УДК 342.7
DOI https://doi.org/10.24144/2307-3322.2023.77.2.20

ІНФОРМАЦІЙНА БЕЗПЕКА В УМОВАХ ВОЄННОГО СТАНУ

Смотрич Д.В.,
доктор філософії,
старший викладач кафедри адміністративного та інформаційного права
Інституту права, психології та інноваційної освіти
НУ «Львівська політехніка»

Браілко Л.,
студент Інституту права, психології та інноваційної освіти
НУ «Львівська політехніка»

Смотрич Д.В., Браілко Л. Інформаційна безпека в умовах воєнного стану.

У сучасних військово-політичних реаліях важко і навіть недоречно заперечувати роль інформації як інструменту протистояння, фактично – зброї. Інформація дозволяє вигравати війни та політичні кризи без жодного пострілу, формуючи та розпалюючи внутрішні протиріччя. Така тактика характерна для війн нового формату – гібридних, де безпосередній військовий фактор є лише однією зі складових цілого.

Варто звернути увагу на те, що в умовах, коли цілий комплекс інформації розрахований на маніпулювання громадською думкою, свідомістю людини та подається за допомогою фізіологічних і психологічних методів і засобів її сприйняття, постає питання низького рівня інформаційної культури, що спричиняє зниження здатності людини до критичного сприйняття, стає важливим аналіз та оцінка отриманої інформації. У цьому випадку здатність до формування власної думки практично відсутня.

Цілком правильно вважати, що інформаційна безпека передбачає: належний рівень інформаційної культури, тобто теоретичну і практичну підготовку особистості, що забезпечує захист і реалізацію її життєво важливих інтересів і гармонійний розвиток в умовах інформаційного суспільства, незалежно від наявності інформаційних загроз; здатність держави створити умови для гармонійного розвитку та задоволення інформаційних потреб особи незалежно від наявності інформаційних загроз; забезпечення, розвиток і використання інформаційного середовища в інтересах особи; захист від різноманітних інформаційних загроз.

У статті розкриваються аспекти забезпечення інформаційних прав та свобод суспільства з врахуванням захисту інформаційної безпеки держави в умовах воєнного стану. Визначаються пріоритетні напрямки захисту інформаційної безпеки. Розглядаються типові загрози інформаційній безпеці та їх походження. Також, важливим є висновок про те, що забезпечення інформаційної безпеки полягає у створенні заходів щодо забезпечення інформаційної безпеки.

Ключові слова: безпека, інформаційна безпека, інформаційний захист, технічні загрози, внутрішні і зовнішні джерела загрози.

Smotrych D.V., Brailko L. Information security under martial law.

In modern military realities, it is difficult and even inappropriate to deny the role of information as a tool of confrontation, in fact - a weapon. Information allows you to win the war without firing a single shot, creating and fueling internal contradictions. Such tactics are characteristic of new format wars - hybrid wars, where the direct military factor is only one of the components of the whole.

It is worth paying attention to the fact that in conditions where a whole set of information is designed to manipulate public opinion, human consciousness and is presented with the help of physiological and psychological methods and means of its perception, the issue of a low level of information culture arises, which causes a decrease in a person's ability to critical perception , the analysis and evaluation of the received information becomes important. In this case, the ability to form one's own opinion is practically absent.

It is quite correct to believe that information security involves: an appropriate level of information culture, that is, theoretical and practical training of an individual, which ensures the protection and realization of his vital interests and harmonious development in the conditions of the information society, regardless of the presence of information threats; the ability of the state to create conditions for harmonious development and satisfaction of the informational needs of the individual, regardless of the presence of informational threats; provision, development and use of the information environment in the interests of the individual; protection against various informational threats.

The article reveals the aspects of ensuring information rights and freedoms, taking into account the protection of information security of the state in the conditions of martial law. Priority areas of protection are defined. Typical threats and their origins are considered. Also, it is important to conclude that ensuring information security consists in creating measures to ensure information security.

Key words: security, information security, information protection, technical threats, internal and external sources of threats.

