Olha Zolotar

System prawnej ochrony bezpieczeństwa informacyjnego Ukrainy

Legal system of information security in Ukraine

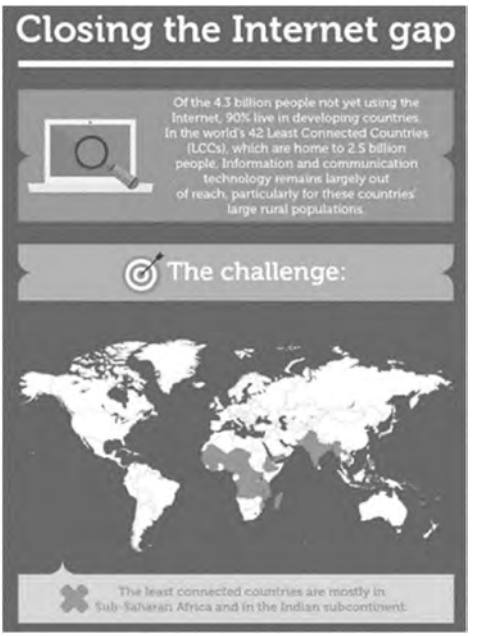
Streszczenie: Artykuł koncentruje się na prawnej ochronie bezpieczeństwa informacji Ukrainy. Poddaje się analizie teoretyczne i prawne podejście do zrozumienia bezpieczeństwa informacji i jego związku z bezpieczeństwem informacyjnym. Określa okresy regulacji prawnych w zakresie relacji informacyjnych i bezpieczeństwa informacji. Szczególną uwagę poświęca ostatnim okresom i dokumentom przyjętym po 2014 r. Analizie poddano zalety i wady doktryny bezpieczeństwa informacji Ukrainy 2017. Określono status i przyszłe sposoby odpowiednich regulacji prawnych.

Słowa kluczowe: bezpieczeństwo informacyjne, Ukraina

Summary: The article focuses on the legal protection of information security of Ukraine. Theoretical and legal approaches to the understanding of information security and its relation to cyber security are analyzed. There are determined periods of legal regulation in sphere of information relations and information security. Special attention is devoted to the last period and the documents adopted after 2014. The advantages and disadvantages of the Doctrine of Information Security of Ukraine 2017 are analyzed. The status and future ways of relevant legal regulation are outlined.

Keywords: information security, Ukraine

Zdecydowana większość naukowych prac na temat bezpieczeństwa informacyjnego zaczyna się od uzasadnień aktualności, które spowodowane są opanowaniem informacyjnymi technologiami wszystkich sfer życia społeczeństwa, a także kształtowaniem się informacyjnego społeczeństwa jako nowego etapu rozwoju społecznego. Problem bezpieczeństwa informacyjnego nabywa nowego znaczenia i stanowi przedmiot regulacji prawnych, jest jednym z głównych kierunków gwarantowania bezpieczeństwa narodowego i bezpieczeństwa państw, a także przesłanką szacunku praw i wolności człowieka i obywatela. Zatem fenomen informacyjnego bezpieczeństwa rozpatruje się przez pryzmat praktycznego stosunku człowieka do państwa i społeczeństwa, zwracając uwagę na potrzeby i interesy podmiotów i przedmiotów bezpieczeństwa. Niewątpliwie, uświadomione bezpieczeństwo zdolne jest wywierać decydujący wpływ na treść i rozwój procesów społecznych. To właśnie decyduje o aktualności badań bezpieczeństwa informacyjnego jako kategorii naukowej i zjawiska społecznego.



Rys. 1. INFOGRAPHIC: Closing the Internet gap[1]

[1] Pobrano: 15 kwietnia 2015, źródło: http://www.euractiv.com/sections/development-policy/infographic-closing-internet-gap-310492

Rozwój nauki o bezpieczeństwie, w kierunku bezpieczeństwa informacyjnego, w dużej mierze zależy od postrzegania przez poszczególne społeczeństwa oraz państwa różnych aspektów eksplozji informacyjnej. Po pierwsze, poziom rozwoju i wykorzystania IKT w świecie jest bardzo zróżnicowany – na przyklad, dostęp do Internetu ma 40% mieszkanców Ziemi. (Rys. 1).

