УДК 681.188.000.93
DOI: 10.33099/2707-1383-2021-41-3-132-145

Сергій Вдовенко
магістр державного військового управління у сфері оборони, 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

Олександр Вдовенко
слухач групи 4209, Інститут забезпечення військ (сил) та інформаційних технологій, Національний університет оборони України імені Івана Черняховського (Київ, Україна)
ORCID: https://orcid.org/0000-0001-8591-1249
Електронна пошта: 4e4eN891@gmail.com

ТЕХНІКА КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ СПОЛУЧЕНИХ ШТАТІВ АМЕРИКИ ПЕРШОЇ ПОЛОВИНИ XX СТОЛІТТЯ

У статті розглядається технічний прогрес у сфері криптографічного захисту інформації та його вплив на систему управління військами в операціях першої половини XX століття на прикладі створення й розвитку техніки криптографічного захисту інформації США. Вирішення завдань скритності управління під час підготовки та проведення операції Збройних Сил в умовах сьогодення, зокрема в операції Об'єднаних сил на Сході України, вимагають врахування та використання в Україні та її Збройних Силах досягнень науково-технічного прогресу на всіх рівнях управління.

Ключові слова: *скрите управління військами, ключові системи, шифрувальна техніка, оперативність.*

Постановка проблеми. Перша половина XX століття, дві світові війни, удосконалюються та з'являються нові засоби збройної боротьби, відбувається їх апробація та застосування в реальних умовах. Під час Першої світової війни та наступні 1920–30-ті роки, при масовому використанні засобів зв'язку, необхідність дотримання скритності управління військами та збереженні у таємниці замислу майбутніх дій призвела до стрімкого розвитку криптографії та криптоаналізу, що згодом поєдналися в єдину науку — криптологія.

Вимога щодо забезпечення скритності управління військами (силами) знаходить своє відображення в розвитку шифрів та автоматизації процесу шифрування. Одним з основних способів вирішення завдань щодо надійного криптографічного захисту і підвищення оперативності обробки та доведення інформації, що циркулює під час управління військами, є впровадження автоматизованих засобів криптографічного захисту інформації. Напередодні та в ході Другої світової війни приймаються на озброєння механічні та електромеханічні пристрої для криптографічного захисту інформації та криптоаналізу (прообраз сучасних комп'ютерів). В декількох країнах світу, а саме Італії, Німеччині, Польщі, СРСР, США, Швеції були розроблені та прийняті на озброєння електромеханічні шифрувальні машини. Тоді ж виникли та отримали розвиток нові напрямки науки: теорія інформації та зв'язку, криптологія та кібернетика (Вдовенко, С. Г. Даник, Ю. Г. & Пермяков, О. Ю. 2020, с. 58; Сумароков, В. 1999, с. 115).

Все це значною мірою впливало та й надалі впливатиме 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. 58; Вдовенко, С. Г. & Даник, Ю. Г. 2017, с. 100).

Огляд основних досліджень. Розвиток засобів криптографічного захисту інформації США першої половини XX століття можна прослідкувати за публікаціями в науково-історичній періодиці та з електронних джерел (Кан, Д. Е. 2000, с. 38–45; Кирьян, М. А. (голов. ред.). 1982, с. 117–215; Гребенніков, В. 2009). На відміну від них, у цій статті автори більш повно намагалися розкрити питання 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. В Україні це питання майже не досліджувалося. За виключенням декількох газетних публікацій. (Вдовенко, С. Г. 2001. Військові відомості, 25 (102), 26 (103)).

Мета статті — на основі проведеного аналізу показати, за якими напрямками розвивалися засоби криптографічного захисту інформації Армії та ВМС США першої половини XX століття.

Виклад основного матеріалу. Для скритого управління військами в Армії та ВМС США з початку 20-х років XX століття і до 1942 р. на тактичному рівні застосовувався пристрій М-94 (в US NAVY — CSP-488), відомий також як прилад Джефферсона (рис. 1, 2). Прилад винайшов ще у 1790 державний секретар США Томас Джефферсон, який згодом став третім президентом США. Незалежно від нього цей винахід повторив майор Армії США Базері.