Постановка питання. У сучасних військово-політичних реаліях важко і навіть недоречно заперечувати роль інформації як інструменту протистояння, фактично – зброї. Інформація дозволяє вигравати війни та політичні кризи без жодного пострілу, формуючи та розпалюючи внутрішні протиріччя. Така тактика характерна для війн нового формату – гібридних, де безпосередній військовий фактор є лише однією зі складових цілого.

Варто звернути увагу на те, що в умовах, коли цілий комплекс інформації розрахований на маніпулювання громадською думкою, свідомістю людини та подається за допомогою фізіологічних і психологічних методів і засобів її сприйняття, постає питання низького рівня інформаційної культури, що спричиняє зниження здатності людини до критичного сприйняття, стає важливим аналіз та оцінка отриманої інформації. У цьому випадку здатність до формування власної думки практично відсутня.

Саме тому, автори ставлять собі за **мету** дослідити окпемі особливості інформаційної безпеки в умовах воєнного стану.

Виклад основного матеріалу. Під воєнною безпекою держави розуміється реалізація життєво важливих національних інтересів держави у воєнній сфері для забезпечення захисту країни від воєнної загрози, збройної агресії та інших посягань із застосуванням військової сили [1, с. 254]. Тобто основною метою забезпечення воєнної безпеки України є попередження (недопущення) воєнних конфліктів, а рівень воєнної безпеки є критерієм ефективності реалізації воєнної політики держави.

Отже, можна стверджувати, що забезпечення оборони і безпеки неможливе без підтримання такого стану обороноздатності країни, який забезпечує запобігання військовим конфліктам і відсіч можливій збройній агресії, а також підвищення ступеня обороноздатності країни, глобальна та регіональна стабільність.

Гібридні способи ведення сучасних воєн роблять надзвичайно важливим забезпечення інформаційної безпеки Збройних сил України. На зміну війні гарячого типу, яка передбачає прямі військові зіткнення, приходить війна гібридного характеру, метою якої є розгортання громадянських воєн та створення керованого інформаційного хаосу на території противника. Для цього використовуються всі можливості – від хакерських атак на найважливіші системи життєзабезпечення держави до цілеспрямованої роботи засобів масової інформації.

Умови життя, в яких опинилася наша держава, змушують під іншим кутом розглядати питання національної безпеки. Якщо рік тому світ навколо нас здавався безпечним, то сьогодні виклики несуть у собі набагато більшу небезпеку, ніж у мирний час.

Ми є свідками того, як здійснюється інформаційний вплив, спрямований на людську свідомість суспільства. Об'єктом цього впливу є як окремі особи, групи осіб, так і цілі держави. Психологічний вплив здійснюється за допомогою засобів масової інформації, а основою використання такого впливу є легкість сприйняття і поверховість. Створення масових інформаційних атак, ботів, фейків, як свідчать сучасні реалії, є ефективними інструментами дезорієнтації суспільства, залякування, маніпулювання та паніки. Спеціально створені інформаційні ресурси привчають людину бездумно сприймати інформацію і вірити в неї [2, с. 290].

Питання інформаційної безпеки та культури в умовах війни є питанням виживання людини, суспільства та держави. Адже забезпечення інформаційної безпеки визначається не тільки інтересами держави, а й інтересами особи в контексті забезпечення її прав і свобод. Основою сучасної інформаційної безпеки є цілісність даних, доступність інформації, конфіденційність і надійність її збереження.

Інформаційна безпека включає не лише нормативно-політичну складову, а й інституційну сферу, яка передбачає діяльність органів, що її забезпечують, а також використання програмно-технічних засобів.

З метою забезпечення інформаційної безпеки в Україні Указом Президента України від 25.02.2017 р. була затверджена «Доктрина інформаційної безпеки України» [3]. В сучасних умовах війни 18 березня 2022 року прийнято рішення РНБО «Щодо реалізації єдиної інформаційної політики в умовах воєнного стану», в якому визначено, що в умовах воєнного стану реалізація єдиної інформаційної політика є пріоритетним питанням національної безпеки» [4]. Наразі в Україні також діє Центр протидії дезінформації при РНБО України, на сайті якого можна ознайомитися з актуальною інформацією та подіями у цій сфері.