Problemy informacyjne 60% ludzkości są na zupełnie innym poziomie. Jednak nie znaczy to, że ich nie ma. Człowiek od zawsze jest „skazany" na zdobywanie, ocenę oraz ochronę informacji (różni się tylko jej treść – od informacji o miejscu zdatnym do polowania, o źródle wody, o obcym plemieniu, aż do tajemnicy przedsiębiorstwa czy danych osobowych). Na tym polega działalność informacyjna, z którą ściśle jest związane bezpieczeństwo informacyjne. Jednak w warunkach IS znaczenie ostatniego gwałtownie wzrasta.[2]

O aktualności bezpieczeństwa informacyjnego na Ukrainie świadczy poziom naukowych opracowań i zainteresowanie naukowców z różnych dziedzin: prawników, politologów, filozofów, socjologów, historyków i nie tylko, co znalazło odzwierciedlenie w pracach: O. Baranowa, K. Beliakowa, O. Dzjobania, O. Dowgania, R. Kaliużnogo, W. Kormicza, W. Łipkana, A. Maruszczaka, J. Maksimenko, J. Malika, A. Nowickiego, O. Olijnika, W. Ostrouchowa, W. Pilipczuka, W. Cimbaliuka, W. Furaszewa itd.

Celem artykułu jest analiza prawnego systemu zapewnienia bezpieczeństwa informacyjnego Ukrainy jako nagłej konieczności w warunkach wojny hybrydowej, ujawnienie luk i zarysowywanie perspektyw dalszego rozwoju.

Stan prawnej ochrony bezpieczeństwa informacyjnego Ukrainy określa się stopniem regulacji społecznych stosunków w obrębie przeciwstawiania się zagrożeniom jej narodowym interesom w zakresie

[2] Zolotar O.O. *Pravova okhorona yak skladova informatsiynoyi bezpeky*: monohrafiya / O.O.Zolotar. - K.: TOV «PanTot». – 2011. – 100 s., Zolotar O.O. *Geneza okhorony i zakhystu informatsiyi v Ukrayini: istoryko-pravovyy aspekt* / O.O. Zolotar //*Derzhavna polityka tsyvil'noyi aviatsiyi KhKhI st.: ekonomichni i stratehichni mozhlyvosti Ukrayiny:* Materialy naukovo-praktychnoyi konferentsiyi, Kyyiv, 19-20 lyutoho 2009 r. – K.: Vyd-vo Yevrop. Un-tu, 2009. – S. 118-129.

informacyjnym przez ustawodawstwo krajowe, normy prawa międzynarodowego oraz umowy międzynarodowe[3].

Szczególnym aspektem, na który warto zwrócić uwagę w analizie problematyki bezpieczeństwa informacyjnego, jest sytuacja polityczna oraz geopolityczna. Krzysztof Liderman, charakteryzując badania na temat bezpieczeństwa informacyjnego w Polsce, wspomina, że „choć coraz więcej decydentów dostrzega znaczenie bezpieczeństwa informacyjnego, a przynajmniej używa tego pojęcia i deklaruje działania mające na celu jego zapewnienie, w rzeczywistości sprawa nie wygląda tak dobrze".[4] Pogląd ten wywodzi się z tego, że w naukach o bezpieczeństwie nie dostrzega się potrzeby włączenia zagadnień bezpieczeństwa informacyjnego[5].

Inaczej sytacja wygląda na Ukrainie. Przez ostatnie 20 lat zagadnienia bezpieczeństwa informacyjnego stale znajdują się w centrum uwagi naukowców, ustawodawców i praktyków. Analiza kształtowania się ustawodawstwa w zakresie informacyjnym ogólnie i ds. informacyjnego bezpieczeństwa w szczególności pozwala wyciągać pewne wnioski. Informacyjne ustawodawstwo i ustawodawstwo ds. informacyjnego bezpieczeństwa jest stosunkowo nową gałęzią ustawodawstwa Ukrainy i wciąż znajduje się na etapie kształtowania się. Można wyodrębnić następne etapy jego powstania:

I. 1992-1996 – kształtowanie się podstaw informacyjnego ustawodawstwa;
II. 1996-2003 – uświadomienie i formułowanie podstaw informacyjnego bezpieczeństwa jako elementu bezpieczeństwa narodowego;
III. 2003-2014 – uświadomienie rozwoju globalnego społeczeństwa informacyjnego, dołączenie do międzynarodowych aktów w zakresie społeczeństwa informacyjnego, prawa i bezpieczeństwa, rozwój krajowego ustawodawstwa według tendencji międzynarodowego prawa. Przy czym, naszym zdaniem, w latach 2010-2014

[3] Kalyuzhnyy R.A., Bayev O.O., *Normatyvno-pravove zabezpechennya informatsiynoyi bezpeky Ukrayiny. Pravova informatyka*, # 4(24) / 2009, s. 5-11.

