

пропагандистських цілях та з метою виховання у воїнів необхідних морально–психологічних якостей.

Військова преса являла собою значну силу. Газета висвітлювала бойові справи і фронтовий досвід військ, була одним із головних засобів морально–психологічного забезпечення та політико–виховної роботи у військах, надавала діючої допомоги керівництву у підготовці військ до наступних операцій, у мобілізації воїнів на розгром ворога. Не тільки політоргани, але й багато хто з командуючих військами цікавились як висвітлюється в газетах бойовий досвід, підказували редакціям, які питання бойової підготовки треба ставити на перший план. У кінцевому рахунку конкретна і цілеспрямована виховна робота, проведена Військовими радами, політорганами, командирами з особовим складом військ фронту дала свої результати. У третій декаді жовтня 1944 року уся територія України повністю була звільнена від німецько–фашистських загарбників.

Отже, виховна робота з особовим складом, як важлива складова морально–психологічного забезпечення військ, відіграла надзвичайно велику роль у досягненні Перемоги у роки Другої світової війни. Вона сприяла безперервному зростанню бойової міцності частин, з'єднань та об'єднань, зміцненню морального духу військ, вихованню ненависті до ворога.

За роки війни склалася струнка система політико–виховної роботи керівництва армії та флоту з підлеглим особовим складом військ (сил), що в кінцевому рахунку дозволило отримати довгоочікувану Перемогу над німецько–фашистськими загарбниками.

Під час Львівсько–Сандомирської операції отримали подальший розвиток основоположні принципи морально–психологічного забезпечення особового складу Збройних сил. Ці принципи – тісний зв'язок із життям, конкретність і цілеспрямованість, активність, єдність організаційної та агітаційно–пропагандистської діяльності.

Досвід виховної роботи і психологічного гарту воїнів у роки Другої світової війни не втратив свого значення і в наші дні, незважаючи на те, що сьогодні відбулися суттєві зміни як в організації й озброєнні Збройних Сил, так і в ідеологічних орієнтирах та ціннісних орієнтаціях військовослужбовців. Вирішальною силою на війні залишається людина.

З урахуванням минулого досвіду, багато чого з “історичного арсеналу” може бути взято на озброєння сучасними організаторами виховної роботи та морально–психологічного забезпечення особового складу Збройних Сил України в сучасних умовах ведення нашою державою неоголошеної війни.

Список використаних джерел

1. Бойко О. В., Голик М. М., Кожевніков В. М. Військове навчання і виховання / Бойко О. В., Голик М. М., Кожевніков В. М. Навчально–методичний посібник. – Львів: ЛІСВ, 2007. – 153 с.
2. Великая Отечественная война 1941–1945: энциклопедия. – М.: Советская энциклопедия, 1985. – 832 с.
3. Горелов В. І., Крутиков С. О. Психологічний гарт, морально–бойове і політичне виховання воїнів Радянських Збройних Сил у період Великої Вітчизняної війни на території України: історичний аналіз (1941–1944 рр.) / Горелов В. І., Крутиков С. О. – К.: НДЦГП ЗСУ, 2005. – 79 с.
4. Крайнюков К. В. Оружие особого рода / Крайнюков К. В. –

М.: Воениздат 1964. – 590 с.

5. Маликов В. Г. Партино–политическая работа в Военно–Воздушных Силах на фронтах Великой Отечественной войны (1941–1945 гг.) / Маликов В. Г. – М.: ВПА им. Ленина, 1984. – 180 с.

6. Партино–политическая работа в Советских Вооруженных Силах в годы Великой Отечественной войны. – М.: Воениздат, 1963. – 528 с.

7. Ягупов В. В. Педагогіка / Ягупов В. В. Навч. посіб. – К.: Либідь, 2002. – 560 с.

References

1. Bojko O. V., Golyk M. M., Kozhevnikov V. M. Vijs'kove navchannya i vyhovannya / Bojko O. V., Golyk M. M., Kozhevnikov V. M. Navchal'no–metodychnyj posibnyk. – L'viv: LISV, 2007. – 153 s.