Вироблений з алюмінію пристрій, складався з 25 дисків, що набиралися на вісь у порядку, визначеному правилами. Кожен диск мав нумерацію від **1** до **25** та присвоєну йому літеру від **B** до **Z**. Літера **A** жодному диску не присвоювалася. На диску у випадковому порядку по колу було розміщено 26 літер латинського алфавіту.

Рис. 1. Прилад Джефферсона, М-94 (CSP-488)

Рис. 2. Диск приладу Джефферсона

Диск **R-17** по колу мав змістовний надпис **“ARMYOFTHEUS”**. М-94 реалізував так званий шифр взаємної підстановки алфавітів (колонної заміни) (Кирьян, М. А. (голов. ред.). 1982, с. 123–235).

В подальшому, у 1940 р. була прийнята на забезпечення військ зв’язку США, а з 1942 р. застосовувалася шифрувальна машина М-209 (в US NAVY — CSP-1500) (Криптографічні засоби: M209 (CSP-1500). 2014). Вона була портативною, літеродрукуючою, з виводом інформації на паперову стрічку, мала ручний привід, призначалася для зашифровування і розшифрування повідомлень в тактичній ланці. М-209 ніколи не застосовувалася у вищих ланках управління, й ніколи не була секретною. Таємницею були правила роботи і безумовно ключова система. В Армії і ВМС США використовувалися різні ключові системи і правила роботи.

Це перший в історії приклад масового виробництва і застосування техніки криптографічного захисту інформації. М-209 (*рис. 3*) була доведена навіть до окремої розвідувально-диверсійної групи. Фактично це був ліцензійний виріб шведського винахідника і підприємця Бориса Хагеліна С-38, який вироблявся з кінця 30-х років (*рис. 4*).

Машина роторного типу М-209 реалізувала шифр колонної заміни. На той час вона забезпечувала достатню криптографічну стійкість для тактичної ланки, її криптографічний період складав 101405850 знаків. Зв’язківці Армії США з любов’ю відносилися до цього виробу за його компактність, легкість та простоту експлуатації. Його маса складала 2,7 кг, швидкість — до 30 знаків за хвилину.

За роки Другої світової війни у США було випущено 140 тис. одиниць М-209. Перше застосування

Рис. 3. Шифрмашина М-209-В (CSP-1500)

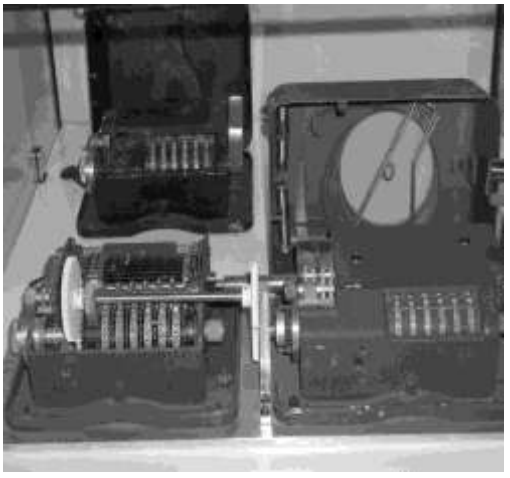

Рис. 4. Шифрмашина С-38

М-209 в ході бойових дій відбулося в 1942 р. під час операції «Торч» в Північній Африці. Виріб експлуатувався під час війни в Кореї, тобто до 50-х років XX століття.

Недоліком машини слід визнати необхідність одночасної роботи не менш як двох фахівців, що знижувало рівень конфіденційності (*рис. 5, 6*). З рештою, для тактичної ланки управління — це не дуже важливо. Суттєвим конструктивним недоліком вважається неспроможність шифрування знаку повідомлення в той самий знак, що значно підвищує імовірність розкриття тексту криптограми противником шляхом криптоаналізу. За спогадами Райнольда Вебера, який в роки війни працював в дешифрувальному підрозділі Вермахту FNAST-5, у 1943–1944 роках німці не лише зламували криптоалгоритм М-209 вручну, але й сконструювали машину-прототип для автоматизації найбільш складних етапів дешифрування (Уинтерботэм, Ф. А. 1991, с. 345).

