УДК 681.188.000.93
DOI: 10.33099/2707-1383-2022-45-3-158-179

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
доктор історичних наук, професор, 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

Сергій Пашкевич
слухач навчальної групи 4210, Інститут забезпечення військ (сил) та інформаційних технологій, Національний університет оборони України імені Івана Черняховського (Київ, Україна)
ORCID: https://orcid.org/0000-0001-8768-6508
Електронна пошта: Paschka@i.ua

ТЕХНІКА КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ НАЦИСТСЬКОЇ НІМЕЧЧИНИ ПЕРІОДУ ДРУГОЇ СВІТОВОЇ ВІЙНИ

У статті розглядаються питання застосування засобів криптографічного захисту інформації Німеччини в період Другої світової війни. Теорія «бліцкрігу» висунула вимоги щодо підвищення оперативності та скритності управління військами, що досягалося впровадженням шифрувальної техніки. Але, системні помилки у сфері організації та забезпечення безпеки криптографічного захисту інформації вплинули на поразку нацистської Німеччини.

Вирішення завдань скритності управління під час підготовки та проведення операції в умовах сьогодення, вимагають врахування та використання в Україні та її Збройних Силах досягнень науково-технічного прогресу у сфері криптографічного захисту інформації з обов'язковим запобіганням можливим системним помилкам.

Ключові слова: *Ключова система, конфіденційність, криптографічний захист інформації, оперативність, приховане управління військами, скритність, шифрувальна техніка, шифрувальна машина.*

Постановка проблеми. Виходячи зі стратегій та воєнних доктрин 1920–30-х років XX століття, оперативно-технічні умови операцій, вимагали одночасного забезпечення секретності й високої оперативності доведення інформації, що циркулює під час управління військами при підготовці та проведенні операцій. В ряді країн світу були розроблені та прийняті на озброєння електромеханічні шифрувальні машини (Вдовенко, С. Г., Гульков, М. О., Сидоров, С. В. & Джола, В. О. 2021, с. 98; Вдовенко, С. Г., Гульков, М. О., Сидоров, С. В. & Вдовенко, О. Г. 2021, с. 134). Стався стрімкий розвиток криптографії та криптоаналізу, що згодом поєдналися в єдину науку — криптологія. Все це значною мірою впливало та й надалі буде впливати на всі етапи підготовки і ведення операцій та бойових дій, докорінно змінюючи в нових умовах зміст заходів щодо управління військами та порядок їх виконання (Вдовенко, С. Г., Даник, Ю. Г. & Пермяков, О. Ю. 2020, с. 33).

Огляд основних досліджень. Розвиток засобів криптографічного захисту інформації Німеччини першої половини XX століття можна прослідкувати за публікаціями в науково-історичній періодиці та з електронних джерел, визначених у списку використаних джерел і літератури. (Уинтерботэм, Ф. А. 1991, с. 176). В Україні це питання майже не досліджувалося.

У даній статті розкрити питання забезпечення криптографічної стійкості та оперативності, ніж розвиток безпосередньо технічних засобів криптографічного захисту, а також вплив цих технічних рішень та процедур на перебіг воєнних дій з точки зору воєнно-історичного аналізу.

Мета статті — на основі проведеного аналізу показати за якими напрямками розвивалися засоби криптографічного захисту інформації Німеччини на передодні та впродовж Другої світової війни, а також визначити окремі системні недоліки у системах криптографічного захисту інформації третього Рейху, що значною мірою вплинули на результати війни.

Виклад основного матеріалу. В німецькій армії і на флоті на рубежі 1920–1930 років для передачі кодованих повідомлень використовувалися кодові книги та диски. Диски використовувалися в парі та утворювали ініціали ES (*рис. 1*). Існувало 5 великих або так званих E-дисків (13 см), і 5 маленьких або S-дисків (10 см). Великі диски були позначенні як німецькі імена Eberhard, Ernst, Erasmus, Egbert, Emil. Кожен з великих дисків мав 58 секторів розмічених від 1 до 31 (ймовірно дні місяця). Малі диски мали кодові позначення за типовими німецькими прізвищами Schmidt, Schilling, Schneider, Schulze, Seidel. Кожен малий диск мав 58 секторів розмічених від 1 до 58. Малі диски встановлювалися на одну вісь з великими та обертаючись відносно один одного утворювали кодові послідовності (German, E. S. Code Disks. 2021).

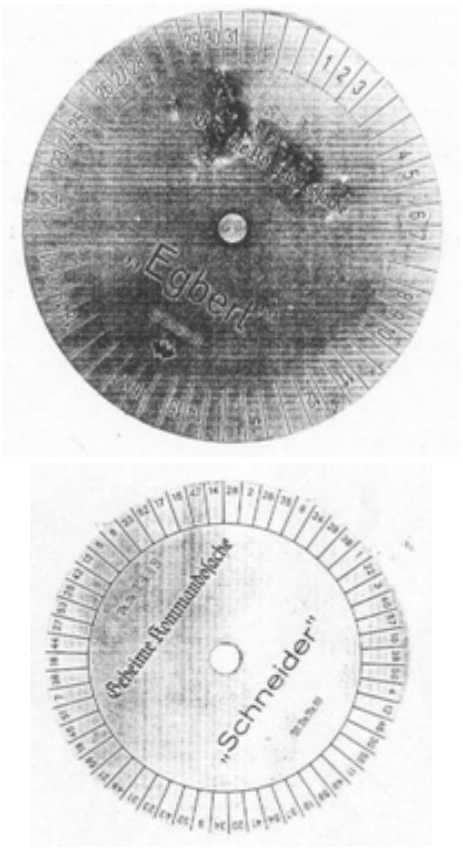

Рис. 1. Німецькі кодові диски ES

ES система використовувалися з радіокодом "Funkbuch für Schießübungen" для кодування сигналів відповідно до Інструкції по кодуванню сигналів та Інструкції для служби кодування підводних човнів 1940 р. M.Dv. Nr. 111 (Marine Dienstvorschrift Number 111). Кодування та розкодування повідомлень з використанням системи займало десятки хвилин. Маючи диски та описи дії ключів, захоплені на німецьких підводних човнах і суднах забезпечення, англійські криптоаналітики з успіхом дешифрували повідомлен-

ня закодовані за допомогою ES системи. (Smith, Michael. 1998, с. 78).