2. Velikaja Otechestvennaja vojna 1941–1945: jenciklopedija. – M.: Sovetskaja jenciklopedija, 1985. – 832 s.

3. Gorelov V. I., Krutikov S. O. Psihologichnyj gart, moral'no–bojove i polityчне vyhovannya voi'niv Radjans'kyh Zbrojnyh Syl u period Velykoj' Vitchyznanoi' vijny na terytorii' Ukraїny: istorychnyj analiz (1941–1944 rr.) / Gorelov V. I., Krutikov S. O. – K.: NDCGP ZSU, 2005. – 79 s.

4. Krajnjukov K. V. Oruzhie osobogo roda / Krajnjukov K. V. – M.: Voениzdat 1964. – 590 s.

5. Malikov V. G. Partijno–politicheskaja rabota v Voенно–Vozdushnyh Silah na frontah Velykoj Otechestvennoj vojny (1941–1945 gg.) / Malikov V. G. – M.: VPA im. Lenina, 1984. – 180 s.

6. Partijno–politicheskaja rabota v Sovetskih Vooruzhennyh Silah v gody Velykoj Otechestvennoj vojny. – M.: Voениzdat, 1963. – 528 s.

7. Jagupov V. V. Pedagogika / Jagupov V. V. Navch. posib. – K.: Lybid', 2002. – 560 s.

Golik M. M., Ph.D., Associate Professor, Department of Humanities, the Army Academy named after Hetman Sahaidachnogo (Ukraine, Lvov), lendmark2014@mail.ru

Education and moral and psychological support personnel of the Red Army under preparation and conduct of the L'vivsko–Sandomirskiy operations in 1944

This research work presents the historical analysis of the importance of educational work in L'vivsko–Sandomirskiy of operation 1944.

Keywords: military powers, applications of types of military powers and births of troops.

Голик Н. М., кандидат исторических наук, доцент, доцент кафедры гуманитарных наук, Академия сухопутных войск им. гетмана П. Сагайдачного (Украина, Львов), lendmark2014@mail.ru

Воспитание и морально–психологическое обеспечение личного состава Красной Армии в условиях подготовки и проведения Львовско–Сандомирской операции 1944 г.

Представлено исторический анализ значения воспитания и морально–психологического влияния на воинов Красной Армии в Львовско–Сандомирской операции 1944 г.

Ключевые слова: вооруженные силы, применение видов вооруженных сил и родов войск.

* * *

УДК 003.26

Чепур Б.

студент, Київський національний університет ім. Т. Шевченка (Україна, Київ), gileya.org.ua@gmail.com

“ЕНІГМА”: ІСТОРИЧНІ АСПЕКТИ ВИНИКНЕННЯ, ЗАСТОСУВАННЯ І ДЕШИФРУВАННЯ. НАЙПОТАЄМНІША СПЕЦОПЕРАЦІЯ “УЛЬТРА”

Розглянуто історичні аспекти виникнення і застосування німецької шифрувальної машини “Енігма”, а також аспекти її розшифрування, зокрема шляхом спецоперації “Ультра”.

Ключові слова: “Енігма”, “Ультра”, дешифрування, радіоелектронне шпигуство.

Протягом багатовікової історії людство завжди цікавила можливість обмінюватися важливою інформацією таємно, без ніякого страху, щоб зміст послання не було викрито. Військова історія була б не такою привабливою, якби обмежувалася лише військовими баталіями, адже поза театрами воєнних дій відбуваються й інші війни та битви, зокрема інформаційні.

Безперечно, війни ведуться за допомогою зброї і солдат, проте лише їх наявність або переважаюча кількість не є головним фактором перемоги. Девіз всесвітньовідомої династії підприємців Ротшильдів, який став вже давно усталеним виразом “Хто володіє інформацією, той володіє світом” підкреслює лише надзвичайну важливість якомога більших знань про супротивника. Тому розвідці та шпигунству в арміях усіх країн світу, під час воєн, приділяють найважливішу увагу. І саме перемагає той, хто має інформацію.

