1942 р. (*табл. 1*).

Табл. 1

ПОРІВНЯЛЬНА ТАБЛИЦЯ ЗРАЗКІВ М-209 ТА К-37

Найменування	М-209 (CSP-1500)	К-37
Офіційне найменування	портативна шифрувальна машина	малогабаритна дискова кодувальна машина
Маса	2,7 кг	19 кг
Рік прийняття на озброєння	1940	1939
Термін застосування	до початку 1950-х рр.	до 1947 р.
Кількість випущених комплектів	140 тис.	> 150 * * станом на 22.06.1941
Мережа застосування	тактична ланка	оперативна ланка
Тип шифратора	роторного типу	роторного типу
Реалізований криптоалгоритм	шифр колонної заміни	шифр колонної заміни
Кількість шифрдисків (роторів)	6	4
Наявність інших технічних елементів шифралгоритму (комутатора)	ні	так
Кількість контактів в одному шифрдиску	26	30
Кількість варіантів ключа	1,02×1016 варіантів	3,76×1033 варіантів
Ступінь автоматизації	Неавтоматизована, літеродрукуюча, з виводом інформації на паперову стрічку, з ручним приводом	Автоматизована, літеродрукуюча, з виводом інформації на паперову стрічку, з електричним приводом
Швидкість	до 30 знаків за хвилину	до 200 знаків /хвил.

Таблиця 1 розроблена за даними (Соболева, Т. А. 2002, с. 34–68).

Рис. 8. Шифрувальна апаратура США М-209 (CSP-1500)

Рис. 9. Шифрувальна машина В-211

Радянські конструктори мали в розпорядженні іноземні зразки електромеханічних шифрувальних машин, зокрема німецьку «Енігму» і машину Бориса Хагеліна B-211 (*рис. 9*), яка у фотоілюстраціях джерел (Crypto–Museum. K–37 Crystal R ussian copy of Hagelin B–211. 2012; Нарышкина, А. В., Торкунова, С. Е. 2015, с. 227; Бабиевский, В., Бутырский, Л., Ларин, Д. & Шанкин, Г. 2002) помилково представлена як К-37. Виріб «Кристал» було розроблено на базі машини B-211, яка в даних джерелах помилково зазначена як французька. Насправді, на той час Б. Хагелін (*рис. 10*) був громадянином Швеції і виробництво було організовано в Швеції.

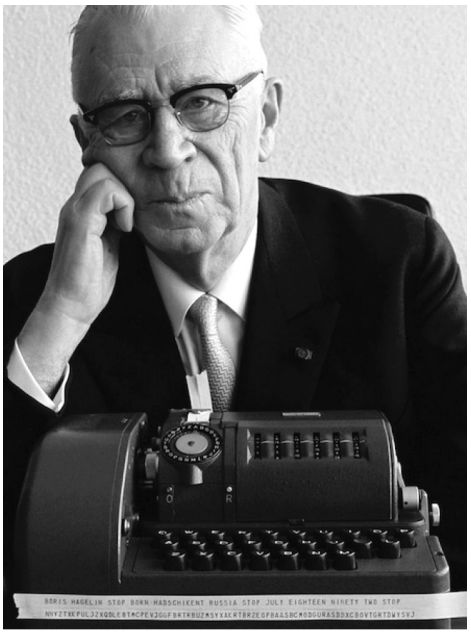

Рис. 10. Борис Хагелін

У 1938 р. для французької армії було виготовлено 500 комплектів B-211. А додатково, за окремим контрактом ще 2 комплекти — для торгової палати СРСР. Правдою є також те, що американська М-209 також сконструйована Б. Хагеліном, якій емігрував до США у 1940 р. А прототипом для B-211 та М-209 була машина С-38 його ж конструкції (*табл. 2*).