[4] Wiecej: Liderman, K. „Bezpieczeństwo informacyjne". Warszawa, PWN, 2012, s. 12.

[5] Może to być w pewien sposób wytłumaczone przynależnością Polski do NATO, w ramach odrębnych państw - członków trwają badania w zakresie bezpieczeństwa informacyjnego już od drugiej połowy XX wieku.

miał miejsce kryzys w sferze bezpieczeństwa informacyjnego, uwarunkowany nieuzasadnioną polityką informacyjną państwa;

IV. 2014 - dotychczas – rozwój ustawodawstwa w sferze bezpieczeństwa informacyjnego, ukierunkowany na wzmacnianie pozycji Ukrainy w przeciwstawianiu się hybrydowym atakom ze strony Federacji Rosyjskiej.

Artykuł 17 Konstytucji Ukrainy z 1996 roku określa zapewnienie bezpieczeństwa informacyjnego jako jedną z najważniejszych funkcji państwa, jako sprawę Narodu Ukrainy. Zgodnie z ustawodawstwem Ukrainy termin „bezpieczeństwo informacyjne" ma następującą definicję: „stan zabezpieczenia niezbędnych interesów człowieka, społeczeństwa i państwa, w którym zapobiega się wyrządzeniu szkody poprzez: niekompletność, nieterminowość i zawodność wykorzystywanej informacji; negatywny wpływ informacyjny; negatywne skutki technologii informacyjnych, nieupoważnione rozpowszechnienie, użytkowanie, naruszenie integralności, poufności i dostępności informacji"[6].

Zgodnie z tą definicją, wyróżniono trzy poziomy bezpieczeństwa informacyjnego: jednostki (człowieka), społeczeństwa, państwa. Bezpieczeństwo informacyjne na poziomie państwowym koncentruje się na informacyjno-analitycznym wsparciu dla instytucji państwowych, informacyjnej polityce wewnętrznej i zagranicznej na poziomie międzynarodowym, systemie ochrony informacji niejawnych, przeciwdziałaniu przestępstwom w sektorze informacyjnym. Poziom społeczny obejmuje tworzenie informacyjno-analitycznej przestrzeni wysokiej jakości, pluralizmu kanałów komunikacji i źródeł informacji, w tym potężnych niezależnych mediów. Informacyjne bezpieczeństwo jednostki (człowieka) jako kategoria prawna pozostaje najmniej zbadane.

Jeszcze pod koniec ubiegłego tysiąclecia, ukraińscy naukowcy ostrzegali przed niebezpieczeństwem wojen informacyjnych[7]. Niestety, ze względu na czynniki polityczne i gospodarcze, na Ukrainie nauka nie

[6] *Pro Osnovni zasady rozvytku informatsiynoho suspil'stva v Ukrayini na 2007-2015 roky*: Zakon Ukrayiny vid 09.01.2007 # 537-V // Vidomosti Verkhovnoyi Rady Ukrayiny. – 2007. – # 12. – St. 102.

[7] I. Zima, *Informatsiyna viyna ta informatsiyna bezpeka: ohlyad dumok zarubizhnykh politolohiv ta voyennykh spetsialistiv* / I.I. Zima, I.M. Nikolayev // „Nauka i oborona". – 1998. – # 1. – S. 56-58.

ma znaczącego wpływu na państwowe i społeczne realia. Wydarzenia z ostatnich lat wskazują na dobrze przemyślaną strategię prowadzenia wojny informacyjnej przez Rosję przeciwko Ukrainie, którą rozpoczęto co najmniej dekadę wcześniej niż stała się ona wyraźnie zauważalna[8].

Uważamy za potrzebne zatrzymać się dokładniej na ostatnim etapie. Decyzją Rady Narodowego Bezpieczeństwa i Obrony Ukrainy (RNBO) z 28 kwietnia 2014 roku «O przedsięwzięciach co do doskonalenia, kształtowania i realizacji państwowej polityki w sferze informacyjnego bezpieczeństwa Ukrainy», uruchomioną Dekretem Prezydenta 449/2014 z 01.05.2014, odwołana została Doktryna bezpieczeństwa informacyjnego Ukrainy, która obowiązywała od 2009 roku. Przewidziano w niej także opracowanie szeregu prawodawczych aktów, w szczególności, Strategię rozwoju informacyjnego obszaru Ukrainy, Strategię cybernetycznego bezpieczeństwa Ukrainy, projekt Ustawy o cybernetycznym bezpieczeństwie Ukrainy. Z planowanych dokumentów, opracowana i uruchomiona Dekretem Prezydenta Ukrainy z 15 marca 2016 roku 96/2016 została tylko Strategia cybernetycznego bezpieczeństwa Ukrainy.