Зрозуміло, що чужу інформацію треба отримати, а свою захистити, тому такий вид воєн триває постійно, а в наші дні тим паче. Це підтверджують останні новини, а саме війна на Сході України проти проросійських банд-формувань, зокрема коли 20–22 січня відбувалися масштабні операції по утриманню донецького аеропорту. Проте намічених цілей “кіборгам” так і не вдалося досягти через багато перешкод, однією з яких, за повідомленням одного з них, який розповів “Українській правді”, стало те, що бойовики ДНР заволоділи рацією бійців ЗСУ і чули абсолютно всі переговори [6].

Тому дослідження історії німецької шифрувальної машини “Енігма”, її виникнення, застосування та дешифрування у період Другої світової війни країнами антигітлерівської коаліції, зокрема й проведену операцію “Ультра” по перехопленні військової інформації задля забезпечення перемоги є актуальним нині та досить важливим як для світу, так і для сучасної України, зважаючи на те, що забезпечення спеціальною шифрувальною технікою, шифрами та іншими засобами секретності при передачі наказів під час бойових дій, є обов’язковим атрибутом сучасних воєн, в тому числі інформаційних.

Мета статті: привернути увагу на перспективність використання шифрувальних машин в якості засобів передачі інформації під час бойових дій або при проведенні антитерористичних операцій.

В сучасній військовій історії певні аспекти проблеми є предметом зацікавлення, насамперед, зарубіжних дослідників, а саме П. Бізлі, І. Монтегю, Б. Анін, Л. Лайнер та інші. Однак донині вітчизняні фахівці слабо акцентують увагу на ній.

Одним із перших, хто почав активно застосовувати шифр у приватних листуваннях і під час військових кампаній був Гай Юлій Цезар, причому його різновид шифру в результаті отримав його ім’я. Загалом в світі існує велика кількість різних видів шифрів, а наука, яка вивчає методи шифрування і дешифрування інформації називається криптологією [1, с.88].

Потреби у шифруванні і дешифруванні інформації проходять крізь віки, але найбільшого розвитку набули в ХХ ст., коли відбулися трагічні Перша та Друга світові війни. Почали виникати один за іншим спеціальні шифрувальні апарати, тому що кожна країна

мала неабияку потребу у передачі, збереженні і нерозповсюдженні таємної стратегічної інформації.

Без сумніву найбільш відомою і практичною шифрувальною машиною в історії була “Енігма”, яка використовувалася Нацистською Німеччиною в роки Другої світової війни. Саме про неї та історію дешифрування знаменитої і, за думкою самих же німців, незламної “Енігми” буде далі йти мова.

Вагомий внесок у дослідженні використанні “Енігми” та зламу її шифрів зроблено у 80–90-х роках ХХ ст., адже лише 12 січня 1978 року уряд Англії дав офіційний дозвіл для робітників, котрі під час Другої світової війни працювали в Центрі урядового зв’язку над розкриттям німецького шифратора “Енігми”, про те, що віднині ті можуть відкрито говорити про дешифрування німецьких телеграм, однак їм все ще було заборонено розповідати про технічні особливості своєї роботи.

Як бачимо, англійський уряд ще близько сорока років після закінчення війни тримав у цілковитій секретності всі подробиці розшифрувальної операції, що отримала назву “Ультра”.

Одним із перших, хто почав відкрито піднімати це питання був Ф. Уінтерботем, колишній керівник авіаційної секції МІ-6. У 1974 році він опублікував книгу під назвою “Секрет Ультра”, яка викликала сенсацію. Перервавши мовчання цілого покоління, Уінтерботем розкрив найбільш ретельно приховану таємницю Другої світової війни: союзники розгадали німецькі коди і протягом всієї війни підслуховували переговори німців, що стосувалися військових, політичних та економічних проблем.

Таке проникнення в думки противника не мало прецедентів у військовій історії, і, щоб оцінити його значення, потрібен час. Здивовані військові історики почали розуміти: якщо одкровення Уінтерботема відповідають істині – а оскільки його книга була заборонена британською владою, схоже, так воно і було, – їм належало переосмислити багато фактів. Якщо, наприклад, генерали союзників, звеличувані за блискуче проведення військових кампаній, знали заздалегідь про плани противника, то не зменшує чи це блиск їхніх перемог? Чи не повинна бути переписана історія цих кампаній з урахуванням тієї переваги, якою володіли воєначальники союзників? Деякі з істориків вважали, що така необхідність є [3].