Для шифрування дипломатичних повідомлень в Німеччині застосовувалася портативна механічна шифрувальна машина “Kryha” (*рис. 2*), (Kryha. From Wikipedia, the free encyclopedia. 2021), що була розроблена на початку 1920 р. Існували, як кишенькові моделі “Kryha”, так й великі електричні, вагою 5 кг. “Kryha” не забезпечувала достатнього рівня криптографічної стійкості. Так, на дешифрування криптограми з 1135 знаків американські криптоаналітики витрачали близько двох годин.

Рис. 2. Шифрувальна машина “Kryha”

На передодні та у період Другої світової війни у Німеччині відбувся стрімкий розвиток озброєння та військової техніки, в т.ч. — криптографічних засобів. Найбільш відомою шифрувальною машиною, що на передодні та під час Другої світової війни застосовувалася Німеччиною та її союзниками для шифрування цілком таємних повідомлень, була “Enigma” (древньогрецькою — загадка). Це загальна назва ряду модифікацій однотипних електромеханічних дискових (роторних) шифрувальних машин, які реалізують багатоалфавітний шифр колонної заміни.

Машина перебувала на озброєнні у Вермахті, Люфтваффе, Крігсмаріне, в Абвері (військової розвідці), та була доведена до дивізії, окремого полку, корабля, бомбардувальника дальньої дії. Її модифікація “Heidrig-Enigma” використовувалась в Міністерстві закордонних справ, на залізничному транспорті і в економіці. Поставлялася також на експорт до інших держав та використовувалася як комерційна модель. (Ларин, Д. А. & Шанкин, Г. П. 2014, с. 123).

Вперше “Enigma” була створена голландським винахідником Хьюго Кочем та у 1917 р. запатентована у США (патент № US1675411A) (*рис. 3*). (US1657411A. Ciphering machine — Google Patents 2021).

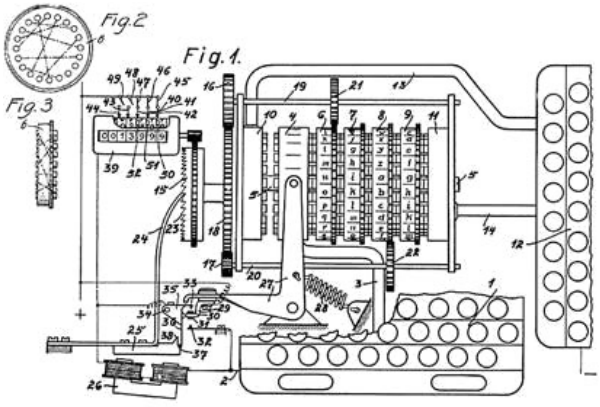

Рис. 3. Патент № US1675411A, схема комутації шифрдисків

У 1918 р. патент був перекуплений німецьким інженером та підприєм-

цем Артуром Шербіусом, якій у середині 20-х років XX століття розпочав продаж машини моделі "Enigma-B" для захисту комерційної таємниці. Її габарити та маса складали, відповідно: 650 × 450 × 350 мм, 50 кг (*рис. 4*) (Kahn, David. 1991, с. 223).

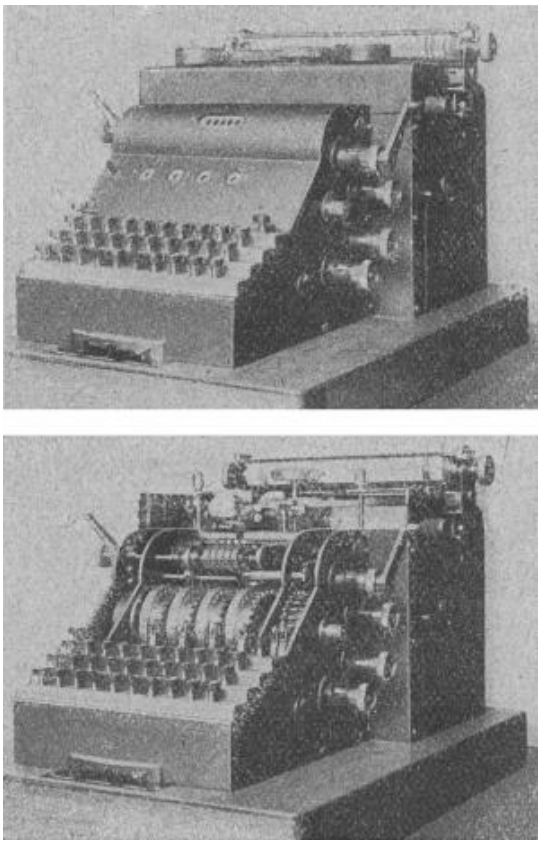

Рис. 4. Шифрувальна машина "Enigma B"

З 1925 р. до кінця Другої світової війни корпорацією "Chiffriermaschinen AG" було виготовлено понад 100 тис. (Черняк, Л. 2003, с. 35), за іншими даними близько 200 тис. машин "Enigma" різних модифікацій (Hamer, David H., Sullivan, Geoff & Weierud, Frode. 1998).

У 1928 р. Вермахтом була запроваджена власна розробка шифрувальної машини на базі "Enigma" під назвою "Enigma G", модифікованої у 1930 р. до моделі "Enigma I". Ця модель використовувалась армійськими частинами, військовими службами та іншими державними організаціями. Розміри машини складали 280 × 340 × 150 мм, а вага складала біля 12 кг (*рис. 5*) (Louis Kruh and Cipher Deavours the commercial enigma: beginnings of machine cryptography. 2021).

Рис. 5. Шифрувальна машина "Enigma I"

Військові моделі машини випускались з різною кількістю шифрдисків. У першій моделі комплектність складала 3 диски, усі з яких використовувалися в процесі шифрування. З кінця 1938 р. до комплекту машини входило 5 дисків, для шифрування використовувалося так само — 3 диски.

Військово-морська модель "M4" (*рис. 6*) (Louis Kruh and Cipher Deavours the commercial enigma: begin-

nings of machine cryptography. 2021), мала 4 шифрдиски, хоча мала такі самі габарити. Пізніш модифікації для військово-морських сил виготовлялися з більшою кількістю шифрдисків в комплекті: 6, 7 або 8. Вони маркувалися римськими цифрами від I до VIII. (Kahn, David. 1991, с. 197). (*табл. 1*). *Таблиця 1* складена за матеріалами (Hamer, David H., Sullivan, Geoff & Weierud, Frode. 1998, с. 44).