Табл. 2

ЗРАЗКИ ВИРОБІВ, ВИГОТОВЛЕНИХ ЗА ПРОТОТИПОМ С-38

Назва зразку	Виробник	Рік виробництва	Кількість шифр дисків/ модуль (кількість літер)	Ступень автоматизації	Швидкість знаків/хв.
С-38	Швеція	1938	6/26	–	25
М-209 (CSP-1500)	США	1940	6/26	–	30
B-211	Швеція	1938	6/26	+	200
К-37	СРСР	1939	6/30	+	220

Таблиця 2 розроблена за даними (Соболева, Т. А. 2002, с. 34-68).

В 1941 р. внаслідок захоплення німецькими військами відбулася компрометація К-37. Це єдиний випадок захоплення противником шифрувальної техніки СРСР під час війни. Дешифрувальники Абверу оцінили його, як криптографічно нестійкий. Радянським командуванням було вжито заходів щодо невикористання цього зразка на Західному фронті. На Далекому Сході машина використовувалася до зняття з озброєння у 1947 р. У 1945-1946 рр. криптограми, зашифровані К-37, дешифрувалися в США спеціально створеним аналогом "Sauterne Mk-I" (Christos military and intelligence corner. 2012).

До початку війни тільки 23 шифрувальних органи ГШ радянського союзу були оснащені технікою спеціального зв'язку, наприкінці війни — вже 130. Техніка спеціального зв'язку була доведена до армійської ланки. Її кількість була незначною та на кінець війни складала всього 396 комплектів (Нарышкина, А. В. & Торкунова С. Е. 2015, с. 2–22; Вдовенко, С. Г. 2008, с. 22). Разом з тим, це вимагало створення системи технічного забезпечення шифрованого зв'язку. З 1938 р. на спеціально створеному відділені курсів «Удосконалення командного складу шифрслужби» почалася підготовка спеціалістів-техніків в обсязі — до 15 офіцерів на рік. З них, відповідно до спільного рішення Генерального штабу та Головного морського штабу, для ВМФ Радянського Союзу — 3–5 офіцерів (Сумароков, В. П. 1999, с. 93).

Шифрувальні машини М-101, К-37, а також лінійні шифратори С-308 та С-309 вироблялися на заводі № 209 (Ленінград). Виробництво не припинялося навіть під час блокади. Крім того, К-37, С-308 та С-309 у період 1942–1945 рр. — на заводі № 707 (Свердловськ). Лінійні шифратори С-308 та С-309 (приставки до телеграфних апаратів) експлуатувалися у військовій стратегічній ланці та на урядових лініях зв'язку з 1939 р. до початку 50–х рр., в оперативній ланці застосовувався військовий телеграфний апарат НТ–20 із приєднуваним до нього шифратором гарантованої стійкості (Бабиевский, В., Бутырский, Л., Ларин, Д. & Шанкин, Г. 2002).

З 1944 р. в тилових мережах фронтів почав застосовуватися кодувальний прилад ВР (М–320) (*рис. 11*), розробка якого проводилася протягом 1936–1939 рр. Виріб мав ручний

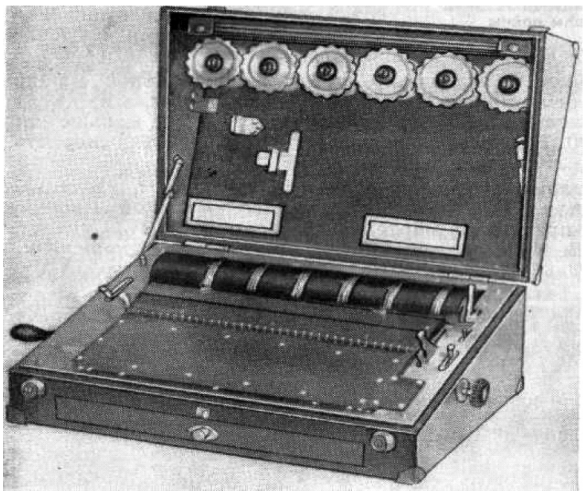

Рис. 11. Кодувальний прилад ВР (М- 320)

привід, був неавтоматизований, характеристики аналогічні М-209 (*табл. 1*), за винятком кількості літер в диску — 30.