Celem strategii cyberbezpieczeństwa Ukrainy jest tworzenie warunków dla bezpiecznego funkcjonowania cyberprzestrzeni, jej stosowanie na rzecz osób fizycznych, społeczeństwa i państwa. Również w Strategii wskazane zostały zagrożenia cyberbezpieczeństwa, krajowy system bezpieczeństwa cybernetycznego, przedmioty zapewnienia bezpieczeństwa cybernetycznego, priorytety i kierunki zapewnienia cyberbezpieczeństwa Ukrainy.

Należy wskazać, że w związku z realizacją Strategii, RNBO podjęła decyzję o stworzeniu specjalnego nowego organu – Narodowe Koordynacyjne Centrum Cyberbezpieczeństwa. Utworzenie takiego centrum, naszym zdaniem, jest uzasadnione, ponieważ pełnomocnictwa do zapewnienia bezpieczeństwa informacyjnego wyposażona została znaczna liczba agencji i instytucji państwowych, m.in. Narodowa Rada Ukrainy ds. Telewizji i Radiofonii, Państwowy Komitet Telewizji i Radia Ukrainy, Służba Bezpieczeństwa Ukrainy, Służba Zewnętrznego Wywiadu Ukrainy, Ministerstwo Obrony Ukrainy, MWS Ukrainy,

[8] Więcej na temat wojny informacyjnej w Ukrainie http://mip.gov.ua/content/informaciyna-viyna.html

MSZ Ukrainy, Ministerstwo Kultury Ukrainy i inne, co doprowadziło do dublowania się i braku działań koordynacyjnych.

W kontekście koordynacji funkcji zapewnienia bezpieczeństwa informacyjnego, warto skupić się na szczególnym statusie RNBO jako przedmiotu stosunków informacyjnych, ponieważ on jest jedynym organem, który ma pełnomocnictwo, funkcje i zadania dotyczące koordynacji i kontroli działań organów władzy wykonawczej w szczególności, centralnych organów władzy, organów ochrony porządku prawnego i organów samorządu lokalnego we wszystkich obszarach zapewnienia narodowego bezpieczeństwa i obrony.

Na podstawie wspomnianej Strategii Bezpieczeństwa Narodowego Ukrainy, Konstytucji, Ustaw Ukrainy oraz Umów międzynarodowych Ukrainy, Prezydent Ukrainy Dekretem z 25 lutego 2017 Nr 47 / 2017 zatwierdził Doktrynę Bezpieczeństwa Informacyjnego Ukrainy. Celem Doktryny jest określenie zasad kształtowania i realizacji polityki informacyjnej państwa, w szczególności w celu przeciwdziałania destrukcyjnemu wpływu informacyjnemu Federacji Rosyjskiej w zakresie wojny hybrydowej. Doktryna Bezpieczeństwa Informacyjnego Ukrainy określa interesy narodowe Ukrainy w sektorze informacyjnym, zagrożenia ich realizacji i priorytety polityki państwa w obszarze informacyjnym.

Jedną z nowych kategorii, wprowadzoną tym dokumentem jest „narracja strategiczna" – specjalnie przygotowany tekst, przeznaczony do prezentacji słownej w trakcie strategicznych komunikacji w celu informacyjnego wpływu na docelowe audytorium. Określono „wsparcie rozwoju mechanizmów samoregulacji środków masowego przekazu na zasadach socjalnej odpowiedzialności". Przedstawiciele organizacji obrony praw człowieka i mediów natychmiast zareagowali na to obawami nacisków na wolność słowa[9].

Trudno po tak krótkim czasie ocenić prawdopodobny wpływ tego dokumentu na ukraińską rzeczywistość obszaru informacyjnego. Przewiduje się, że głównymi przedmiotami uprawnień, zgodnie z nią, powinny być Rada Ministrów, Ministerstwo Polityki Informacyjnej, Ministerstwo Spraw Zagranicznych, Ministerstwo Kultury Ukrainy, Państwowa Agencja Ukrainy ds. Kina, Krajowa Rada Ukrainy ds.