За першою книгою про спецоперацію “Ультра” швидко пішли й інші. Їх автори – Патрік Бізлі, Р. В. Джонс, Івен Монтегю, Ральф Беннет і Пітер Калвокорессі, як і Уінтерботем мали свого часу відношення до операції “Ультра”. Вражений таким потоком одкровень, британський уряд був вимушений відкрити деякі досє, пов’язані з “Ультра”, що дозволило Левіну написати книгу ““Ультра” йде на війну”, що стала першим звітом про найбільшу таємницю Другої світової війни, на основі офіційних документів.

В результаті змінилися акценти: генерал Ейзенхауер вважав, що “Ультра” внесла “вирішальний внесок у перемогу”, генерал Макартур надавав “найбільше значення” “Ультра”, Черчіль не міг нею натішитися, так як вважав, що “Ультра” – це те, “чим ми виграли війну” [3].

Протеоднозначнопроголосити, що лише завдяки “Ультрі” вдалося виграти війну, мабуть буде все ж неправильно, адже насправді героїчні зусилля солдат і правильні рішення командирів дали позитивний результат, але і заперечувати визначний внесок від цієї широкомасштабної дешифрувальної операції не буде правильним.

Власне кажучи, історія шифрувальної машини “Енігма” розпочинається з 1917 року, коли голландець Кох запатентував електричний роторний шифрувальний пристрій для захисту комерційної інформації. У 1918 році німець Артур Шербіус купив цей патент, доопрацював його і побудував нову шифрувальну машину. В цьому ж році він разом зі своїм другом Річардом Ріттером заснував компанію “Шербіус і Ріттер”. Спочатку її основною продукцією були подушки з підігрівом. Товар користувався попитом, і справи фірми йшли в гору. Однак Шербіус мріяв не тільки про матеріальний успіх, але й про впровадження у виробництво свого улюбленого дітища – електромеханічного пристрою для автоматизації процесу шифрування повідомлень, яке він охрестив “Енігмою”, що в перекладі з грецької означає “загадка”.

До 1923 року А. Шербіус зумів створити надійно працюючий і цілком компактний, розміром з друкарську машинку, зразок. Винахідник позиціонував “Енігму” в першу чергу як засіб збереження конфіденційності ділового листування від конкурентів і пропонував її крупним фірмам. Незважаючи на активну рекламну кампанію, розгорнуту ним в пресі, охочих придбати “Енігму” не було. Потенційних споживачів відлякувала надто висока ціна.

Тоді А. Шербіус запропонував свій продукт військовим. Але ті теж поставилися до машини з прохолодою. Тут історія “Загадки” могла б і закінчитися, так власне і не розпочавшись, якби не Вінстон Черчіль, який в роки Першої світової війни був англійським військово–морським міністром (Першим лордом Адміралтейства). Все в тому ж 1923 він опублікував мемуари, в яких розповів, як англійці зламали німецький військово–морський код і регулярно читали німецькі шифровки [5, с. 20].

Отже, саме це досягнення англійської розвідки в Першій світовій війні змусило німецьких військових визнати, що командування військово–морськими силами Німеччини, чії повідомлення по радіо перехоплювалися і дешифрувалися англійцями, образно кажучи, нівелювали всі їхні здобутки та плани.

Всебічно дослідивши шифрувальну машину, німецькі військові прийшли до однозначного висновку, що саме “Енігма” допоможе їм не допустити повторення подібної ситуації в майбутньому. У 1925 році Шербіус приступив до масового виробництва “Енігми”, якою, починаючи з наступного року, стали оснащуватися збройні сили і спецслужби Німеччини. Протягом наступних двох десятиліть було виготовлено більше 30 тисяч екземплярів “Енігми”.

На жаль, Артур Шербіус помер дуже рано, щоб повною мірою насолодитися грандіозним успіхом свого винаходу. 12 травня 1929 він їхав в екіпажі, запряженому кіньми, аж раптом, коні понеслися і він не зміг їх зупинити, і на повному ході екіпаж розбився об

стіну. На наступний день А. Шербіус помер не приходячи до тями [4].