Стійкість радянських шифрувальних засобів стратегічної та оперативної ланок управління дозволяла передавати повідомлення будь-якого ступеня секретності. Вона гарантувала нерозкриття противником шифрованих повідомлень навіть за наявності окремих елементів шифру. За свідченнями начальника штабу оперативного керівництва верховного командування Вермахту генерала А. Йодля, полонених дешифрувальників, німцям ніколи не вдавалося розшифрувати радіограми радянської Ставки, штабів фронтів і армій, оскільки вони були стійкими і дешифруванню не піддавалися, незважаючи на відомі їм принципи роботи з шифрами (Бабиевский, В., Бутырский, Л., Ларин, Д. & Шанкин, Г. 2002; Вдовенко, С. Г. 2008, с. 22).

Велика увага в роботі з шифрами надавалася конспірації. Так, під час подій на Халхин-Голі шифрувальний орган був розміщений у звичайній юрті, але під посиленою охороною. Отриманий бойовий досвід здійснення прихованого управління військами показав, що для успішного застосування в РСЧА машинного шифрування необхідна автономна робота шифрувальних органів, їх конспірація та мобільність при передислокації військ. З цією метою у 1939 р. в США було придбано 100 автобусів «Студебекер», переобладнаних під спецапаратні — шифроргани. Таким чином, з'явилася можливість зашифровувати та розшифровувати телеграми не тільки під час зупинок, а й під час руху колон. В 1939–40 рр. був розроблений штабний автобус, обладнаний для роботи шифрорганів (з урахуванням автоматизації). В 1941 р. була вироблена перша партія. А вже в 1944 р. всі шифрувальні органи штабів фронтів і армій РСЧА мали свої спеціальні апаратні, які були обладнані бензоелектричними агрегатами і акумуляторними батареями (Нарышкина, А. В. & Торкунова С. Е. 2015, с. 22–23; Вдовенко, С. Г. 2008, с. 22).

Радянські воєначальники високо цінували результати роботи підлеглих їм шифрувальників та неодноразово відзначали, що шифрувальна робота як підсистема скритого управління військами зіграла ключову роль у системі управління військами (Штеменко, С. М. 1987, с. 469; Баграмян, И. Х. 1988, с. 37, 357).

Висновок. В СРСР напередодні та в ході Другої світової війни створена надійна система шифрованого зв'язку та підсистема її технічного забезпечення. В умовах війни було налагоджено випуск складної електромеханічної шифртехніки, яку від зразків інших держав відрізняла абсолютна криптостійкість. На відміну від збройних сил інших держав-учасників війни, організа-

ційно-технічними заходами було забезпечено вищу ступінь конспірації в роботі з шифрами.

З метою підвищення оперативності та конфіденційності шифрованого зв'язку, з урахуванням розвитку засобів криптоаналізу противника, в умовах повного переходу на цифрові засоби зв'язку, вважається за необхідне досвід розвитку та впровадження шифрувальної техніки в РСЧА і РСЧФ під час Другої світової війни враховувати в сучасних умовах шляхом впровадження в різних ланках управління, в тому числі і тактичній, новітніх національних зразків техніки криптографічного захисту інформації.

Зважаючи на застосування в ЗС України окремих зразків радянської шифрувальної техніки, щодо яких в РФ є повна технічна документація, математична модель криптоалгоритму, правила роботи, що значно спрощує криптоаналіз, ми наголошуємо на нагальності вирішення даних пропозицій. Особливо актуальними вони є для підготовки та ведення операцій Збройних Сил України, зокрема операції Об'єднаних сил на території Донецької та Луганської областей.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ І ЛІТЕРАТУРИ

Бабаш, А. В. & Шанкин, Г. П. (2002). *История криптографии* (в 2 т. т. 1). Москва: Гелиос АРВ, 73 с.