Для обміну шифрованими повідомленнями в оперативній і стратегічній ланках управління США використовували автоматизовану шифрувальну машину роторного типу з виводом інформації на стрічковий носій М-134 Sigaba («Сайджеба»), у ВМС — ECM (Electric Cipher Machine — електрична шифрувальна машина) CSP-888/889 Mark II (*рис. 7)*. М-134 могла працювати як в автономному так і в лінійному режимах.

Ранній зразок виробу М-134-А під назвою Sigmyc («Сайджмик») (*рис. 8*) мав шифратор із зовнішнім носієм шифру у вигляді перфострічки, на зразок радянського зразку М-101 (Вдовенко, С. Г., Гульков, М. О., Сидоров, С. В. & Джола, В. О. 2021, с. 100, 101). Він використовувався також на лініях урядового зв'язку під кодовим позначенням POTUS — PRIMER

Рис 5. Шифрування повідомлення з використанням М-209

Рис 6. Робота шифрувальників в бойових умовах (Нова Гвінея)

Рис. 7. Шифрмашина M-134 Sigaba/Mark II CSP-888/889.

Рис. 8. Шифрмашина M-134-A Sigmyc.

(President of the United States — Prime Minister UK) для забезпечення шифрованим зв'язком Президента США з прем'єр-міністром Великої Британії. Але, при абсолютній надійності цього зразку, для американських криптографів задача розсилання великої кількості симетричних ключів була занадто складною.

Згодом Френк Роулетт (Frank Rowlett) з відділу «С» розвідувальної служби військ зв'язку Армії США (Army's Signal Intelligence Service) винайшов складний шифратор (на той час ноу-хау). Він складався з 15 шифрдисків, механізм руху шифрдисків забезпечував аперіодичний і випадковий (псевдовипадковий) рух. По-перше, певні диски рухалися за напрямком вперед, інші в зворотному напрямку. По-друге, на відміну від інших зразків, взаємозв'язок між шифрдисками забезпечувався певними елементами ключа. В той час, як один диск міг обернутися на повний цикл, інший — провернутися лише на один крок. Електрична схема машини передбачала можливість шифрування символу у такий самий символ. Машина CSP-888/889 використовувалася у ВМС США до 1959 року, а до 1996 року була секретною. Повідомлення, що були зашифровані із застосуванням цього зразку не були жодного разу дешифровані противником.

Відділ «С» відповідав за своєчасне забезпечення військ шифрувальною апаратурою, кодовими книгами та шифрами, розробку правил та інструкцій з безпеки зв'язку. Фахівці відділу розробляли спеціальні інструкції, що унеможливлювали втрату шифрувальної апаратури, аналізували усі випадки, що були пов'язані з втратами шифрів та апаратури. Безпосередньо організацію робіт щодо створення шифрувальної апаратури для Армії США було покладено на відділ «F» розвідувальної служби

військ зв'язку. За участю спеціалістів цього відділу поряд з шифрувальною машиною М-134 було розроблено модель М-228 Sigcum («Сайджкам»), позначення для NAVY — CSP-1515, яка стала поставлятися у війська починаючи з 1943 року (Криптографічні засоби: Sigaba Mark II. 2012). Це був пристрій, який забезпечував шифрування тексту в лінію. Враховуючи значне збільшення обсягів інформації під час проведення великих воєнних операцій, це значно підвищувало оперативність і давало суттєвий виграш в часі (*рис. 9*).