Створення глобального простору суттєво посилило загрози застосування інформаційних заходів стратегічним противником або глобальним тероризмом, як з боку розгортання окремих військово-політичних операцій, так і з боку розвитку його стратегічного потенціалу в цілому.

Захист від загроз подібного характеру необхідний самим Збройним Силам та їх особовому складу, з якими в першу чергу застосовуються засоби гібридної війни.

Зростає цінність інформації. Ступінь її захищеності від злочинних посягань стає все вищим, а можливості для її отримання - збільшуються. Уміння правильно управляти інформаційними масивами та їх використання стає найважливішим завданням, яке стоїть перед військовослужбовцями.

Інформаційна безпека збройних сил як найважливішого державного інституту є запорукою безпеки самої держави. Захист військових інформаційних ресурсів має стати пріоритетним завданням фахівців з безпеки. Щоб якнайкраще нейтралізувати загрози, першочергово їх необхідно ідентифікувати та класифікувати за походженням, характером впливу, ступенем небезпеки. Експерти поділяють види джерел загроз на дві групи: внутрішні; зовнішні.

Іноді в одному явищі можна виявити зовнішні та внутрішні джерела загроз. Це може статися, коли спрямована дія, що походить ззовні, транслюється через операторів, розташованих у країні. Сьогодні такі підрозділи мають у своєму розпорядженні новітні електронні засоби поширення інформаційних потоків.

Одним із основних джерел інформаційних загроз також є напруженість або дестабілізація суспільно-політичної обстановки в місцях дислокації Збройних Сил. Створення штучно нагрітої атмосфери, провокування кадрових конфліктів з місцевим населенням, іноді навіть масових заворушень, викликаних цілеспрямованим інформаційним впливом, стають серйозними загрозами для стабільності обстановки у військовій частині та у військах загалом. Протистояти їм можна лише проводячи цілеспрямовану психолого-просвітницьку роботу з особовим складом, паралельно контактуючи з регіональною владою з метою недопущення провокаційної роботи засобів масової інформації та інших джерел поширення інформаційних атак.

Важливою загрозою є спрямований вплив на моральний стан військ шляхом фальсифікації фактів військової історії, посилення соціальної напруги, спроб втягнути особовий склад у розгортання політичних конфліктів. Виконавцями таких погроз інформаційного характеру найчастіше виступають засоби масової інформації, спрямовані на створення напруженої ситуації. У ряді випадків навіть контакт особового складу з представниками преси може стати способом спеціальної обробки поданої ними інформації, що призведе до можливої втрати бойового духу особового складу.

Іноді заходами такого впливу досягаються не тільки психологічні зриви, що призводять до військових злочинів чи дезертирства, а й створення у військах угруповань, спрямованих на свідомий підрив обороноздатності країни. Поширення радикального ісламізму може стати серйозною загрозою інформаційній безпеці армії. Військовослужбовець, який пройшов спеціальну психологічну терапію, вважає себе вже не військовослужбовцем, а релігійною громадою, виконує радше вказівки наставників, ніж накази командування. Такий боєць стає серйозною загрозою для інформаційної безпеки військових частин, особливо розташованих у регіонах з переважно мусульманським населенням [5, с. 70].

Технічні загрози інформаційного характеру стосуються як функціонування інформаційних систем, що використовуються у військах, у тому числі систем управління, так і збереження конфіденційної інформації, що передається військовими каналами зв'язку. Види технічних загроз діяльності Збройних Сил можуть бути різного характеру: від умисного пошкодження систем і крадіжки інформації до недбалості окремих співробітників. Заходи захисту в цьому випадку передбачатимуть підвищення рівня безпеки автоматизованих систем управління та навчання персоналу необхідним вимогам захисту інформації. Стандарти безпеки визначаються ГОСТами та іншими методиками, розробленими та

затвердженими на державному рівні, але часто на практиці відбувається зволікання з впровадженням нових програмно-технічних засобів, здатних протистояти загрозам з боку противника. Така затримка зумовлена особливостями функціонування системи державних закупівель і як така стає загрозою безпеці.