Крім німців, цю шифрувальну машину придбали й армії інших європейських країн. Так, наприклад, одну з версій “Енігми” придбав для своїх нужд шведський генеральний штаб [1, с.118].

Варто зауважити, що пристрій шифрувальної машини “Енігма” на той час був дуже складним. Ззовні вона виглядала як друкарська машинка, встановлена в дерев’яному ящику, і складалася з декількох складових частин. На клавіатурі, що була схожою на клавіатуру звичайної друкарської машинки, набирался відкритий текст. У так званій шифрувальній частині відбувалося перетворення букв і цифр відкритого тексту в шифроване повідомлення. На сигнальній панелі розташовувалися електричні лампочки, світіння яких вказувало букву шифрованого тексту, адекватно якій замінювалася відповідна літера відкритого тексту.

З передньої сторони машини, під клавіатурою, знаходилася сполучна панель або контактна панель з шістьма кабелями. Безпосередньо шифрувальна частина в комерційних версіях “Енігми” складалася з трьох взаємозамінних комутаційних дисків, які стали називатися скремблерами – від англійського слова “scramble”, що можна перекласти як “хаотично збирати” [1, с.118].

Слід наголосити, що в німецькій армії широко використовувалися декілька версій “Енігми”. Найпростіша версія використовувалася у сухопутних військах. Більш складні моделі, що забезпечували і більш високий ступінь захисту передачі шифрованих повідомлень, комплектували деякі літаки німецьких військово–повітряних сил. Але найбільш досконалі версії “Енігми” встановлювалися на кораблях і підводних човнах німецького флоту.

Зрештою, потрібно визнати, що машина “Енігма” забезпечувала набагато більш високий рівень захисту шифрованих повідомлень, ніж більшість відомих в той час електромеханічних шифрувальних апаратів. Тому німці, безумовно, пишалися своїм винаходом. Тим не менш постійно велися роботи по удосконаленню “Енігми” [1, с.120].

До початку Другої світової війни німці продовжували вірити у невразливість своєї системи шифрування, проте багато шифрограм “Енігми” були прочитані противниками Німеччини ще до 1 вересня 1939 року.

Першою зайнялася розшифровкою німецьких кодів Польща. Після Першої світової війни вона перебувала в постійній військовій небезпеці з боку обох своїх сусідів – Німеччини та СРСР, які мріяли повернути собі втрачені землі, що перейшли до Польщі. Щоб не опинитися перед несподіванками, поляки записували радіоповідомлення і займалися їх розшифровкою. Вони були сильно стурбовані тим, що після введення в лютому 1926 р. в німецькому військово–морському флоті “Енігми”, а також після її введення в сухопутних військах у липні 1928 р. їм не вдалося розшифрувати зашифровані цією машиною повідомлення.

Можливо поляки так би й не відіграли значної ролі та й не дали старт у розшифровці німецьких кодів, якби не один вагомий випадок.

У січні 1929 р. на варшавську митницю з посольства Німеччини в Польщі прийшло повідомлення, згідно з яким необхідно було якомога швидше передати працівникам посольства коробку, що потрапила через непорозуміння на варшавську митницю. Таке жорстке прохання Берліна привернуло увагу до цієї коробки і поляки відкрили її. Там було виявлено комерційний варіант “Енігми”. Лише після вивчення її віддали німцям, але це не допомогло розкрити їх хитрощі. Справа в тому, що в міністерстві оборони Німеччини був прийнятий на озброєння шифратор, який значно відрізнявся від комерційного варіанту “Енігми” [4].

Спеціально для боротьби з “Енігмою” військова розвідка Польщі створила “шифрувальне бюро” з кращих математиків, що вільно володіли німецькою мовою, до складу якого увійшли Маріан Режевський, Генріх Зігальський та Єжи Рожицький. Згодом, саме ця трійця і зуміє розгадати перші шифри “Енігми”. Але все ж передумовами розкриття таємниці стали наступні події.