Рис. 6. Шифрувальна машина “Enigma M4”

Таблиця 1.

МОДИФІКАЦІЇ ШИФРМАШИНИ “ENIGMA”

Рік	Тип	маса	кількість				елементи конструкції			користувачі
			дисків шифратора	дисків в комплекті	контактів диску	знаків клавіатури / електричного табло	комутатор	відбивач / кількість кутових положень	пристрій друку	
Комерційні та експортні моделі										
1923	“Enigma A”	50	3	3	28	28/–	–	–	+	
1924	“Enigma B”	50	3	3	28	28/–	–	–	+	
1926	“Enigma C”	12	3	3	28	28/–	–	+/2	–	
1927	“Enigma D”	12	3	3	26	26/26	–	–	–	Англія,США, Голландія, Італія, Іспанія, Польща, Швеція, Японія
1940	“Enigma K”	12	3	3	26	26/26	–	–	–	Швейцарія
1942	“Enigma T” (Tirpiz)	12	4	8	26	26/26	–	+/1	–	Японія

Рік	Тип	маса	кількість				елементи конструкції			користувачі
			дисків шифратора	дисків в комплекті	контактів диску	знаків клавіатури / електричного табло	комутатор	відбивач / кількість кутових положень	пристрій друку	
Моделі для збройних сил										
1926	“Enigma M-4” (Kriegsmarine M4)	12	4	4	26	26/26	–	–	–	Крігсмаріне
1926	“Enigma C” (Funkschlüssel C)	12	3	3	28	26/26	–	–	–	Вермахт
1928	“Enigma G”	12	4	4	26	26/26	–	–	–	Абвер
Enigma I										
1930	“Enigma Z”	12	4	4	10	10/10	–	–	–	Люфтваффе
1930	“Enigma I”	12	3	5	26	26/26	+	+/4	–	Вермахт
1933										Люфтваффе
1931	“Enigma G31” (Umkehrwalze A)	12	4	4	26	26/26	+	+/26	–	Абвер
1934		12	3	6	26	26/26	+	+/4	–	Вермахт
1935										Люфтваффе
1937	(Umkehrwalze B)	12	3	7	26	26/26	+	+/4		Вермахт Люфтваффе
1941	(Umkehrwalze C)	12	3	8	26	26/26	+	+/4	–	
1934	“Enigma M” (Funkschlüssel M)	12	4	6	26	26/26	+	+/4	+	Крігсмаріне
1939		12	4	8	26	26/26	+	+/4	+	
1939	“Reichsbahn Enigma”	12	4	4	26	26/26	+		–	Рейхсбан
1942	“Enigma M4” (Triton)	12	4	8	26	26/26	+	+/26	+	Крігсмаріне
1942	“Enigma T”		4	8	26	26/26	+	+	–	Крігсмаріне
1944	“Enigma I” (Umkehrwalze D)	12	4	8	26	26/26	–	+/26	–	Абвер
Enigma II										
1933	“Enigma H” (Enigma II)		8	8	26		+	+	+	Стратегічна ланка

Машина комбінувала у своєму складі як механічні так і електричні системи. Вона складалася з блоку шифрдисків (*рис. 7*), клавіатури і лампових індикаторів (*рис. 8*). (Шифрувальні машини і криптологія. Технічні деталі. Enigma machine. 2021). Військовий зразок машини мав модуль 26 (кількість літер що використовуються для обробки та відображення інформації) на відміну від модуля 28 в комерційної моделі (Kruh, Louis & Deavours, Cipher. 2002, с. 15). Основна відмінність між комерційними та військовими зразками полягала у наявності в останніх комутаційної панелі клавіатури для зміни попарної комутації контактів букв (*рис. 9*) (Шифрувальні машини і криптологія. Технічні деталі. Enigma machine. 2021), що урізноманітнювало варіанти комутації електричних ланцюгів та суттєво збільшувало рівень криптографічної стійкості шифрувальної машини. Повідомлення, що підлягало шифруванню, вводилось з клавіатури машини. При натисканні на клавішу, електричний струм проходив через електричний ланцюг, утворений шифрдисками, що обертаються, і комутатором (*рис. 9*) та вмикав один з індикаторів (*рис. 8*). Текст криптограми записувався на бланк, а потім передавався традиційним шляхом (радіо, телефон, телеграф). При чому шифрувальники Вермахту та Люфтваффе відправляли криптограми п'ятизначними групами. Шифрувальники Кригсмаріне, що використовували 4-х дискову версію машини, відправляли повідомлення групами по 4 символи.

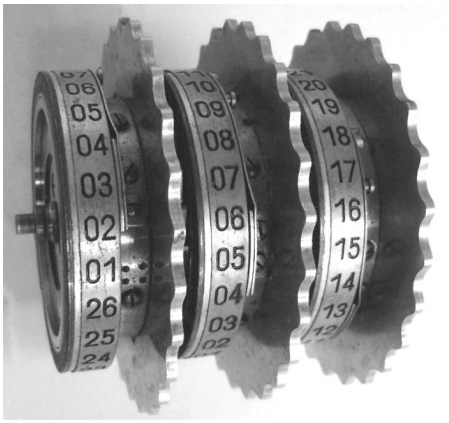

Рис. 7. Блок шифрдисків "Enigma"

Рис. 8. Клавіатура і панель

Рис. 9. Комутаційна панель

Розшифрування криптограми відбувалась зворотнім шляхом: оператор вводив зашифровані символи на

клавіатурі, а розшифрований символ відображався на клавіатурі шляхом увімкнення лампочки, розташованої під відповідною літерою. Увімкнення лампочок фіксував та записував на бланк розшифрований текст інший оператор.

Ключі до машини друкувались в спеціальних шифрувальних книгах. Більшість ключів зберігалась лише визначений період часу, зазвичай одну добу. Для кожного нового повідомлення задавались нові ключі.