У рамках цього виду атаки можна розглядати навмисне пошкодження техніки і ліній зв'язку, що іноді відбувається з вини особового складу, місцевого населення, а також в результаті цілеспрямованої діяльності противника. Порушення систем життєзабезпечення військового корабля, викликане недбалістю або спланованими атаками, може призвести до загибелі екіпажу. Контроль за збереженням військової техніки – одне з найважливіших завдань, яке стоїть перед відповідальними військовослужбовцями. Особливо серйозними можуть бути проблеми з інформаційними системами космічних сил або ядерних установок. Порушення систем управління космічними кораблями через неефективний код, вбудований в програмний продукт, часто призводить не тільки до фінансових втрат, а й до порушення цілісності системи безпеки країни.

Надзвичайно важливою стає загроза внесення неправдивої інформації в систему відстеження можливої атаки. Зберігається ризик спрацьовування систем ППО через неправдиву інформацію, надіслану противником навмисно. Уявні загрози в минулому мало не призводили до початку ядерної війни, зараз цей ризик зменшився, але він залишився.

Серйозною проблемою сьогодні є недостатня розвиненість законодавчої бази щодо захисту інформації та протидії новим загрозам. Значна кількість явищ інформаційного простору досі не класифікована та не відображена в нормативних актах, що ускладнює застосування заходів відповідальності за вчинення будь-яких дій чи організацію діяльності, яка може завдати шкоди інформаційній безпеці Збройних Сил та безпосередньо військовослужбовцям. Але ці напрямки розвиваються, приймаються нормативно-правові акти, які законодавчо регулюють допустимість використання в техніці, що постачається у війська, тих чи інших технологій іноземного виробництва.

З моменту оголошення воєнного стану в Україні прийнято зміни до нормативно-правових актів з урахуванням реалій війни. Вони стосуються регулювання окремих аспектів інформації, правовідносин щодо заборони розповсюдження певної інформації з урахуванням її суспільно небезпечного характеру; врегулювання важливих моментів щодо технічного запису інформації в умовах воєнного стану; встановлення або посилення відповідальності за поширення певної інформації; регламентація процесуальних дій щодо отримання інформації.

Так, Верховна Рада прийняла законопроект про кримінальну відповідальність за незаконну фото- та відеофіксацію пересування Збройних Сил та міжнародної військової допомоги під час воєнного стану.

22 березня 2022 року набув чинності Закон України, який спрощує проведення слідчих дій та тимчасовий доступ до речей і документів, слідчий може фіксувати комп'ютерні дані на місці обшуку, навіть якщо про це не вказано в дозволі: зміни до Кримінально-процесуального кодексу [6] .

Посилено кримінальну відповідальність за виготовлення та розповсюдження забороненої інформаційної продукції відповідно до Закону України «Про внесення змін до деяких законодавчих актів України» від 3 березня 2022 року № 2110-IX

Закони України щодо посилення кримінальної відповідальності за виготовлення та розповсюдження забороненої інформаційної продукції.

До зовнішніх джерел загроз слід віднести ті, які знаходяться за межами території України чи її союзників. Цей вид загроз різноманітний, противник розробляє та регулярно використовує нові інформаційно-психологічні заходи для особового складу. При цьому застосування нових видів інформаційної зброї, частина з яких спрямована на виведення з ладу інформаційних систем, а частина – на прямий психологічний вплив на особовий склад, стає цілком реальною загрозою. При цьому механізм дії такої зброї, на думку аналітиків, заснований на використанні ультразвуку, електромагнітних полів, мікрохвиль різної природи. Не виключено застосування медичних та хімічних засобів, які допоможуть зорієнтувати поведінку військовослужбовців у мирний час та бойову обстановку. Такі засоби проведення психологічних операцій можуть бути застосовані в тих місцях, де в поточних конфліктах беруть участь збройні сили України. У пресі згадується велика кількість видів психологічної зброї, але офіційних підтверджень її використання поки немає [7, с. 63].

Ні для кого не секрет, що у збройних силах стратегічного супротивника чи організацій глобального тероризму є спеціальні підрозділи інформаційно-психологічного впливу. Їх діяльність вивчається лише на рівні профільних науково-дослідних інститутів, а заходи боротьби з новими загрозами розробляються та активно впроваджуються в практику.