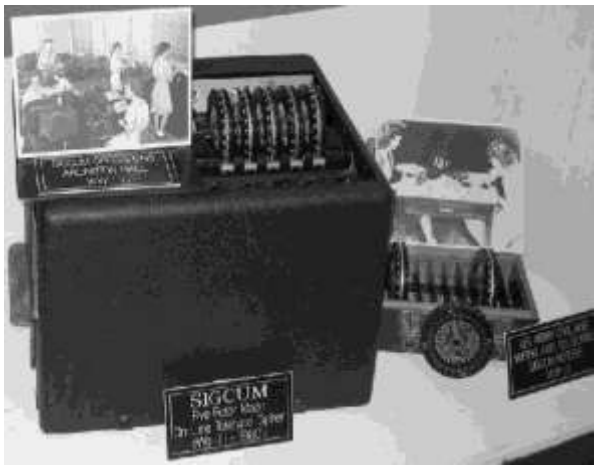

Рис. 9. Лінійний шифратор М-228 Sigcum/CSP-1515

Виріб використовувався на лініях зв'язку до 1960 р. Однак поруч із цією перевагою, конструкція пристрою мала й суттєвий недолік — при неуважності оператора відбувалися порушення безпеки зв'язку. Особливість полягала в тому, що обладнання дозволяло передавати в лінію як відкритий, так й зашифрований текст, для чого оператор повинен був перед початком роботи перевести перемикач режиму роботи у відповідне положення. За роки Другої світової війни зафіксовані принаймні два випадки відкритої передачі в ефір секретних повідомлень, що відбулися з вини операторів. Шифратор виробу складався з п'яти шифрдисків, що обертаючись утворювали шифрувальний електричний ланцюг. Алгоритм руху дисків був не складний, кожен наступний диск обертався на один крок після повного обертання попереднього диску. Всього до комплекту входило десять шифрдисків, що дозволяло ускладнювати ключ. Незважаючи на це, криптографічна стійкість не була високою. В решті решт, після проведених криптографічних випробувань, було дозволено використовувати виріб для передачі в лінію телеграфних повідомлень зі ступенем секретності SECRET для дротових каналів зв'язку, та CONFIDENTIAL — по радіо. М-228 також використовувалася у військах зв'язку Великої Британії для утворення спільних мереж зв'язку об'єднаного командування. Вдосконалену версію виробу М-228-М Sighuad («Сайджхуд») дозволялося використовувати для передачі більш секретних повідомлень, але відповідні правила роботи диктували необхідність використання для шифрування повідомлень шифрувальну машину М-134 Sigaba, або лінійний шифратор CSP-2599 Sigtot («Сайджтот»).

Беручи до уваги вище перелічені зразки засобів криптографічного захисту інформації (далі — КЗІ) США логічно буде виділити декілька ключових характеристик, які активно розвивалися (вдосконалювалися) (*табл. 1*).

Таблиця 1

ПОРІВНЯЛЬНА ТАБЛИЦЯ ЗРАЗКІВ ТЕХНІКИ КЗІ США ЧАСІВ ДРУГОЇ СВІТОВОЇ ВІЙНИ

Найменування	Криптографічний період	Швидкість (груп/год)
М-94, (прилад Джеферсона)	≈ 17576	до 30
М-209, (CSP-1500)	≈ $101{,}4\times10^5$	до 50–60
М-134, Sigaba (Сайджеба)	≈ $94{,}3\times10^6$	до 100
М-134А, Sigmyc	теоретично недешифруємий	до 100
М-228, Sigcum (Сайджкам)	≈ $15{,}9\times10^6$	до 100

Таблиця розроблена за даними (Криптографічні засоби: Sigaba Mark II. 2012; Криптографічні засоби: М209 (CSP-1500). 2014). Основними ключовими характеристиками виступали:

стійкість (криптографічний період) шифру;

оперативність (швидкість обробки інформації).

В навчальних закладах (підрозділах) США, які готували інженерів зв'язку та здійснювали підготовку курсантів в галузі криптографії, з 1943 року використовувалась машина М-325Т Sigfoy («Сайджфой») (рис. 10, 11). Цей портативний виріб був значно менш крипостійким ніж М-209, але він був вже з електричним приводом. Виріб ніколи не застосовувався для шифрування повідомлень, інакше ніж в навчальних цілях. (Літер Т у найменуванні означає — training, навчальна).