Криптостійкість системи майже повністю залежала від механізму руху шифрдисків, що так би мовити, був примітивним. З повним обертанням (на 26 обертів) диска № 1, диск № 2 здійснював свій перший крок. Криптографічний період шифратора складав 26x26x26=17576 циклів. З 1926 р. у всіх моделях машини, починаючи з "Enigma C", було застосовано відбивач електричного сигналу, або рефлектор, винахід партнера Шербіуса Віллі Корна (Willi Korn), що збільшило криптографічний період до 35152 циклів. З метою його більш суттєвого збільшення у виробі було застосовано комутатор, утворюючий додаткові змінні шифруючи ланцюги. Порядок комутації ланцюгів також складав частину ключа. Таким чином, криптографічний період машини було збільшено до числа 10^{92}, що німцями вважалося цілком достатнім (Marks, Philip & Weierud, Frode. 2000, с. 57).

Однак, така впевненість дорого коштувала німцям — значна кількість криптограм зашифрованих за допомогою "Enigma" дешифрувалася. (Hinsley, F. H. & Stripp, Alan. 1993, с. 85).

По-перше, як видно з *табл. 1*, комерційні та експортні варіанти "Enigma" використовували і інші країни. Криптограми таких машин були дешифровані криптоаналітиками: спочатку польськими, потім ними ж у французькому розвідувальному центрі, а згодом спираючись на їхні напрацювання, але використовуючи розвідувальну інформацію та новітні досягнення науки й техніки — англійськими та американськими. (Smith, Michael. 1998, p. 445). При дешифруванні був використаний суттєвий конструктивний недолік машини — неспроможність шифрування знаку повідомлення в той самий знак, що значно підвищувало ймовірність дешифрування криптограми противником шляхом криптоаналізу (Hinsley, F. H. & Stripp, Alan. 1993, p. 84).

По-друге, виріб не забезпечував належної криптостійкості й з інших, організаційних, причин. Наприклад, масове застосування одного типу шифрувальної техніки у всіх ланках управління, за умов чисельних порушень шифрувальниками правил роботи, знижувало криптографічну стійкість системи.

По-третє, і головне, систематично порушувалися вимоги щодо режиму

секретності в ході розробки та виробництва засобів криптографічного захисту інформації, а також — щодо забезпечення безпеки шифрованого зв'язку при їх застосуванні (Kahn, David. 1991, p. 244). Крім того, конструктивні особливості виробу, вимагали одночасної роботи на одному комплекті 2–3 осіб, що також знижувало рівень конфіденційності.

Необхідно відмітити, що спеціально для здійснення зв'язку між німецьким та японським військовими флотами на базі "Enigma K" в 1942 р. була розроблена модифікація шифратора "Enigma T" (Enigma TIRPITZ) (*рис. 10*) (Enigma T. Photo. 2021). Вона була обладнана одним відбивачем і 8 шифрдисками в комплекті, що забезпечувало більшу криптостійкість в порівнянні з попередніми моделями "Enigma". Не менше 244 машин було виготовлено та частково відправлено до Японії. Частина машин при транспортуванні була втрачена, а деякі — захоплені військами США.

Рис. 10. Enigma TIRPITZ

Окремо в цьому ряду, слід відмітити дві модифікації: "Enigma Z" (*рис. 11*) (Enigma Z. Photo. 2021), використовувалась у Люфтваффе для шифрування метеорологічних повідомлень, мала лише 10 цифрових клавіш, 10 індикаторів від 0 до 9 та конструктивно не мала комутатора та рефлектора; "Enigma H", або Enigma II незначний період часу використовувалася для шифрованого зв'язку між міністерствами та штабами стратегічного рівня, була автоматизованою, літеро друкуючою. У комплекті мала 8 шифрдисків, які усі встановлювалися до шифратора, комутатор та рефлектор. Виявилася не надійною в експлуатації та була знята з озброєння.

Рис. 11. "Enigma Z"

На початку війни у Німеччині була розроблена та з 1941 р. на підприємстві Вандер-верк у Хемніці випускалася шифрувальна машина SG-41 "Hitlermuhle" ("Hitler Mill")

(*рис. 12*), що призначалася на заміну машині "Enigma" (SG-41. Collection Deutsches Museum No. 2013-1092. 2021) SG-41 мала роторний шифратор з шести шифрдисків та дозволяла зашифровувати і розшифровувати повідомлення в попередньому (автономному) режимі роботи з виводом на друкуючий пристрій, котушки із двома паперовими стрічками (для зашифрованого і розшифрованого тексту) розташовувалася в піддоні машини. В дію шифрмашина приводилася механічним способом. SG-41 була розроблена на основі шифрувальної машини Б. Хагеліна С-38. Значна кількість конструкторських рішень було скопійовано з цього зразку, як до речі й у К-37 (СРСР) та М-209 (США) (*табл. 2, 3*). *Таблиці 2, 3* складені за матеріалами (Вдовенко, С. Г., Гульков, М. О., Сидоров, С. В. & Джола, В. 2021, с. 103–105; Вдовенко, С. Г., Гульков, М. О., Сидоров, С. В. & Вдовенко, О. Г. 2021, с. 135).

Рис. 12. Шифрувальна машина "SG-41"

Хоча, слід відмітити, новим в даному зразку було те, що шостий шифрдиск керував кутом розвороту всіх інших, ускладнюючи криптоалгоритм шифратора SG-41. Сам винахідник спростовував наявність будь-яких ліцензійних угод з німецьким урядом або промисловістю.

Таблиця 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 (до 50)
SG-41	Німеччина	1941	6/26	-	30
В-211	Швеція	1938	6/26	+	200
К-37	СРСР	1939	4/30	+	220

Таблиця 3

ПОРІВНЯЛЬНА ТАБЛИЦЯ СЕРІЙНИХ ЗРАЗКІВ ШИФРТЕХНІКИ ПРОТИБОРЧИХ СТОРІН, СТВОРЕНИХ НА ОСНОВІ ШИФРАТОРА Б. ХАГЕЛІНА С-38

Найменування	**К-37**	**М-209 (CSP-1500)**	**SG-41**
Держава	СРСР	США	Німеччина
Офіційне найменування	малогабаритна дискова кодувальна машина	портативна шифрувальна машина	Ключовий пристрій 41
Маса	19 кг	2,7 кг	13,5 кг
Рік прийняття на озброєння	1939	1940	1941
Термін застосування	до 1947 р.	до 1950-х р.р.	до 1945
Кількість випущених комплектів	> 150 * * станом на 22.06.1941	140 тис.	2000
Мережа застосування	оперативна ланка	тактична ланка	тактична ланка
Тип шифратора	роторного типу	роторного типу	роторного типу
Реалізований криптоалгоритм	шифр колонної заміни	шифр колонної заміни	шифр колонної заміни
Кількість шифрдисків	4	6	6
Наявність інших технічних елементів шифралгоритму (комутатора)	так	ні	ні
Кількість контактів в одному шифрдиску	30	26	26
Кількість варіантів ключа	$3{,}76\times10^{33}$	$1{,}02\times10^{16}$	$2{,}2\times10^{43}$
Ступінь автоматизації	Автоматизована, з електричним приводом, літеродрукуюча з виводом інформації на паперову стрічку	Неавтоматизована, з ручним приводом, літеродрукуюча з виводом інформації на паперову стрічку	Неавтоматизована, з ручним приводом, літеродрукуюча з виводом інформації на паперову стрічку
Швидкість	до 200 знаків / хвил.	до 50–60 знаків / хвил.	до 30 знаків / хвил.
Підтверджені дані щодо дешифрування противником	так	так	ні