Бабиевский, В., Бутырский, Л., Ларин, Д. & Шанкин, Г. (2002). Советская шифровальная служба: 1920–40-е. Защита информации. INSIDE. URL: http://www.agentura.ru/press/about/jointprojects/inside-i/sovietcryptoservice [дата зверн.: 05.04.2021].

Баграмян, И. Х. (1988). *Так начиналась война.* Киев: Політвидавництво України, 180 с.

Василевский, А. М. (1973). *Дело всей жизни* (в 2 т., т. 1). Москва: Знамя, 206 с.

Вдовенко, С. Г. & Даник, Ю. Г. (2017). Концептуальні напрями комплексного вирішення проблеми захисту інформації в системі скритого управління збройних сил. Сучасні інформаційні технології у сфері безпеки та оборони. *Науковий журнал*, № 2 (29), с. 98–106.

Вдовенко, С. Г. (2001). Забезпечення збереження таємниць та вимог прихованого управління в операціях Другої світової війни. *Військові відомості*, 5 червня № 21 (98), с. 13.

Вдовенко, С. Г. (2008). Юстас — Алексу. *Журнал. Військо України*, № 05 (95), с. 22–23.

Вдовенко, С. Г., Даник, Ю. Г. & Пермяков, О. Ю. (2020). Досвід розвитку систем кібербезпеки та кібероборони провідних країн світу. Сучасні інформаційні технології у сфері безпеки та оборони. *Науковий журнал*, № 1 (37), с. 31–48. DOI: 10.33099/2311-7249/2020-37-1-31-48.

Волинець, С. І. (2007). Скритий зв'язок високої проби. *Народна армія*, 25 грудня № 236, с. 5.

Всё о Второй мировой. Исторический, научно-образовательный сайт о Второй мировой войне. Шифровальные устройства СССР. (2016). URL: http://wwii.space/shifrovalnyie-ustroystva-sssr [дата зверн.: 05.04.2021].

Гребенніков, В. (2009). Ужгород. Історія криптології & секретного зв'язку. Видання друге, виправлене, доповнене, ілюстроване. Аппаратура засекречивания и техника шифрования СССР URL: https://reibert.info/media/albums/apparatura-zasekrechivanija-i -texnika-shifrovanija-sssr.10860/; https://reibert.info/media/m-100-spektr.466114; https://reibert.info/media/ moj-kniga-na-ukrainskom.466125/ [дата зверн.: 05.04.2021].

Єсіна, М. І., Вдовенко, С. Г. & Горбенко, І. А. (2019). Моделі безпеки постквантових асиметричних шифрів на основі нерозрізнюваності. *Збірник наукових праць*. № 16, с. 15–26. DOI: 10.46972/2076-1546.2019.16.02.

Жуков Г. К. (1969). *Спогади і роздуми.* Київ: Політвидавництво України, 356 с.

К-37 «Кристалл». Материал из Википедии — свободной энциклопедии. (2012). URL: https://ru.wikipedia.org/wiki/К-37_«Кристалл» [дата зверн.: 05.04.2021].

Кан, Д. Е. (2000). *Взломщики кодов.* Москва: Издательство Центрполиграф, 130 с.

Нарышкина, А. В. & Торкунова С. Е. (2015). *Криптографы вступают в бой.* (В 7 т., т. 7). Москва: МГИМО, 458 с.

Сеоев, В. Б., Мазуркевич, Р. В., Петров, Б. Н. & Шеховцов, Н. И. (1986). *Внезапность в наступательных операциях Великой Отечественной войны.* Москва: Наука, 234 с.

Соболева, Т. А. (2002). *История шифровального дела в России.* Москва: «ОЛМА–ПРЕСС», 130 с.

Сумароков, В. П. (1999). *Военная профессия — шифровальщик.* Москва: РНТ-технологии безопасности, 174 с.

Шеннон, К. Е. (1963). *Теория связи в секретных системах. Работы по теории информации и кибернетики.* Москва: Иностранная литература, 560 с.