Влітку 1931 року агент французької розвідки Рудольф Лемуан завербував співробітника шифрувального бюро Міністерства оборони Німеччини Ганса Шмідта, а восени зумів отримати від нього копію керівництва з експлуатації до шифрувальної машини “Енігма”. На розчарування Лемуана французькі криптографи вирішили, що цей документ не має ніякої цінності, адже не дає розуміння саме про пристрій машини, а тільки пояснює, які операції повинен здійснювати на ній шифрувальник. Французи не придумали нічого іншого, як надати цей матеріал польському шифрбюро, яке вже давно намагалося навчитися читати німецьку секретну переписку. Поляки також підтвердили, що ці матеріали не дозволяють читати німецьку військову переписку, тому що необхідні були ще ключові установки для “Енігми”, які пізніше – в травні та вересні 1932 р. були отримані від Шмідта [5, с. 21].

Після цього фірма “AVA”, яка виконувала різні замовлення польської розвідки, виготовила точну копію “Енігми”. Використовуючи її, криптографи Режевський, Рожицький і Зігальський розробили так званий характеристичний метод обчислення початкових установок. За допомогою нього поляки довгий час досить успішно читали шифровані німецькі повідомлення, починаючи з 1933 і до 1938 року, коли німці серйозно змінили процедуру використання ключових установок, ввівши, зокрема, “разові ключові установки” (початкові положення дисків змінювались при кожному сеансі зв’язку). Це призвело до серйозних труднощів у роботі польських криптоаналітиків [4].

Проте у відповідь поляки придумали два нових методи, яким згодом судилося зіграти дуже істотну роль при зломі “Енігми”. Це були перфокарти і так звана “Бомба”.

Після війни ніхто з польських криптоаналітиків так і не зміг пригадати, чому кілька з’єднаних разом “Енігм” назвали “Бомбою”. За однією з версій, Режевський, Зігальський і Рожицький, коли їх осінила ця ідея, сиділи в кафе і їли фірмове морозиво під назвою “Бомба”. За іншою версією, у винайденому ними пристрої досить своєрідним датчиком служили кілька невеликих грузил, які, подібно бомбі, падали вниз, коли

розкривалися шукані ключові установки для “Енігми”. Перша “Бомба” була виготовлена в листопаді 1938 р. і складалася з шести “Енігм” – по одній для кожного варіанту розташування дисків в “Енігмі”. Щоб визначити порядок проходження дисків в “Енігмі”, було потрібно не більше двох годин роботи “Бомби”. До цього часу продуктивність “Бомби” стала вирішальним фактором, який забезпечив полякам успіх у роботі над зломом “Енігми”. Якщо на початку 1933 року, коли Режевський зумів відновити внутрішні з’єднання всіх дисків і рефлектора “Енігми”, німці міняли порядок проходження дисків кожні три місяці, то в 1936 році це вже робилося спочатку щомісяця, а потім і щодня [4].

Анексія Австрії і всезростаюча загроза зі сторони Німеччини спонукали Англію, Польщу і Францію об’єднати свої зусилля в області радіошпигунства. До цього часу німці модифікували і “Енігму”, і процедуру передачі повідомлень, зашифрованих нею.

Зміни в практиці шифрування повідомлень за допомогою “Енігми” надали ще більшої важливості давно запланованій трьома країнами зустрічі спеціалістів–криптоаналітиків стосовно обговорення наявного стану справ по розкритті “Енігми” та прискорили її проведення [2, с. 343].

У Варшаві 24–25 липня 1939 року пройшла нарада, в якій брали участь англійський криптограф Ділі Нокс, директор англійської Урядової криптографічної школи Алістер Денністон, начальник шифрувального відділу французького Другого бюро Гюстав Бертран і французький криптограф Генрі Бракені. Вони дізналися, нарешті, від своїх польських колег про дешифрування ними “Енігми”. Присутні на нараді англійці і французи отримали від польської сторони по одній копії шифратора разом з інструкціями з виготовлення та використання перфокарт для з’ясування ключових установок [4].

Невдовзі після зустрічі Польща зазнала нищівної поразки від Німеччини, і польські криптоаналітики були змушені переїхати до Франції. З цього часу криптоаналітичні методи, випробувані на практиці польськими спеціалістами, почали використовувати й англійці. На початку 1940 року вони навіть самостійно розкрили ключ “Люфтваффе”, а також зайнялися вдосконаленням “Бомби” [2, с. 343].