Модифікація SG-41Z (*рис. 13*) (SG-41. Collection Deutsches Museum No. 2013–1092. 2021), мала тільки 10 цифрових клавіш та призначалась на заміну "Enigma Z" для шифрування метеорологічних повідомлень в мережах Люфтваффе.

Рис. 13. Шифрувальна машина SG 41Z

У зв'язку з відсутністю легких металів, машина виявилась занадто важкою для мобільного використання. До середини 1944 р. німецьке верховне командування замовило для забезпечення військ 11 тис. виробів SG-41 і понад 2 тис. виробів SG-41Z — для підрозділів метеослужби Люфтваффе. Але, в супереч значному замовленню, всього було випущено біля 5 тис. машин SG-41 26-модульного зразку, з них близько тисячі використовувались у Абвері. Виробів SG-41Z всього було випущено близько 2 тисяч машин, а у війська поставлено лише 501 комплект. Виробництво SG-41 та її модифікацій було припинено з вступом Радянської Армії на територію Німеччини, а варіант з електричним приводом взагалі серійно не випускався. Даних щодо дешифрування противником даного зразку техніки не знайдено.

Існує легенда, що саме на машині цього зразку німцями відправлено останню криптограму у Другій світовій війні. Під час операції в Норвегії було захоплено комплект техніки і роздруковану телеграму такого змісту: *«Фюрер мертвий. Боротьба продовжується. Деніц»*.

Під час Другої світової війни німецькі військові також застосовували апаратуру лінійного шифрування. Передавання в телеграфну лінію зв'язку повідомлення з одночасним його зашифровуванням значно скорочувало час. Фірмою "Siemens & Halske" виготовлювався телетайп "T-37" та його модифікація "T-37 ICA" ("Fjernskriver") (*рис. 14*) (T-37 ICA Fjernskriver (Teletypewriter) by Bjarne Carlsen SSGT, Royal Danish Air Force (Ret'd.). 2021), що працював у двох режимах: відкритому та з застосуванням шифратора, синхронність налаштування якого щодо встановлення ключа забезпечувалася операторами передавальної та приймальної станцій по відкритим каналам зв'язку. Це значно знижувало рівень криптографічної стійкості системи зважаючи на чисельні порушення операторами правил роботи на обладнанні.

Фірмами "Lorenz" та "Siemens" з 1940 р. випускався шифратор "SZ", який був додатком до стандартного телетайпу Лоренца. Він використовувався в стаціонарних умовах

Рис. 14. Шифрувальна машина-телетайп Т-37

і обслуговувався висококваліфікованим персоналом. В 1942 р. шифратор був модернізований і отримав позначення SZ-42A та SZ-42B (*рис. 15*) (Lorenz SZ-40/42 TUNNY. 2021). Шифратор складався з 12 дисків, на кожному з яких розташовувалась різна кількість контактів. Використовуючи 5-ти бітовий код, шифратор генерував псевдовипадковий поточний шифр, який накладався на вихідні символи відкритого тексту телетайпу та формував криптограму. Габарити апаратури — 480 х 390х 430 мм. В 1942 р. англійці, а в 1943 р. і шведи, зламали криптоалгоритм виробу з вищезазначених причин.

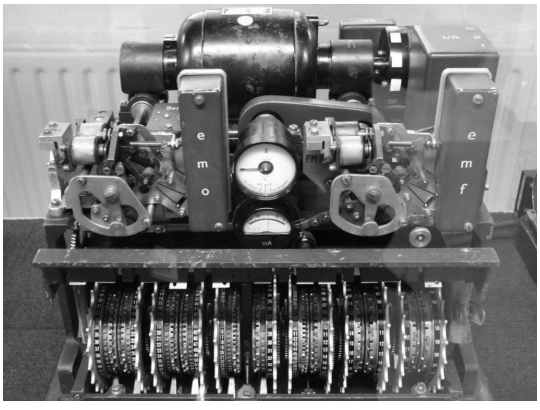

Рис. 15. Шифрратор SZ-42

Основним виробом, що використовувався на телеграфних лініях стратегічного рівня, був розроблений в середині 1930-х років фірмою “Siemens & Halske” електромеханічний букводрукуючий шифрувальний пристрій Т-52 (“Geheimschreiber”) (*рис. 16*) (T-52 Geheimschreiber. 2021), що реалізував шифр колонної заміни. В Т-52 було встановлено 12 шифрдисків. Зразок був декілька разів модернізований та мав індекси модифікацій від A до D. Всього було виготовлено 1200 машин.

Рис. 16. Шифрувальна машина-телетайп “T-52D”

Виріб був громіздким, масою близько 100 кг. Використовувався переважно на території Німеччини в стратегічній ланці для передачі особливо секретних повідомлень, зокрема застосовувався Люфтваффе для зв’язку з авіабазами в Норвегії. Канали зв’язку проходили через територію Швеції. Німецькі оператори часто порушували встановлені правила зв’язку, допускали велику кількість помилок, що приводило до чисельних (до 40 разів) повторень

тексту телеграм. При цьому, в супереч інструкціям, ключ не змінювався. Таке недбале відношення до безпеки шифрованого зв'язку було використано шведськими криптоаналітиками, якім вдалось зламати криптоалгоритм машини та протягом 1940–1942 рр. дешифрувати більше 0,5 млн. повідомлень. Дешифровані телеграми потрапили до рук радянської розвідки, в результаті чого криптоаналітики СРСР самостійно зламали криптосистему Т-52. Однак, в 1943 р., в ході чергової модернізації машини до модифікації D, криптоалгоритм був змінений, дані щодо злому криптогалгоритму цього зразку відсутні.

