Буга Леся Василівна
викладач,
Львівський університет бізнесу та права
https://orcid.org/0000-0002-9034-7301

ДОСВІД США ТА НІМЕЧЧИНИ ЩОДО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ЗБРОЙНИХ СИЛАХ

JEL Classification: K 19
SECTION "LAW": Право.

Анотація. У статті, на основі аналізу наукових поглядів вчених, розглянуто досвід США та Німеччини щодо забезпечення інформаційної безпеки в збройних силах. Наголошується, що удосконалення сфери забезпечення інформаційної безпеки в Збройних силах України неможна проводити швидко, за рахунок «наспіх створеного» пакету нормативно-правових актів, воно повинно грунтуватись, перш за все, на дослідженні зарубіжного досвіду в аналогічних галузях.

Ключові слова: інформаційна безпеки, збройні сили, США, Німеччина, забезпечення, законодавство.

Annotation. The article, based on the analysis of scientific views of scientists, examines the experience of the USA and Germany in providing information security in the armed forces of Ukraine. It is noted that improvement of the sphere of information security in the Armed Forces of Ukraine can not be carried out quickly due to the "hastily created" package of normative legal acts, and should be based, first of all, on the study of foreign experience in similar industries.

It should be noted that Germany is one of the States that actively uses the benefits of the private sector in providing state agencies. Thus, the "Hercules" program is the largest public-private partnership project ("Public-Private Partnerships") in Europe. Implementation of the program within the framework of an agreement between the federal agency for the development and procurement of armaments of the Bundeswehr and the joint venture "Information-stechnik GmbH". The purpose of the latter is the introduction of the latest technologies, in particular in the field of information security, in the activities of the Ministry of Defense of Germany and the Armed Forces. In general, much attention is paid to the innovative provision of the Ministry of Defense of the Federal Republic of Germany and the Armed Forces of this country. The sector is constantly implementing new information systems and communication technologies, as well as software for their protection.

The analysis of foreign experience, allowed to highlight the peculiarities of building an information policy and different approaches to providing information security in the Armed Forces in the United States and Germany.

That is why the purpose of the article is to: to consider the positive experience of the USA and Germany in providing information security in the armed forces of Ukraine.

Keywords: information security, armed forces, USA, Germany, provision, legislation.

Вступ

Сучасна Україна є правовою державою, а також активним та досить значимим гравцем міжнародної арени. Про це кажуть хоча б ті факти, що наша країна є членом великої кількості всесвітніх організаціях, таких як, наприклад, Рада Європи, Організація Об'єднаних Націй, Європейська економічна комісія ООН тощо. Крім того, з недавніх пір вектор розвитку України набув євроінтеграційного направлення, що пов'язано із активною ескалацією політико-економічних процесів з метою входження нашої держави до складу Європейського Союзу. Такі глобальні цілі еволюції обумовлюють необхідність змін багатьох правових механізмів у відповідності до міжнародних стандартів, адже, як показує практика, зарубіжні моделі управління тією чи іншою сферою життєдіяльності суспільства в більшості випадків є прогресивнішими за вітчизняні. Водночас, сліпе впровадження нових правових тенденцій, категорій чи явищ, без апробаційного періоду та попереднього аналізу, може привести до більш негативних результатів, ніж використання чогось застарілого. Особливо гостро даний аспект постає, якщо мова йде про забезпечення інформаційної безпеки в Збройних Силах України.

Дослідженню зарубіжного досвіду забезпечення інформаційної безпеки в збройних силах присвячували увагу: І.О. Чернухін, С.В. Смолинов, О.В. Олійник, С.О. Комов, В.О. Копилов, В.В. Копєйчиков, Т.А. Костецька, О.В. Кохановська, В.Г. Крисько, С.П. Кудрявцева, Н.В. Кушакова, М.Б. Левицька, та багато інших. Однак, реалії сьогодення, вимагають від законодавця пошуку нових шляхів удосконалення зазначеної сфери. Реалізацію таких реформ неможна проводити швидко, за рахунок «наспіх створеного» пакету нормативно-правових актів, а повинно ґрунтуватись, перш за все, на дослідженні зарубіжного досвіду в аналогічних галузях.