В Англії центром робіт зі взламу “Енігми” став маєток вікторіанської епохи Блетчлі–парк в ста кілометрах від Лондона, де збиралися найкращі уми того часу. Блетчлі–парк став свого роду студентським містечком для особливо обдарованих англійських математиків, лінгвістів та криптографів. Першим серед них був Алан Тюрінг. В історію науки він увійшов як один із засновників сучасної інформатики. Також туди увійшли Мілнер Баррі, Гордон Уелгмет та інші. Саме їм вдалося здійснити величезний внесок подальше розшифрування “Енігми” – створити дешифрувальну машину “Бомба”, принцип якої полягав у переборі можливих варіантів ключа шифру і спроб розшифровки тексту, якщо була відома частина відкритого тексту або структура розшифрованого повідомлення. Перебір ключів виконувався за рахунок обертання механічних барабанів, що супроводжувався звуком, схожим на цокання годинника, через що “Бомба” і отримала свою назву.

Після першого успішного читання німецького шифр-повідомлення з 1940 р. перед англійцями постала проблема: з однієї сторони, треба було не скомпрометувати винахід, а з іншої – максимально використовувати джерело інформації. Було вирішено, що начебто інформація надходить від високопоставленого агента в Берліні під псевдонімом Боніфацій [2, с. 345].

Сама ж операція із розшифрування “Енігми” отримала назву “Ультра” і трималася в надзвичайній таємниці. Прем’єр-міністр Великої Британії Вінстон Черчіль особисто контролював роботу в Блетчлі-парк і надзвичайно ретельно зберігав усі дані про неї. Найбільш відомий випадок в історії, в той же час, найбільш жахливий з точки зору людської моралі, пов’язаний з “Енігмою”, коли національні й світові інтереси були поставлені вище людських життів стався 15 листопада 1940 року. З матеріалів “Ультра” англійці напередодні дізналися про варварський план Німеччини: в ніч з 14 на 15 листопада її літаки повинні були здійснити наліт на англійське місто Ковентрі і стерти його з лиця землі. В. Черчіль прийняв нелегке, однак жорстоке щодо власного народу рішення: в інтересах збереження таємниці навколо “Ультра” не попередив про наліт і не здійснив ніяких заходів щодо захисту міста. У призначений день від містечка Ковентрі залишилася лише одна назва.

Були й інші випадки, менш масштабніші, коли гинули й спеціальні агенти і невинні люди, аби таємницю “Ультри” було не розкрито. І як ми бачимо, справді, про розкриття інформації щодо дешифрування “Енігми” світова спільнота дізналася через десятки-десятки років після завершення Другої світової війни. Англійці вміло зберігали свої секрети. Навіть якщо взяти до уваги саму назву операції “Ультра”, то за деякими даними з неї був знятий гриф “Цілком таємно”, проте “Ультри” надали рівень надсекретності, та назву “Ультра таємно”, скорочено “Ультра”.

Підсумовуючи вище викладене, варто наголосити на, справді значному внеску англійських спецслужб у радіошифруванні і, особливо, у розшифруванні німецької шифрувальної машини “Енігма”, завдяки чому була надана суттєва допомога країнам антигітлерівської коаліції у боротьбі та руйнуванні планів спецоперацій нацистської Німеччини. Британські та американські дослідники, прославляючи внесок співробітників з Блетчлі-парку у перемозі над німцями, вкотре акцентують увагу на тому, що завдяки дешифруванню “Енігми” вдалося перемогти і закінчити війну на декілька років раніше. Тому британці дуже вихваляють свої здобутки.

Очевидно, що така думка, безумовно, в певній мірі є вірною. Проте, не можна не згадати, про надзвичайно важливий внесок польських вчених, які фактично задали алгоритм зламу кодів “Енігми”, а також французьких спецслужб, які здобули найціннішу інформацію, яка допомогла в майбутньому.

В решті-решт, перемога була здобута зусиллями країн, що воювали проти Німеччини, шляхом втрати величезних людських життів в продуманих тактичних операціях, які в свою чергу були максимально забезпечені інформацією про ворога, що надавала розвідка. Тому знання про кількість, стан, моральний

дух і плани супротивника – це майже половина перемоги у битві або війні. “Інформований – значить забезпечений” – таким принципом завжди керувалися, керуються і будуть керуватися в майбутньому як задля особистої безпеки, так і задля національної безпеки країни.