Часто застосування цілеспрямованого інформаційного впливу заздалегідь ретельно готується роботою засобів. Військовослужбовці зобов'язані вміти класифікувати та ідентифікувати такі загрози, для чого необхідно провести відповідну підготовку.

Найбільш серйозною проблемою безпеки є соціальні мережі, за допомогою яких військовослужбовці можуть випадково оприлюднити важливу інформацію. Одним із основних завдань захисту безпеки держави має стати виявлення таких загроз та їх своєчасне усунення.

Заходи, які можуть бути застосовані для захисту інформації та забезпечення безпеки, також поділяються на дві групи: [8, с.117]

– захист інформаційних систем від пошкодження та інформації від витоку та перехоплення;

– захист психіки особового складу від цілеспрямованого інформаційно-психологічного впливу.

Ці заходи мають здійснюватися комплексно, на основі нових наукових розробок і програмних продуктів.

Перша група заходів:

– захист об'єктів військової дислокації та розташованої в них комп'ютерної техніки від пошкодження вогнем або іншого навмисного виведення з ладу;

– захист систем від віддаленого вторгнення зловмисника, зокрема з установкою програмних продуктів, що забезпечують повний захист периметра від вторгнень, наприклад, системи DLP та системи SIEM;

– захист інформації, яка становить державну або військову таємницю, від витоку чи умисного розкрадання;

– радіоелектронний захист;

– використання захищених моделей комп'ютерів і програмного забезпечення, які не можуть бути пошкоджені заздалегідь створеними проблемами в їх кодах;

– розробка засобів електронної розвідки;

– використання соціальних мереж для свідомої дезінформації противника;

– захист систем зв'язку.

Друга група заходів включає:

– запобігання навмисного психологічного впливу на психіку військовослужбовців;

– корекція інформації, що транслюється потенційним супротивником.

Розробка та впровадження комплексу цих заходів потребує створення окремих підрозділів, що працюють у сфері інформаційної безпеки.

Морально-психологічне забезпечення військ передбачає застосування комплексу заходів блокування, які застосовуються під час гібридної війни. Сьогодні існують інститути і аналітичні центри, які спрямували всі свої зусилля на розробку різноманітних методик морально-психологічного стану військ. У рамках цих досліджень вивчаються психологія, безпека психоенергетичної діяльності.

Для протидії спрямованому інформаційно-психологічному впливу командування Збройних Сил передбачає такі методи:

– проведення досліджень методів, спрямованих на психіку;

– використання всіх доступних видів психологічної роботи з військовослужбовцями,

здійснення цілеспрямованих захисних заходів.

Усі ці заходи необхідні для створення стійкого захисту від інформаційного впливу та готовності військовослужбовця до відсікання інформації, яка має ознаки спрямованого впливу з метою дестабілізації його морально-психологічного стану. Напад противника не повинен бути причиною зниження боєздатності військ, їх мотивації, пригнічення волі. Важливим буде проведення виховної роботи та організація дозвілля військовослужбовців.

Особливо важливо контролювати тих військовослужбовців, до сфери відповідальності яких входить робота із засобами зв'язку, автоматизованими системами управління та передачі інформації. Вони, швидше за все, стануть об'єктами розробки ворогом.

Передбачаючи, який саме комплекс заходів застосує потенційний супротивник, необхідно за допомогою засобів атаки перекрити його можливості. Такі дії, як:

– навмисне введення супротивника в оману щодо намічених заходів і способів протидії загрозам інформаційній безпеці;

– руйнування засобів зв'язку та інформаційних систем;

– внесення свідомих спотворень у роботу інформаційних систем противника;

– виявлення опорних пунктів противника, що діють на території України, та їх знищення;

– отримання конфіденційної інформації про наміри противника знизити рівень безпеки військ і використання цієї інформації для формування стратегії оборони;

– застосування засобів морально-психологічного придушення інформаційних сил противника

Розробка інформаційної зброї розглядається як окремий напрям оборонної стратегії. Він повинен бути розроблений не тільки для відображення загроз, а й для їх передбачення. Противник досить ефективно використовує інформаційну зброю, що можна побачити на прикладі країн, які беруть участь у військових конфліктах. Зброя використовується не лише в зонах бойових дій, а й у тих регіонах, які мають стати осередками дестабілізації. Подібна вітчизняна зброя повинна демонструвати такий самий і більш високий рівень ефективності.