Лінійний шифратор "Schlüsselzusatz 40/42" (Шифрувальна приставка–40) фірми "Lorenz" застосовувався в Сухопутних військах Німеччини для шифрування повідомлень, що передавалися телеграфними каналами стратегічної ланки. В якості кінцевого пристрою для даного виробу використовувався міжнародний телеграфний апарат "Baudot" (Бодо). В машині оберталися два комплекти зубчастих дисків по п'ять дисків в кожному, які мали різну кількість зубців. Їх кількість на диску можна було змінювати шляхом зсування їх у бік, або висування їх на місце. На вісі також постійно оберталися два ведучих, так званих «моторних», диска, кожен з яких обертав свій напівкомплект дисків. З кожним обертанням дисків, до інформаційного сигналу, що складався з п'яти електричних імпульсів (одиниць або нулів), випадково додавалося ще два набори імпульсів. В псевдовипадковому генеруванні додаткових імпульсів значення мало первинне встановлення вихідного положення дисків перед початком зашифровування. Перед передаванням тексту радіооператор повідомляв адресатові вихідне положення дисків та кількість зубців на кожному з них. Установочні дані змінювалися перед кожним сеансом зв'язку. Встановивши такі ж самі положення дисків на своєму шифраторі, радист приймаючої станції забезпечував автоматичне розшифрування і відповідність розшифрованого повідомлення відкритому тексту. Криптосистема виробу була зламана криптоаналітиками США з причин систематичних порушень правил безпеки шифрованого зв'язку, аналогічних порушенням допущеним операторами виробів Т-37 та Т-52.

Черговим німецьким засобом шифрування стала апаратура Т-43 (*рис. 17*) (Siemens T-43. 2021), яка була створена компанією "Siemens & Halske" в 1944 р. на базі Т-52 і "Lorenz SZ-42". Виріб поєднував функції шифратора і телетайпа. Він використовувався верховним командування Вермахту, на флоті та в Міністерстві іноземних справ. Носієм ключа слугувала стандартна 17-мм перфорована паперова стрічка, яку можна було використовувати лише

один раз, що виключало помилки персоналу (Вдовенко, С. Г., Гульков, М. О., Сидоров, С. В. & Джола, В. 2021, с. 101). Всього було випущено близько 50 машин. Інформації про дешифрування криптограм Т-43, якій безперечно мав високий ступінь криптостійкості, не знайдено.

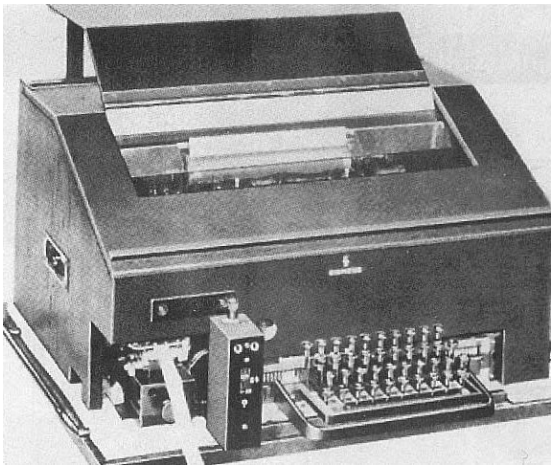

Рис. 17. Шифрувальна машина-телетайп Т-43

Ряд заходів розвідувального, організаційного та науково-технічного характеру дозволило англійцям зламати криптоалгоритми та читати німецькі шифровані повідомлення. Починаючи з 1939 р. Великобританія з невеликими перервами, після чергової модернізації "Enigma", могла дешифрувати більшість інформації, що була перехоплена в мережах, в яких застосовувалася ця шифрмашина. З 1940 р. у Центрі дешифрування поблизу Лондона було розпочато дешифрування німецьких криптограм, зашифрованих за допомогою апаратури лінійного шифрування "Schlüsselzusatz 40/42" та Т-52. Криптоаналітики СРСР та США, останні спільно з англійцями, також досягли в цьому значних успіхів. Дешифрування німецьких повідомлень у період Другої світової війни буде напрямком подальших досліджень.

Висновки. Напередодні та в ході Другої світової війни, Німеччина, як й інші держави світу — учасники війни, для захисту від розвідок противника урядової та військової інформації, масово виробляла та застосовувала технічні засоби криптографічного захисту інформації. Автоматизація процесів шифрування покращувала оперативність управління. Комплексне застосування різнотипних засобів криптографічного захисту інформації для організації різних мереж автономного та лінійного шифрованого зв'язку на стратегічному, оперативному й тактичному рівнях дозволяло утворювати гнучкі та дублюючі мережі скритого зв'язку, підвищуючи його живучість та конфіденційність. Разом з тим, розробка в Німеччині нових зразків шифрувальної техніки на загальнопоширеному у світі принципі роторного шифратора, не докладаючи вичерпних зусиль щодо підвищення інженерними та організаційними заходами їх криптографічної стійкості, нехтування з боку шифрувальників вимогами нормативно-правових актів та правилами роботи на криптографічному обладнанні в частині, що вимагає забезпечення безпеки шифрованого зв'язку та конфіденційності в роботі, не сприяли збереженню

інформації в таємниці, та відповідно, знижували рівень захищеності військ. Неврахування таких факторів значною мірою вплинуло на результат війни.

Вищезазначені висновки враховані при прийняті організаційно-технічних рішень щодо впровадження в різних ланках управління Збройних Сил та сил оборони України, в тому числі і тактичній, різноманітних новітніх зразків техніки криптографічного захисту інформації з національними криптоалгоритмами. Що дозволило багатократно підвищити рівень безпеки застосування засобів криптографічного захисту та оперативності доведення інформації під час проведення операцій з відбиття Україною збройної агресії Російської Федерації (Вдовенко, С. Г. & Даник, Ю. Г. 2017, с. 103).

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ І ЛІТЕРАТУРИ

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

Вдовенко, С. Г., Гульков, М. О., Сидоров, С. В. & Джола, В.М. (2021). Засоби криптографічного захисту інформації СРСР періоду ІІ Світової війни. *Воєнно-історичний вісник.* № 1 (39), с. 97–113. DOI: 10.33099/2707-1383-2021-39-1-97-113.