Саме тому **метою статті є:** розглянути позитивний досвід США та Німеччини щодо забезпечення інформаційної безпеки в збройних силах України.

Результати дослідження

Першим об'єктом наукової розробки в рамках даного наукового дослідження є досвід Сполучених Штатів Америки. Зазначимо, що на сьогоднішній день ця країна володіє найпотужнішою оборонною системою та одними з найбільш сильних Збройними Силами у світі. Даний аспект обумовлю наявність ефективного та дієвого механізму внутрішнього забезпечення інформаційної безпеки в усіх ланках державного та військово-адміністративного управління зокрема. Головною перевагою досвіду США в сфері забезпечення інформаційної безпеки в ЗС є те, що керівництво держави почало перейматись даним питанням ще у XX столітті, так як в цей період Сполучені Штати вже мали статус лідера у розвитку інформаційних технологій. Соціально-економічні, воєнні та політичні наслідки інформаційної революції стали найбільш відчутними в цій державі. Америка раніше за інші країни зіткнулася з інформаційними загрозами національної безпеки. В результаті цього США стали першими, хто розпочав розробки державної політики у сфері інформаційної безпеки [1, с.281]. Крім того, якщо брати до уваги механізм забезпечення інформаційної безпеки в Збройних Силах Сполучених Штатів, то його формування почалось у 50-60-х роках XX століття. Смолінов С.В. з цього приводу зазначає, що закінчення Другої світової війни не наблизило людство до загального і остаточного миру. Відразу ж після її завершення між колишніми союзниками по антигітлерівській коаліції розгорнулося запекле протистояння в рамках «холодної війни», в якій важливою складовою була інформаційна війна. У зв'язку із цим виникла необхідність забезпечення інформаційної безпеки не тільки суспільства на території Сполучених Штатів, а й інформаційної безпеки військовослужбовців Збройних Сил цієї держави [2].

Починаючи з 1992 року основні зусилля по організації заходів у сфері інформаційної безпеки в Збройних Силах було здійснено Міністерством оборони США в рамках концепції «Інформаційного протиборства», що орієнтована на вирішення завдань боротьби з системами управління воєнними силами супротивника на різноманітних рівнях і забезпечення безпеки та ефективності своїх інформаційних систем армії США. Подальший розвиток ця концепція отримала в 1996 році у вигляді польового статуту армії США «Інформаційні операції». В цілому ж початком сучасної цілеспрямованої систематичної організаційної діяльності у сфері інформаційної безпеки на національному рівні можна вважати директиви адміністрації Президента Білла Клінтона «Presidential Decision Directive 63» (PDD 63) (Захист критично важливої інфраструктури)» 1998 року. На цьому документі базується підписаний Клінтоном Б. на початку 2000 року «Загальнонаціональний план захисту інформаційних систем», який визначає основні напрями діяльності держави та всього суспільства у сфері забезпечення інформаційної безпеки [1, с.282; 3].

На сьогоднішній день рівень забезпечення інформаційної безпеки в Збройних Силах США є досить високим. Це обумовлюється особливостями адміністративного регулювання в даній сфері та постійним впровадженням новітніх технологій. Так, ключовими суб'єктами забезпечення інформаційної безпеки в структурі ЗС США виступає Кіберкомандування США та спеціальний підрозділ Міністерства оборони – Управління програм з інформаційної безпеки.

Спектр повноважень останнього є досить широким. Головним здобутком є те, що Управлінням формуються й реалізуються програми всебічного навчання, тренування й інформування («Education, Training and Awareness») військовослужбовців, цивільного персоналу і службовців за контрактом. Тобто, формується необхідний мінімум базових знань у галузі інформаційної безпеки, що діє для усіх користувачів інформаційних систем та без якого вони не можуть бути допущені до роботи. Однією з ключових вимог даного підрозділу є щорічна перепідготовка, яку повинен проходити увесь персональний склад. Навчально-методичні матеріали, які створені фахівцями управління, активно впроваджуються для навчання і тестування персоналу інших відомств [4]. Таким чином, найбільш позитивним аспектом у роботі Управління програм з інформаційної безпеки виступає саме навчальний процес, відповідно до якого військовослужбовців не просто контролюють в процесі дотримання якихось правил в сфері забезпечення інформаційної безпеки, а надають їм нових навичок, знань та вмінь в цій галузі.