Практично кожен військовий об'єкт зараз знаходиться в зоні можливого ураження, тому до захисту його безпеки необхідно підходити комплексно. Держава неухильно займається вирішенням цих завдань і нарощує свій оборонний потенціал. Розробка пропрієтарного програмного забезпечення допомагає уникнути системних ризиків.

Також власні канали передачі даних в мережі Інтернет повинні забезпечувати можливість спілкування без порушення архітектури Всесвітньої мережі.

Тому і на цих етапах має бути створена цілковита безпека для користувачів. Відсутність належного нагляду за постачальниками та підрядниками призводить до того, що військам постачається обладнання, яке забезпечує віддалений доступ потенційного супротивника. У деяких випадках використання таких пристроїв заборонено законом, але ще не все технічне оснащення армії модернізовано.

Серйозна вразливість систем автоматизованої системи управління армії також виникає через передачу інформації закритого характеру відкритими лініями зв'язку, що іноді дозволяють собі цивільні фахівці. Цю загрозу необхідно локалізувати якомога швидше.

Відповідно до Закону України «Про національну безпеку України» загрози національній безпеці України - це явища, тенденції та фактори, які унеможливлюють або утруднюють або можуть унеможливити чи утруднити реалізацію національних інтересів і збереження національної цінності України [9].

Висновки. Незаперечним є той факт, що сучасні загрози інформаційній безпеці є викликом далеко за межі нашої держави та посягають не лише на національний простір, а й мають важкі глобальні наслідки. З огляду на це, для запобігання та протидії сучасним інформаційним загрозам необхідно не лише прийняти нормативно-правову базу, а й забезпечити функціонування інституційного механізму забезпечення інформаційної безпеки, в тому числі освітньої складової. Йдеться про послідовну системну діяльність державно-правових інституцій, які б ефективно реалізовували національні інтереси в інформаційній сфері, були б здатні не лише вчасно реагувати на поширення інформаційних фейків та неправдивої інформації, а й були б здатні загалом попереджати інформаційні конфлікти та формувати інформаційну культуру суспільства в цілому. Крім того, враховуючи існуючі глобальні загрози та виклики, видається можливим ефективна протидія інформаційній агресії шляхом залучення до цього процесу міжнародних організацій, інституцій та міжнародної спільноти. Адже, як свідчать реалії сьогодення, у веденні війни в інформаційному полі немає кордону.

Список використаних джерел:

1. Остроухов В.В., Петрик В.М., Присяжнюк М.М. та ін. Інформаційна безпека (соціально-правові аспекти): підручник. К.: КНТ, 2010. 776 с.
2. Лизанчук В.В. Інформаційна безпека України: теорія і практика: підручник. Львів: ЛНУ ім. Івана Франка, 2017. 725 с
3. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України»: Указ Президента України від 25 лютого 2017 року № 47/2017 URL: https://zakon.rada.gov.ua/go/47/2017.
4. Про рішення Ради національної безпеки і оборони України від 18 березня 2022 року «Щодо реалізації єдиної інформаційної політики в умовах воєнного стану»: Указ Президента України від 19 березня 2022 року № 152/2022 URL: https://zakon.rada.gov.ua/go/152/2022.
5. Боднар І. Інформаційна безпека як основа національної безпеки. *Механізм регулювання економіки.* 2014. № 1. С. 68–75.
6. Про внесення змін до деяких законодавчих актів України щодо посилення кримінальної відповідальності за виготовлення та поширення забороненої інформаційної продукції. Закон України. URL: https://zakon.rada.gov.ua/ laws/show/2110-20#Text.

7. Кавун С.В., Носов В.В., Манжай О.В. Інформаційна безпека. Навчальний посібник. Ч. 2. Харків: Вид. ХНЕУ, 2018. 196 с.
8. Інформаційна безпека. Підручник. Під ред. В.В. Остроухова. К.: Видавництво Ліра-К, 2021. 412 с
9. Стратегія інформаційної безпеки. URL: https://zakon.rada.gov.ua/laws/show/685/2021#n14.