Технічний прогрес не обійшов і сферу захисту інформації, була створена й випробувана в бойових умовах техніка криптографічного захисту інформації. Історичним слід вважати набутий досвід масового виробництва та застосування шифртехніки, доведення окремих її зразків до тактичної ланки управління, що безумовно підвищувало рівень оперативності спеціального зв'язку. Питання захисту спільних секретів коаліційних сил вирішувалися сумісно, в тому числі й за допомогою криптографічних засобів. Застосування в різних ланках управління різної шифрувальної техніки забезпечувало належний рівень криптографічної стійкості повідомлень. Застосування

під час війни для підготовки фахівців несекретної навчальної шифрувальної техніки, слабшої в криптографічному відношенні за інші, але значно більш прогресивної в плані автоматизації і конструкторських рішень дозволило підвищити рівень спеціально-технічної підготовки випускників, а головне — здійснювати підготовку рекрутів до оформлення допуску до таємниці відповідного рівня.

Рис. 10. Шифрувальна машина М-325(Т)

Рис. 11. Шифрдиски М-325(Т)

За результатами своїх досліджень здійснених під час військової служби в період Другої світової війни, Клод Шеннон (Claude Elwood Shannon) виступає у 1945 р. в Конгресі США із секретною доповіддю «Теорія зв'язку в секретних системах», яка стала точкою відліку для самостійної науки — криптології. Доповідь була розсекречена у 1949 р. та видана у вигляді монографії разом з роботою «Математична теорія зв'язку», в якій була доведена теорема відліків, або теорема Віттакера — Найквиста — Шеннона — Котельникова. Виникли та отримали розвиток нові напрямки науки: теорія зв'язку та інформації, криптологія, кібернетика (Шеннон, К. Е. 1963, с. 345).

В залежності від рівня застосування техніки (оперативний, тактичний) можливо стверджувати, що розвиток засобів криптографічного захисту інформації здійснювався в напрямках, які суттєво впливали на результати операцій та бойових дій того часу.

Висновки. Необхідність практичної реалізації завдань щодо захисту від розвідок противника урядової та військової інформації США в ході

Другої світової війни призвела до ряду змін в теорії та практиці забезпечення національної безпеки США, що вплинуло на розвиток поглядів на забезпечення безпеки у післявоєнний період у всьому світі та продовжується сьогодні в умовах четвертої промислової революції. До надбань, слід віднести наступні:

масове виробництво та застосування засобів криптографічного захисту інформації (КЗІ), що було організоване вперше в історії, дозволило автоматизувати процеси шифрування, покращуючи оперативність управління;

комплексне застосування різнотипних засобів КЗІ 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;

застосування навчально-тренувальної апаратури КЗІ (емуляторів, тренажерів) для підготовки персоналу дозволило підвищити якість спеціально-технічної підготовки особового складу, одночасно надаючи змогу навчати рекрутів під час їх перевірки до моменту оформлення сертифікату відповідного рівня секретності;

організація захисту спільних секретів коаліційних сил, в тому числі із використанням засобів КЗІ, дозволила відпрацювати практичні юридично значимі, разом з тим процесті процедури взаємного обміну секретною інформацією, що дозволило застосувати цей досвід в НАТО та призвело до уніфікації національних вимог щодо захисту інформації з обмеженим доступом;

аналіз результатів практичної реалізації зазначених заходів та теоретичних досліджень, призвів до виникнення та подальшого розвитку нових напрямків науки: теорії зв'язку та інформації, криптології, кібернетики;

потужна науково-промислова база та розвиток теорії криптології (криптографії та криптоаналізу) призвели до розробки та прийняття на озброєння нових електронно-механічних (електронних) засобів КЗІ та дешифрування, а також до змін в системі забезпечення національної безпеки США, а саме формування в 1947 році Агенції Національної Безпеки (АНБ — National Security Agency, NSA);

останнє змусило працювати весь світ, зокрема СРСР, та спрямовувати значний науково-промисловий потенціал на розробку та прийняття на озброєння нових електронно-механічних (електронних) засобів КЗІ та алгоритмів дешифрування, що в свою чергу вплинуло на форми і способи їх застосування.