Безпосередньо в структурі Збройних Сил Сполучених Штатів Америки, суб'єктом забезпечення інформаційної безпеки виступає Кіберкомандування США, яке синхронізує, об'єднує, координує та провадить відповідні дії щодо керування функціонування і захистом інформаційних мереж спеціалізованого типу Міністерства оборони США. Трьома основними напрямами роботи командування є: захист інформаційних мереж та систем Збройних Сил США та Міноборони; надання підтримки командувачам-комбатантам для виконання своїх місій по всьому світу та посилення здатності США у сфері протистояння кібер-атакам; реагувати на кібер-атаки [5].

Командування об'єднує напрями операцій в кіберпросторі, зміцнює можливості Збройних Сил у кіберпросторі, покращує можливості ЗСУ щодо використання надійних інформаційно-комунікаційних мереж, протидії загрозам кіберпростору та забезпечення доступу до кіберпростору. Окрім того, Кіберкомандування розробляє структуру кібер-сил, вимоги до підготовки та стандарти сертифікації, які дозволять іншим державним службам будувати кібер-сили, необхідні для виконання поставлених завдань [5].

Не менш позитивним є досвід США у питання програмно-технічного супроводження механізму забезпечення інформаційної безпеки в Збройних Силах. Зокрема, необхідно відмітити ефективність дії автоматизованої системи управління військами, нормативно-правовою основою якої виступає стратегічна концепція США «З'єднання та функціональна інтеграція систем керування, зв'язку, обчислювальної техніки та розвідки» («C4I» або «Command, Control, Communications, Computers and Intelligence»). В основу інформаційної інфраструктури «C4I» покладено сукупність інформаційних систем оперативно-стратегічного, оперативно-тактичного і тактичного рівнів управління, взаємопов'язаних як по вертикалі, так і по горизонталі. Головні принципи створення і вдосконалення інфраструктури є: висока надійність централізованого управління; можливість децентралізованого управління в окремому регіоні; високий ступінь готовності системи, що забезпечує безперервність управління; широкі можливості з оперативного збору, обробки і доведення необхідної інформації; забезпечення стійкості і живучості системи управління; висока скритність управління як під час повсякденної діяльності, так і під час ведення операцій. З технічного боку «C4I» – це глобальна територіально розподілена інтегрована телекомунікаційна система інформаційно-обчислювальних центрів та автоматизованих робочих місць, розгорнутих на командних пунктах штабів і пунктах управління збройних сил, що функціонує за принципом єдиного інформаційного простору [6, с.4].

На наступному етапі наукового дослідження розглянемо позитивні моменти в сфері забезпечення інформаційної безпеки в Збройних Силах Німеччини. Слід відмітити, дана країна є однією з найбільш розвинутих держав Західної Європи в галузі інформаційної безпеки. Вона має розвинуту структуру органів, які займаються захистом різних видів інформації, зокрема інформації з обмеженим доступом. Від самого початку створення цієї системи захисту інформації увагу було направлено на захист від промислового шпигунства й охорону державних секретів. Характерною особливістю для цієї країни є те, що установи, які вперше займалися окресленими питаннями, почали створюватися ще в 19 столітті. Наступним етапом у становленні німецької системи захисту інформації став початок XX століття. Адже відомо, що саме в Німеччині в 1914 – 1918 роках під час Першої світової війни, особливо в армії, була достатньо сильною й передовою на той час система криптографічного захисту інформації [7, с.7].