Штеменко, С. М. (1987). *Генеральний штаб у роки війни.* Київ: Видавництво політичної літератури України, 908 с.

Bob, Lord's Crypto Museum. (2019). B., Bob Lord. The U.S. Army used the M-209 encryption device during WWII. URL: https://www.ilord.com/m-209. [дата зверн.: 05.04.2021].

Christos military and intelligence corner. Military and intelligence history mostly dealing with World War II. Thursday, The Soviet K-37 'Crystal' cipher machine. (2012). June 14. URL: http://chris-intel-corner.blogspot.gr/2012/06/soviet-k-37-crystal-cipher-machine.html. [дата зверн.: 05.04.2021].

Crypto-Museum. K-37 Crystal Russian copy of Hagelin B-211. (2012). URL: https://www.cryptomuseum.com/crypto/ussr/k37/index.htm [дата зверн.: 05.04.2021].

Gorbenko, I., Kuznetsov, A., Gorbenko, Yu., Alekseychuk, A. & Tymchenko, V. (2018). *Stream Cipher. Computer Science and Cyber security.* № 1 (9), "Strumok", p. 8–9.

Gorbenko, I., Kuznetsov, A., Gorbenko, Yu., Vdovenko, S., Tymchenko, V. & Lutsenko, M. (2019). *Studies on Statistical Analysis and Performance Evaluation for Some Stream Ciphers. International Journal of Computing.* № 18 (1), p. 82–88.

REFERENCES

Babash, A. V. & Shankin, G. P. (2002). *Istoriya kriptografii* [Cryptography history]. (Vol.1). Moskva: Gelios ARV, 73 s. [in Russian].

Babiyevskiy, V., Butyrskiy, L., Larin, D. & Shankin, G. (2002). Sovetskaya shifroval'naya sluzhba: 1920–40-e. Zashchita informatsii [Soviet encryption service: 1920–40-s. Data protection]. INSIDE. URL: http://www.agentura.ru/press/about/jointprojects/inside-i/sovietcryptoservice [data zvern.: 05.04.2021]. [in Russian].

Bagramyan, I. KH. (1988). *Tak nachinalas' voyna* [So the war began]. Kyiv: Polítvidavnitstvo Ukraíni, 180 s. [in Russian].

Vasilevskiy, A. M. (1973). *Delo vsey zhizni* [Life's work. Moscov]. (Vol. 1). Moskva: Znamya, 206 s. [in Russian].

Vdovenko, S. H. & Danyk, YU. H. (2017). Kontseptualni napryamy kompleksnoho vyrishennyu problemy zakhystu informatsiyi v systeme skryty upravlinnya Zbroynykh syl. Suchasni informatsiyni tekhnolohiyi u sferi bezpeky ta oborony [Conceptual directions of complex solution of the problem of information protection in the system of hidden control of the armed forces. Modern information technologies in the field of security and defense]. *Naukovyy zhurnal*, № 2 (29), s. 98–106. [in Ukrainian].

Vdovenko, S. H. (2001). Zabezpechennya Zberezhennya Tayemnyts ta vymoh prykhovanoho upravlinnya v operatsiyakh Druhoyi Svitovoyi Viyny [Securing secrets and Secret management requirements in the II World War Operations]. *Viyskovi Vidomosti*, 5 chervnya № 21 (98), s. 13. [in Ukrainian].

Vdovenko, S. H. (2008). Yustas — Aleksu. [Justas — Aleksu] *Zhurnal. Viysko Ukrayiny*, № 05 (95), s. 22–23. [in Ukrainian].

Vdovenko, S. H., Danyk, YU. H. & Permyakov, O. YU. (2020). Dosvid rozvytku system kiberbezpeki ta kiberoboroni providnikh stran svitu. Suchasni informatsiyni tekhnolohiyi u sferi bezpeky ta oborony [Experience in the development of cyber security and cyber defense systems of foreign countries. Modern information technologies in the field of security and defense]. *Naukovyy zhurnal*, № 1 (37), s. 31–48. DOI: 10.33099 / 2311-7249 / 2020-37-1-31-48. [in Ukrainian].