Спираючись на вищезазначені події і факти доцільно буде ці знання застосувати і в сучасних умовах, з метою підвищення оперативності, впровадження різноманітних новіт-

ніх зразків апаратури криптографічного захисту інформації в різних ланках управління в тому числі і тактичній, під час проведення операцій Збройних Сил України, зокрема операції Об'єднаних сил на території Донецької та Луганської областей (Вдовенко, С. Г. & Даник, Ю. Г. 2017, с. 99).

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ І ЛІТЕРАТУРИ

Вдовенко, С. Г. (2001). Забезпечення збереження таємниць та вимог прихованого управління в операціях Другої світової війни. *Газета, Північного оперативно-територіального командування. Військові відомості*, 25 (102), 26 (103), с. 2.

Вдовенко, С. Г., Гульков, М. О., Сидоров, С. В. & Джола, В. О. (2021). Засоби криптографічного захисту інформації СРСР періоду Другої світової війни. *Воєнно-історичний вісник: збірник наукових праць.* К.: НУОУ ім. І. Черняховського. Вип. 1 (39), с. 97–113. DOI:http:dx.doi.org/10.33099/2707-1383-2021-39-1-97-113.

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., Даник, Ю. Г. & Пермяков, О. Ю. (2020). Досвід розвитку систем кібербезпеки та кібероборони іноземних держав. *Сучасні інформаційні технології у сфері безпеки та оборони. Науковий журнал.* № 1 (37), с. 56–73. DOI: 10.33099/2311-7249/2020-37-1-31-48.

Гребенніков, В. (2009). Ужгород. Історія криптології & секретного зв'язку. Видання друге, виправлене, доповнене, ілюстроване. URL: https://reibert.info/media/albums/apparatura-zasek rechivanija-i-texnika-shifrovanija-sssr.10860/; https://reibert.info/media/m-100-spektr.466114; https://reibert.info/media/moj-kniga-na-ukrainskom.466125/ [дата зверн.: 27.05.2020].

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

Кирьян, М. А. (голов. ред.). (1982). *Внезапность в операциях ВС США*. Москва: Воениздат, 328 с.

M-209 (CSP-1500). (2021). URL: http://www.jproc.ca/crypto/m209.html [дата зверн.: 27.05.2021].

K-37 Crystal (2021). URL: http://www.jproc.ca/crypto/ecm2.html [дата зверн.: 27.05.2021].

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

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

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

REFERENCES

Vdovenko, S. H. (2001). Zabezpechennia zberezhennia taiemnyts ta vymoh prykhovanoho upravlinnia v operatsiiakh Druhoi svitovoi viiny [Securing secrets and Secret management requirements in the II World War Operations]. *Hazeta, Pivnichnoho operatyvno-terytoryalnoho komanduvannia. Viiskovi vidomosti*, 5 chervnya № 21 (98), s. 13. [in Ukrainian].

Vdovenko, S. H., Hulkov, M. A., Sydorov, S. V. & Dzhola, V. A. (2021). Zasoby kryptohrafichnoho zakhystu informatsii SRSR periodu Druhoi svitovoi viiny [Means of Cryptographic Information Protection of the USSR During the Second World War]. *Voienno-istorychnyi visnyk: zbirnyk naukovykh prats. K.: NUOU im. I. Cherniakhovskoho. Vyp.* 1 (39), s. 97–113. DOI:http:dx.doi.org/10.33099/2707-1383-2021-39-1-97-113. [in Ukrainian].

Vdovenko, S. H. & Danyk, YU. H. (2017). Kontseptualni napriamy kompleksnoho vyrishennia problemy zakhystu informatsii v systemi skrytoho upravlinnia zbroinykh syl [Conceptual directions of complex solution of the problem of information protection in the system of hidden control of the armed forces]. *Suchasni informatsiyni tekhnolohiyi u sferi bezpeky ta oborony. Naukovyy zhurnal*, № 2 (29), s. 98–106. [in Ukrainian].