На сьогоднішній день питання інформаційної безпеки в Німеччині не втратило своєї актуальності, особливо, якщо мова йде про військову сферу. Цей аспект, зокрема, досить яскраво виражається у низці нормативно-правових актів доктринального характеру до яких відноситься: «Ключові напрями політики ФРН в галузі оборони» від 2003 року; «Концепція реформування бундесверу» від 2004 року; «Про засади діяльності вищих органів військового управління ФРН» від 2005 року; «Медіаконцепція бундесверу», «Концепція проведення інформаційних операцій» тощо [8].

Щодо організаційної сторони забезпечення інформаційної безпеки в Збройних Силах Німеччини, то вона характеризується високим рівнем централізації. При цьому, як і у Великобританії, одним з ключових секторів інформаційної безпеки виступає кіберзахист. З огляду на даний фактор, з метою оптимізації оперативного співробітництва між усіма державними установами й поліпшення координації заходів із захисту інформації, протидії кібератакам в ФРН створено Національний центр кіберзахисту («Nationales CyberAbwehrzentrum» – NCAZ). Центр функціонує у сфері управління Федерального відомства захисту інформаційних систем (формує вимоги із захисту інформації в інформаційних системах держави) при безпосередній участі співробітників Федерального відомства захисту конституційного ладу [9; 10, с.32].

Крім зазначених відомств забезпеченням інформаційної безпеки в Збройних Силах Німеччини також знаходиться у віданні Міністерства оборони ФРН та його структурних підрозділів. Відповідно до покладених на Міноборони Обов'язків, останнє є федеральним органом виконавчої влади, що здійснює функції з вироблення і реалізації державної політики в галузі оборони, а також інші встановлені федеральними законами Німеччини, актами уряду країни і міжнародними договорами функції в цій області. Міноборони

забезпечує нормативно-правове регулювання в галузі оборони та діяльності Збройних Сил, а також підтримує останні в бойовій готовності. Відповідні повноваження зазначений орган має у сфері забезпечення інформаційної безпеки в Збройних Силах України, реалізацією яких займається його структурний підрозділ – Головне управління кібер та інформаційних технологій [11]. Останнє відповідає за формування і реалізацію політики в області кібероборони держави, займається плануванням дій в інформаційно-комунікаційному просторі, реалізацією заходів інформаційно-технічної безпеки бундесверу, плануванням розвитку сил і засобів кібероперацій, їх застосування і вивчення такого досвіду, а також забезпеченням програм модернізації Збройних Сил ФРН та інформаційної безпеки у їх структурі [11]. У системному підпорядкуванні цього органу знаходиться Командування зв'язку та інформаційних технологій, яке призначено для організації централізованого управління і зв'язку між видами Збройних Сил і міжвидових підрозділів, забезпечення функціонування автоматизованих систем управління і засобів комунікації, навчання фахівців цього профілю [12].

В додаток до наведених моментів, необхідно відмітити, що Німеччина є однією з держав яка активно використовує переваги приватного сектору в процесі забезпечення державних відомств. Так, програма «Геркулес» є найбільшим в Європі спільним проектом державного і приватного секторів («Public-Private Partnerships»). Виконання програми в рамках відповідного договору між федеральним відомством з розробки та закупівлі озброєнь бундесверу і спільним підприємством «Information-stechnik GmbH». Ціллю останньої виступає впровадженням новітніх технологій, зокрема в сфері забезпечення інформаційної безпеки, у діяльність Міноборони Німеччини та Збройних Сил. Загалом, інноваційному забезпеченню діяльності Міноборони ФРН та ЗС цієї держави приділяється велика увага. В даний сектор постійно здійснюється впровадження нових інформаційних систем та технологій зв'язку, а також формується програмне забезпечення щодо їх захисту [8].

Таким чином, в означеній вище країні необхідно констатувати наявність серйозного підходу керівництва держави до забезпечення інформаційної безпеки службовців оборонного сектор, зокрема, військовослужбовців Збройних Сил.