Вдовенко, С. Г., Гульков, М. О., Сидоров, С. В. & Вдовенко, О.Г. (2021). Техніка криптографічного захисту інформації Сполучених Штатів Америки першої половини ХХ століття. *Воєнно-історичний вісник*. № 3 (41), с. 132–145. DOI: 10.33099/2707-1383-2021-41-3-132-145.

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

Ларин, Д. А. & Шанкин, Г. П. (2014). *Вторая мировая война в эфире: некоторые аспекты операции «Ультра». Защита информации.* Москва: «Издательство “Инсайд”», 345 с.

Уинтерботэм, Ф. А. (1991). *Операция «Ультра». Секретные операции.* Москва: «Издательство “Политическая литература”», 654 с.

Черняк, Л. (2003). Тайны проекта “Ultra”. *Отркрытые системы. СУБД.* № 07–08, с. 34–40.

Шифрувальні машини і криптологія. Технічні деталі. Enigma machine (2021). URL: https://www.ciphermachinesandcryptology.com/en/enigmatech.htm. [дата зверн.: 07.11.2022].

Enigma T. Photo. (2021). URL: https://www.cryptomuseum.com/ crypto/enigma/t/index.htm [дата зверн.: 07.11.2022].

Enigma Z. Photo. (2021). URL: https://www.cryptomuseum.com/ crypto/enigma/z/ [дата зверн.: 07.11.2022].

German, E. S. (2021). Code Disks. URL: http://www.jproc.ca/ crypto/german_code_disks. html photo [дата зверн.: 07.11.2022].

Hamer, David H., Sullivan, Geoff & Weierud, Frode. (1998). Enigma Variations: an Extended Family of Machines, Cryptologia. URL: http://www.blueangel.demon.co.uk/crypto/ [дата зверн.: 10.08.2022].

Hinsley, F. H. & Stripp, Alan. (1993). *The Enigma Machine: Its Mechanism* and Use // Codebreakers: The Inside Story of Bletchley Park, pp. 83–88.

Kahn, David. (1991). *Seizing the Enigma: The Race to Break the German U-Boats Codes, 1939–1943.* Pubisher: Houghton Miffin Harcourt, 336 p.

Kruh, Louis & Deavours, Cipher. (2002). The Commercial Enigma, *Cryptologia.* № 1 (26), pp. 1–16.

Kryha. From Wikipedia, the free encyclopedia. (2021). URL: https://en.wikipedia.org/wiki/ Kryha.photo [дата зверн.: 07.11.2022].

Lorenz SZ-40/42 TUNNY. (2021). URL: https://www.cryptomuseum. com/crypto/lorenz/sz 40/ [дата зверн.: 07.11.2022].

Louis Kruh and Cipher Deavours the commercial enigma: beginnings of machine cryptography. (2021). URL: https://www.apprendre-en-ligne.net/crypto/bibliotheque/PDF/KruhDeavours.pdf. Photo. Text. [дата зверн.: 07.11.2022].

Marks, Philip & Weierud, Frode. (2000). Recovering the Wiring of Enigma's. Umkehrwalze A.*: Cryptologia.* № 1 (24), pp. 55–66.

SG-41. Collection Deutsches Museum No. 2013-1092. (2021). URL: https://www.researchgate. net/publication/339697016_What_We_Know_About_Cipher_Device_Schlusselgerat_SG-41_so_Far/figures?lo=1 [дата зверн.: 07.11.2022].

Siemens T-43. (2021). URL: https://www.cryptomuseum.com/ crypto/siemens/t 43/index. htm [дата зверн.: 07.11.2022].

Smith, Michael. (1998). *Station X: The Codebreakers of Bletchley Park.* Hardcover: 845 p.

T-37 ICA Fjernskriver (Teletypewriter) by Bjarne Carlsen SSGT, Royal Danish Air Force (Ret'd.). (2021). URL: http://www.jproc.ca/crypto/t37.html [дата зверн.: 07.11.2022].

T-52 Geheimschreiber. (2021). URL: https://www.cryptomuseum.com/ crypto/siemens/t 52/ [дата зверн.: 07.11.2022].

US1657411A. Ciphering machine — Google Patents. (2021). URL: https://patents.google. com/patent/US1657411A/en [дата зверн.: 07.11.2022].

REFERENCES

Vdovenko, S. H. & Danyk, Yu. H. (2017). Kontseptualni napryamy kompleksnoho vyrishennya problemy zakhystu informatsiyi v systemi skrytoho upravlinnya zbroynykh syl [Conceptual directions of a comprehensive solution to the problem of information protection in the system of covert control of the armed forces]. *Naukovyy zhurnal.* № 2 (29), s. 98–106. [in Ukrainian].

Vdovenko, S. G., Gulkov, M. O., Sidorov, S. V. & Dzhola, V. (2021). Zasoby kryptohrafichnoho zakhystu informatsiyi SRSR periodu II Svitovoyi viyny [Means of cryptographic protection of information of the USSR during World War II]. *Voenno-istorychnyy visnyk.* № 1 (39), s. 97–113. DOI: 10.33099/2707-1383-2021-39-1-97-113. [in Ukrainian].

Vdovenko, S. G., Gulkov, M. O., Sidorov, S. V. & Vdovenko, A. G. (2021). Technicka kryptohrafichnoho zakhystu informatsiyi Spolychenych Shtativ Ameryky pershoi polovyny XX stolittia [Technique of information cryptographic protection of the United States of America in the first half of the XX century]. *Voenno-istorychnyy visnyk.* № 3 (41), s. 132–145. DOI: 10.33099/2707-1383-2021-41-3-132-145. [in Ukrainian].

Vdovenko, S. G., Danyk, Y. G. & Permyakov, O. Yu. (2020). Dosvid rozvytku system kiberbezpeky ta kiberoborony providnykh krayin svitu [Experience in the development of cyber security and cyber defense systems of the world's leading countries]. *Naukovyy zhurnal.* № 1 (37), s. 31–48. DOI: 10.33099/2311-7249/2020-37-1-31-48. [in Ukrainian].

Larin, D. A. & Shankin, G. P. (2014). *Vtoraya mirovaya voyna v efire: nekotoryye aspekty operatsii "Ul'tra". Zashchita informatsii* [World War II on Air: Some Aspects of Operation Ultra. Data protection]. Moskva: «Izdatel'stvo "Insayd"», 345 s. [in Russian].