Volynets, S. I. (2007). Skrytyy zv'yazok visokoyi prob [Hidden bundle of high quality]. Narodna armiya, 25 grudny, s. 5. [in Ukrainian].

Vse pro Druhu svitovu. Istorychnyy, naukovo-osvitniy sayt pro Druhu svitovu viynu. Shyfruvalni prystroyi SRSR [All about WWII Historical scientic site about WWII USSR]. (2016). URL: http://wwii.space/shifrovalnyie-ustroystva-sssr [data Zverny.: 05.04.2021]. [in Russian].

Hrebennikov, V. (2009). Uzhhorod. Istoriya kriptolohiyi & sekretnoho zv'yazku. Vydannya druhe, vypravlennya, dopovnene, ilyustrovane. Aparatura zasekrechuvannya ta tekhnika shyfruvannya SRSR [History of cryptology and secret communication]. URL: https://reibert.info/media/albums/apparatura zasekrechivanija i texnika shifrovanija sssr.10860/;https://reibert.info/media/m-100-spektr.466114; https://reibert.info/media/ moj-kniga-na-ukrainskom.466125 / [data Zverny.: 05.04.2021]. [in Ukrainian].

Yesina, M. I., Vdovenko, S. H. & Horbenko, I. A. (2019). Modeli bezpeky postkvantovikh asymetrychnyy shifriv na osnove nerozriznyuvanosti [Security models of post-quantum asymmetric ciphers based on indistinguishability]. *Zbirnyk naukovykh prats*. № 16, s. 15–26. DOI: 10.46972 / 2076-1546.2019.16.02. [in Ukrainian].

Zhukov H. K. (1969). *Spohady y rozdumy* [Memories and reflections]. Kyiv: Politvidavnitstvo Ukrayiny, 356 s. [in Ukrainian].

K-37 "Krystal" [Diamand]. Material z Vikipediyi — vilnoyi entsyklopediyi. (2012). URL: https://ru.wikipedia.org/wiki/K-37_«Krystall»[data Zverny .: 05.04.2021]. [in Russian].

Kan, D. YE. (2000). *Zlomshchyky kodiv* [The codebreakers]. Moskva: Vydavnytstvo Tsentrpolihraf, 130 s. [in Russian].

Naryshkina, A. V. & Torkunova S. YE. (2015). *Kryptohrafy vstupayut v biy* [Cryptographs enter the fray] (Vol. 7). Moskva: MHYMO, 458 s. [in Russian].

Seoev, V. B., Mazurkevych, R. V., Petrov, B. N. & Shekhovtsov, N. I. (1986). *Raptovist v nastupalnykh operatsiyakh Velykoyi Vitchyznyanoyi viyny* [Surprise in the offensive operations of the Great Patriotic War]. Moskva: Nauka, 234 s. [in Russian].

Sobolyeva, T. A. (2002). *Istoriya shyfruvalnoho spravy v Rosiyi* [The history of encryption in Russia]. Moskva: "OLMA-PRESS", 130 s. [in Russian].

Sumarokov, V. P. (1999). *Viyskova profesiya — shyfruvalnyk* [Military profession — cryptographer]. Moskva: RNT-tekhnolohiyi bezpeky, 174 s. [in Russian].

Shennon, K. E. (1963). *Teoriya zv'yazku v sekretnykh systemakh. Roboty po teoriyi informatsiyi i kibernetyky* [Communication theory in secret systems. Works on information theory and cybernetic]. Moskva: Ynostrannaya lyteratura, 560 s. [in Russian].

Shtemenko, S. M. (1987). *Heneralnyy shtab u roky Viyny* [General Staff during the war]. Kyyiv: Vydavnytstvo Politychnoyi literatury Ukrayiny, 908 s. [in Ukrainian].