І на останок, з цього уроку історії важливо зробити застереження – ніяка техніка, навіть суперсучасна по шифруванню таємної інформації не може ставати “ідолом” заради якого можна віддавати накази чинити злочини проти людства.

Список використаних джерел

1. Адаменко М. В. Основы классической криптологии: секреты шифров и кодов. – М.: ДМК Пресс, 2012. – 256 с.
2. Анин Б.Ю. Радиоэлектронный шпионаж. – “Секретная папка”. – М.: ЗАО Изд-во Центрполиграф, 2000. – 493 с.
3. Knightley Ph. The Second Oldest Profession: Spies and Spying in the Twentieth Century. – London, 1987 // Найтли Ф. Шпионы XX века [Електронний ресурс]. – Режим доступу: http://militera.lib.ru/research/knightley_p/08.html
4. Лайнер Л. Погоня за “Энигмой”. Как был взломан немецкий шифр. – М.: Молодая гвардия, 2004. – 316 с. [Електронний ресурс]. – Режим доступу: http://www.ereading.link/bookreader.php/1017951/Layner_Pogonya_za_Enigmoy_Kak_byl_vzloman_nemeckiy_shifr.html
5. Смирнов К. “Загадка”, так и оставшаяся загадкой / Константин Смирнов // Техника-молодёжи. – 2011. – №934. – С.20–25.
6. Українська правда – інтернет-газета [Електронний ресурс]. – Режим доступу: <http://www.pravda.com.ua/news/2015/01/22/7055931/?attempt=1>

References

1. Adamenko M. V. Osnovy klassicheskoy kriptologii: sekrety shifrov i kodov. – M.: DMK Press, 2012. – 256 s.
2. Anin B. Ju. Radioelektronnyj shpionazh. – “Sekretnaja papka”. – M.: ZAO Izd-vo Centrpoligraf, 2000. – 493 s.
3. Knightley Ph. The Second Oldest Profession: Spies and Spying in the Twentieth Century. – London, 1987 // Najtli F. Shpiony XX veka [Elektronnyj resurs]. – Rezhym dostupu: http://militera.lib.ru/research/knightley_p/08.html
4. Lajner L. Pogonja za “Jenigmoj”. Kak byl vzloman nemeckij shifr. – M.: Molodaja gvardija, 2004. – 316 s. [Elektronnyj resurs]. – Rezhym dostupu: http://www.ereading.link/bookreader.php/1017951/Layner_Pogonya_za_Enigmoy_Kak_byl_vzloman_nemeckiy_shifr.html
5. Smirnov K. “Zagadka”, tak i ostavshajasja zagadkoj / Konstantin Smirnov // Tehnika-molodjozhi. – 2011. – №934. – S.20–25.
6. Ukrai'ns'ka pravda – internet-gazeta [Elektronnyj resurs]. – Rezhym dostupu: <http://www.pravda.com.ua/news/2015/01/22/7055931/?attempt=1>

Chepur B., student, Taras Shevchenko National University of Kyiv (Ukraine, Kyiv), gileya.org.ua@gmail.com

“Enigma”: historical aspects of occurrence, application and decryption. Secret special operations “Ultra”

The historical aspects of the origin and use of the German cipher machine “Enigma” and also the history of its decryption, in particular by special operation “Ultra”.

Keywords: “Enigma”, “Ultra”, deciphering, radioelectronic spying.

Чепур Б., студент, Киевский национальный университет им. Т. Шевченко (Украина, Киев), gileya.org.ua@gmail.com

“Энигма”: исторические аспекты возникновения, применение и дешифровки. Тайная спецоперация “Ультра”

Рассмотрены исторические аспекты возникновения и применения немецкой шифровальной машины “Энигма”, а также аспекты ее дешифровки, в частности путем спецоперации “Ультра”.

Ключевые слова: “Энигма”, “Ультра”, дешифрование, радиоэлектронный шпионаж.

* * *