Висновки

- Отже, аналіз зарубіжного досвіду, дозволив висвітлити особливості побудови інформаційної політики та різні підходи до забезпечення інформаційної безпеки в Збройних Силах на території США та Німеччини, в результаті чого було зроблено наступні висновки:
- по-перше, в цих країнах на сьогоднішній день велику увагу приділено питанню кібербезпеки, яка виступає органічною частиною інформаційної безпеки в ЗСУ;
- по-друге, забезпечення інформаційної безпеки в Збройних Силах ґрунтується на високому рівні централізації повноважень в цій сфері в межах декількох органів, взаємопов'язаних та взаємозалежних між собою;
- по-третє, механізм забезпечення інформаційної безпеки постійно удосконалюється в аспекті активної технологізації, а також відповідної «перебудови» нормативних положень, в яких прописується правова позиція держави щодо впровадження інноваційних технологій.

Список використаних джерел

1. *Олійник О.В. Інформаційна безпека США / О.В. Олійник // Боротьба з організованою злочинністю і корупцією (теорія і практика). – 2012. – №1(27). – С.280 – 288.*
2. *Смолинов С.В. Информационная безопасность военнослужащих США в 50-90-е гг. XX века: По опыту локальных войн и военных конфликтов: автореферат / С.В. Смолинов // Москва. – 2000. – 221 с. – [Електронний ресурс]. – Режим доступу: http://www.dissercat.com/content/informatsionnaya-bezopasnost-voennosluzhashchikh-ssha-v-50-90-e-gg-xx-veka-po-opytu-lokalnyk.*
3. *Общая политика США в сфере информационной безопасности / [Елетронний ресурс]. – Режим доступу : http//:www.INTUIT.ru.*
4. *Деньщиков А. Л. Информационная стратегия США: автореферат/ А. Л. Деньщиков // [Електронний ресурс]. – Режим доступу: http: rudocs. exdat. com.*
5. *U.S. Cyber Command: стаття // Офіційний сайт Кіберкомандування США. – [Електронний ресурс]. – Режим доступу: https://www.cybercom.mil/About/Mission-and-Vision/.*
6. *Клімушин П.С., Кротов В.Д. Автоматизована система управління Збройних Сил України як сучасний різновид стратегічного озброєння / П.С. Клімушин, В.Д. Кротов // Теорія та практика державного управління. – 2014. – Вип.1(44). – С.1 – 8.*

7. Сідак В. Організація системи захисту інформації в Німеччині: еволюція та сучасний стан / В.Сідак // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2006. – Вип.2(13). – С.7 – 11.

8. Корчагин С. Информационное обеспечение военной политики ФРГ / С. Корчагин // Зарубежное военное образование. – 2008. – №12. – С.14 – 22. – [Електронний ресурс]. – Режим доступу: http://factmil.com/publ/strana/germanija/informacionnoe_obespechenie_voennoj_politiki_frg_2008/41-1-0-592.

9. Gesetz über die Errichtung des Bundesamtes für Sicherheit in der Informationstechnik (BSI-Errichtungsgesetz) vom 01.01.1991 [Електронний ресурс] // Офіційний сайт Федерального відомства безпеки інформаційних систем ФРН. – Режим доступу : https://www.bsi.bund.de.

10. Чернухін І.О. Досвід Федеративної Республіки Німеччини в побудові системи захисту інфраструктури від кібернетичних загроз / І.О. Чернухін // Information Security of the Person, Society and State. – 2014. – №1(14). – С.27 – 43.

11. Хабаров С. Министерство обороны Германии: функции и структура / С. Хабаров // Зарубежное военное образование. – 2018. – №2. – С.22 – 30. – [Електронний ресурс]. – Режим доступу: http://factmil.com/publ/strana/germanija/ministerstvo_oborony_germanii_funkcii_i_struktura_2018/41-1-0-1288.

12. Круглов Д. Силы кибероперацій и информационного обеспечения бундесвера / Д. Круглов // Зарубжное военное образование. – 2017. – №7. – С.23 – 25. – [Електронний ресурс]. – Режим доступу: http://factmil.com/publ/strana/germanija/sily_kiberoperacij_i_informacionnogo_obespechenija_bundesvera_2017/41-1-0-1191.