Bob, Lord's Crypto Museum. (2019). B., Bob Lord. The U.S. Army used the M-209 encryption device during WWII. URL: https://www.ilord.com/m-209. [дата зверн.: 05.04.2021]. [in English].

Christos military and intelligence corner. Military and intelligence history mostly dealing with World War II. Thursday, The Soviet K-37 'Crystal' cipher machine. (2012). June 14. URL: http://chris-intel-corner.blogspot.gr/2012/06/soviet-k-37-crystal-cipher-machine.html. [дата зверн.: 05.04.2021]. [in English].

Crypto-Museum. K-37 Crystal Russian copy of Hagelin B-211. (2012). URL: https://www.cryptomuseum.com/crypto/ussr/k37/index.htm [дата зверн.: 05.04.2021]. [in English].

Gorbenko, I., Kuznetsov, A., Gorbenko, Yu., Alekseychuk, A. & Tymchenko, V. (2018). *Stream Cipher. Computer Science and Cyber security.* № 1 (9), "Strumok" p. 8–9. [in English].

Gorbenko, I., Kuznetsov, A., Gorbenko, Yu., Vdovenko, S., Tymchenko, V. & Lutsenko, M. (2019). *Studies on Statistical Analysis and Performance Evaluation for Some Stream Ciphers. International Journal of Computing.* № 18 (1), p. 82–88. [in English].

Serhii Vdovenko
Master of State Military Management
in the field of defence, Associate Professor
of the Communication and Information Systems
Department of the Tropes (Forces) Support
and Information Technologies Institute,
The National Defence University of Ukraine
named after Ivan Cherniakhovskyi
(Kyiv, Ukraine)
ORCID https://orcid.org/0000-0001-8139-7975

Mykola Hulkov
Lecturer at the Department
of the Communication and Information Systems
Department of the Tropes (Forces) Support
and Information Technologies Institute
The National Defence University of Ukraine
named after Ivan Cherniakhovskyi
(Kyiv, Ukraine)
ORCID https://orcid.org/0000-0003-1883-4954

Serhii Sydorov
Doctor of Sciences (History), Full Professor,
Professor of the Department of History
of Wars and Martial Arts, Institute
of State Military Administration
The National Defence University
of Ukraine named after Ivan Cherniakhovskyi
(Kyiv, Ukraine)
ORCID https://orcid.org/0000-0002-1961-4251

Volodymyr Dzhola
Student of group 4109 of the Tropes (Forces)
Support and Information Technologies Institute
The National Defence University
of Ukraine named after Ivan Cherniakhovskyi
(Kyiv, Ukraine)
ORCID https://orcid.org/0000-0002-9344-7172

MEANS OF CRYPTOGRAPHIC INFORMATION PROTECTION OF THE USSR DURING THE SECOND WORLD WAR

The article examines the ways of creating and developing the technology of cryptographic information protection in the USSR on the eve and during the Second World War and their impact on the command and control system of Workers and Peasants Red Army and Navy. The theory of "deep operation", in fact — the military strategy of the USSR at that time, was a result of the technical progress of the means of armed struggle, in particular the means of communication. Changes in views on the organization of troops, their operational structure, the spatial and temporal characteristics of operations required fundamental changes in troop command and control and organization interaction of joint groupings. One of the ways to achieve this goal was the automation of information encryption processes.

Undoubtedly, the scientific and technological progress affects the forms and methods of warfare. The development of weapons and military equipment, forms and methods of their use requires implementation of the communication and informatization systems, technical intelligence, cryptanalysis.

The requirements are examined to be considered for increasing the secrecy and efficiency of command and control of troops within the preparation and during the conduct of operations, including Joint Forces Operations, based on the experience gained by the USSR.

Key words: *confidentiality, cryptographic protection of information, efficiency, covert command and control of troops, secrecy, encryption machine, encryption authority, encryption equipment.*