Vdovenko, S. H., Danyk, YU. H. & Permyakov, O. YU. (2020). Dosvid rozvytku system kiberbezpeky ta kiberoborony inozemnykh derzhav [Experience in the development of cyber security and cyber defense systems of foreign countries]. *Suchasni informatsiyni tekhnolohiyi u sferi bezpeky ta oborony. Naukovyy zhurnal*, № 1 (37), s. 31–48. DOI: http:dx.doi.org/10.33099/2311-7249/2020-37-1-31-48. [in Ukrainian].

Hrebennikov, V. (2009). Uzhhorod. Istoriia kryptolohii & sekretnoho zviazku [History of cryptology and secret communication]. Vydannya druhe, vypravlennya, dopovnene, ilyustrovane. 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/ [Accessed: 27.05.2020]. [in Ukrainian].

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

Kyrjjan, M. A. (ed.). (1982). *Vnezapnost v operatsiyah VS SSHA* [Surprise in U. S. operations]. Moskva: Voenizdat, 328 s. [in Russian].

M-209 (CSP-1500). (2021). URL: http://www.jproc.ca/crypto/m209.html [Accessed: 27.05.2021]. [in English].

K-37 Crystal (2021). URL: https://www.cryptomuseum.com/crypto/ussr/k37/index.htm [Accessed: 27.05.2021]. [in English].

Sumarokov, V. P. (1999). Voennaya professiya — shifrovalschik [Military profession — cryptographer]. Moskva: RNT-tehnologii bezopasnosti, 174 s. [in Russian].

Uinterbotem, F. A. (1991). *Operatsiya "Ultra". Sekretnyie operatsii* [Operations "Ultra". Secretic operations]. Moskva: "Politicheskaya literatura", 654 s. [in Russian].

Shennon, K. E. (1963). *Teoriya svyazi v sekretnyih sistemah. Rabotyi po teorii informatsii i kibernetiki* [Communication theory in secret systems. Works on information theory and cybernetic]. Moskva: Inostrannaya literatura, 560 s. [in Russian].

Serhii Vdovenko
Master of State Military Management in the field of defence, Associate Professor of the Communication and Automated Systems Department of the Troopes (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
Faculty Instructor at the Communication and Information Systems Chair of the Troopes (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
Dr. habil., Professor of Chair of War History and Military Art, Institute of State Military Management,
The National Defence University of Ukraine named after Ivan Cherniakhovskyi
(Kyiv, Ukraine)
ORCID: https://orcid.org/0000-0002-1961-4251

Oleksandr Vdovenko
Student of group 4209 of the Troopes (Forces) Support and Information Technologies Institute, The National Defence University of Ukraine named after Ivan Cherniakhovskyi (Kyiv, Ukraine)
ORCID: https://orcid.org/0000-0001-8591-1249

TECHNIQUE OF INFORMATION CRYPTOGRAPHIC PROTECTION OF THE UNITED STATES OF AMERICA IN THE FIRST HALF OF THE XX CENTURY

The article considers technical progress in the field of information cryptographic protection and its impact on the command and control system in the operations of the first half of the twentieth century on the example of the creation and development of cryptographic equipment in the United States.

As historical experience shows, technical progress in the field of information cryptographic protection significantly influenced the results of operations and hostilities of that time.

Considering the military-historical aspects of this influence, it can be argued that the mass production of cryptographic information technology, integrated use of technology at various levels, tactical and operational, the use of training cryptographic equipment has influenced the development of cryptology, led to the development and adoption of new electronic and mechanical (electronic) means of cryptographic protection of information and decryption, as well as changes in the system of the United States national security.

Analysis of the results of practical implementation of these measures and theoretical research has led to the emergence and further development of new areas of science, communication and information theory, cryptology, cybernetics in the postwar period around the world and continues today.

It will be appropriate to apply this knowledge in modern conditions, based on the above events and facts, in order to increase efficiency, the introduction of various new models of cryptographic information security in various areas of management, including tactical.

Solving problems of management secrecy during the preparation and conduct of the Armed Forces Operation in modern conditions, in particular in the Joint Forces Operations in the East of Ukraine, requires consideration and use in Ukraine and its Armed Forces at all levels of management, scientific and technological progress.

Keywords: *covert troop management, cryptology, key systems, encryption technology, efficiency.*