Uinterbotem, F. A. (1991). *Operatsiya "Ul'tra". Sekretnyye operatsii* [Operation "Ultra". Secret operations]. Moskva: «Izdatel'stvo "Politicheskaya líteratura"», 654 s. [in Russian].

Chernyak, L. (2003). Tayny proyekta "Ultra" [Secrets of the project "Ultra"]. *Otrkrytyye sistemy. SUBD.* № 07–08, s. 34–40. [in Russian].

Shyfrovalni mashyny i kryptolohiya. Tekhnichni detali. Enigma machine [Encrypting machines and cryptology. Technical details. Enigma machine]. (2021). URL: https://www.ciphermachinesandcryptology.com/en/enigmatech.htm [Accessed: 07.11.2022]. [in Ukrainian].

Enigma T. Photo. (2021). URL: https://www.cryptomuseum.com/ crypto/enigma/t/index. htm [Accessed: 07.11.2022]. [in English].

Enigma Z. Photo. (2021). URL: https://www.cryptomuseum.com/ crypto/enigma/z/[Accessed: 07.11.2022]. [in English].

German, E. S. (2021). Code Disks. URL: http://www.jproc.ca/crypto/ german_code_disks. html photo [Accessed: 07.11.2022]. [in English].

Hamer, David H., Sullivan, Geoff & Weierud, Frode. (1998). Enigma Variations: an Extended Family of Machines, Cryptologia. URL: http://www.blueangel.demon.co.uk/crypto/[Accessed: 10.08.2022]. [in English].

Hinsley, F. H. & Stripp, Alan. (1993). *The Enigma Machine: Its Mechanism* and Use // Codebreakers: The Inside Story of Bletchley Park, pp. 83–88. [in English].

Kahn, David. (1991). *Seizing the Enigma: The Race to Break the German U-Boats Codes, 1939–1943.* Pubisher: Houghton Miffin Harcourt. 336 p. [in English].

Kruh, Louis & Deavours, Cipher. (2002). The Commercial Enigma, *Cryptologia.* № 1 (26), pp. 1–16. [in English].

Kryha. From Wikipedia, the free encyclopedia. (2021). URL: https://en.wikipedia.org/wiki/Kryha. photo [Accessed: 07.11.2022]. [in English].

Lorenz SZ-40/42 TUNNY. (2021). URL: https://www.cryptomuseum. com/crypto/lorenz/sz 40/ [Accessed: 07.11.2022]. [in English].

Louis Kruh and Cipher Deavours the commercial enigma: beginnings of machine cryptography. (2021). URL: https://www.apprendre-en-ligne.net/crypto/bibliotheque/PDF/KruhDeavours.pdf. Photo. Text [Accessed: 07.11.2022]. [in English].

Marks, Philip & Weierud, Frode. (2000). Recovering the Wiring of Enigma's. Umkehrwalze A.*: Cryptologia.* № 1 (24), pp. 55–66. [in English].

SG-41. Collection Deutsches Museum No. 2013–1092. (2021). URL: https://www.researchgate.net/publication/339697016_What_We_Know_About_Cipher_Device_Schlusselgerat_SG-41_so_Far/figures?lo=1 [Accessed: 07.11.2022]. [in English].

Siemens T-43. (2021). URL: https://www.cryptomuseum.com/ crypto/siemens/t 43/index. htm [Accessed: 07.11.2022]. [in English].

Smith, Michael. (1998). *Station X: The Codebreakers of Bletchley Park.* Hardcover: 845 p. [in English].

T-37 ICA Fjernskriver (Teletypewriter) by Bjarne Carlsen SSGT, Royal Danish Air Force (Ret'd.). (2021). URL: http://www.jproc.ca/crypto/t37.html [Accessed: 07.11.2022]. [in English].

T-52 Geheimschreiber. (2021). URL: https://www.cryptomuseum.com/ crypto/siemens/t 52/ [Accessed: 07.11.2022]. [in English].

US1657411A. Ciphering machine — Google Patents. (2021). URL: https://patents.google.com/patent/US1657411A/en [Accessed: 07.11.2022]. [in English].

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

Mykola Hulkov
Lecturer of the Communication and Information Systems Chair of the Troops (Forces) Support and Information Technologies Institute,
The National Defence University of Ukraine named after Ivan Chernyakhovskyi (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 Chernyakhovskyi (Kyiv, Ukraine)
ORCID: https://orcid.org/0000-0002-1961-4251

Serhii Pashkevych
Student of group 4210 of the Troops (Forces) Support and Information Technologies Institute,
The National Defence University of Ukraine named after Ivan Chernyakhovskyi (Kyiv, Ukraine)
ORCID: https://orcid.org/0000-0001-8768-6508

TECHNIQUE OF CRYPTOGRAPHIC PROTECTION OF INFORMATION OF NAZI GERMANY PERIOD OF THE SECOND WORLD WAR

The article considers the application of cryptographic protection of German information on the eve and during the Second World War. The theory of "blitzkrieg", as the main military doctrine of Nazi Germany, changed the views on the spatial and temporal characteristics of operations, put forward demands to increase the efficiency and secrecy of military management, which was achieved by the introduction of encryption technology. Automation of encryption processes has improved management efficiency. Due to the complex application of various types of cryptographic information protection, flexible networks of autonomous and linear encrypted communication at the strategic, operational and tactical levels have been formed. This greatly increased the survivability and confidentiality of the encrypted connection.

At the same time, in Germany, new models of encryption technology were developed on the world-wide principle of a rotary encoder, without making exhaustive efforts to increase their cryptographic stability by engineering and organizational measures. The neglect of cryptographic equipment by cryptographers, which required confidentiality and security of encrypted communications, did not keep information secret and, consequently, reduced the level of security of troops.

Failure to take such factors into account and systemic errors in the organization and security of cryptographic protection of information greatly contributed to the defeat of Nazi Germany.

Solving the problem of ensuring the secrecy of management during the preparation and conduct of the operation in today's conditions requires consideration and use in Ukraine and its Armed Forces of scientific and technological progress in the field of cryptographic protection of information with mandatory prevention of possible systemic errors.

Keywords: *Key system, confidentiality, cryptographic protection of information, efficiency, covert command and control of troops, secrecy, encryption technique, encryption machine.*