[9] *Doktryna informatsiynoyi bezpeky Ukrayiny – tse lyshe deklaratsiya – eksperty* http://www.radiosvoboda.org/a/28336852.html

Telewizji i Radia, Państwowy Komitet Telewizji i Radiofonii Ukrainy, Służba Bezpieczeństwa Ukrainy, agencje wywiadowcze, Państwowa Służba Specjalna Komunikacji i Ochrony Informacji, Narodowy Instytut Badań Strategicznych; Rada Bezpieczeństwa Narodowego jako organ, który koordynuje działania władzy wykonawczej na rzecz bezpieczeństwa narodowego w obszarze informacyjnym. Znacząco zostały wzmocnione i określone uprawnienia Ministerstwa Polityki Informacyjnej.

Funkcjonowanie Doktryny, że dokument ten jest zdecydowanie jednostronny. „Stosowanie przez Federację Rosyjską technologii hybrydowej wojny przeciwko Ukrainie przekształciło obszar informacyjny w kluczową arenę konfrontacji. Właśnie przeciwko Ukrainie Federacja Rosyjska wykorzystuje najnowsze informacyjne technologie wpływu na świadomość obywateli, skierowane na rozpalanie narodowej i religijnej nienawiści, propagandę agresywnej wojny, zmianę konstytucyjnego ustroju drogą siły albo naruszenie suwerenności i terytorialnej integralności Ukrainy". A więc, dokument ten określa główne źródło zagrożenia, a mianowicie kierunek ruchu oporu. Niewątpliwie, jest to ważne ze względu na hybrydową wojnę przeciwko Ukrainie. Jednak, naszym zdaniem, takie «punktowe» dokumenty przy nieobecności kompleksowej prawnej regulacji zagadnień bezpieczeństwa informacyjnego są niewystarczające.

Warto wspomnieć, iż nadal ważna jest na Ukrainie ustawa „O podstawowych zasadach społeczeństwa informacyjnego na Ukrainie w latach 2007-2015", którą w styczniu 2007 roku uznano za jeden z priorytetów Ukrainy. Podkreślono znaczenie zbudowania zorientowanego na ludzi i otwartego na wszystkich, mającego na celu rozwój, społeczeństwa informacyjnego, gdzie każdy może tworzyć i gromadzić informacje i wiedzę, mieć swobodny dostęp do nich, korzystać i wymieniać się nimi, by dać możliwość każdemu człowiekowi w pełnej mierze zrealizować swój potencjał, sprzyjając społecznemu i osobistemu rozwojowi i podwyższając jakość życia[10].

W tej ustawie po raz pierwszy jest użyta definicja „bezpieczeństwo informacyjne jest to stan ochrony najbardziej istotnych interesów człowieka, społeczeństwa i państwa, przy który uniemożliwia szkody

[10] *Pro osnovni zasady rozvytku informatsiynoho suspil'stva v Ukrayini na 2007-2015 roky:* Zakon Ukrayiny // Uryadovy kuryer [Tekst]. – 2007. – 14 lyut.

przez: niekompletność, niestosowność i niewiarygodność informacji, co wiąże się z: negatywnym wpływem informacyjnym; negatywnymi skutkami stosowania informacyjnych technologii; niesankcjonowanym rozpowszechnianym, użytym i naruszeniem całości, poufności i dostępności informacji”[11].

Wynika z tego również, że rozwiązanie problemu bezpieczeństwa informacyjnego powinno następować przez: stworzenie funkcjonalnej infrastruktury informacyjnej państwa i ochrony krytycznych elementów; podwyższenie poziomu koordynacji działalności organów państwowych co do ujawnienia, oceny i przewidywania zagrożeń dla bezpieczeństwa informacyjnego, zapobieganie takim zagrożeniom i zabezpieczenie likwidacji ich skutków, międzynarodową współpracę w tych sprawach; polepszenie aktów normatywnych co do zabezpieczenia bezpieczeństwa informacyjnego, w szczególności ochrony informacyjnych zasobów, przeciwdziałania komputerowej przestępczości, obrony danych osobowych, a także działalności ochrony porządku prawnego w obszarze informacyjnym; wdrożenie i rozwój narodowego systemu związku poufnego jako nowoczesnej chronionej bazy transportowej, zdolnej zintegrować geograficznie rozproszone systemy informatyczne, które obsługują informacje poufne.

Spodziewano się, że realizacja podstawowych zasad rozwoju społeczeństwa informacyjnego na Ukrainie w latach 2007-2015 będzie stanowić pozytywną zmianę w życiu społeczeństwa i człowieka, a mianowicie: w celu zwiększenia poziomu ochrony praw człowieka i jego dobra, zwiększenie udziału społeczeństwa w rządzie, promowanie demokracji; w celu zwiększenia konkurencyjności, efektywności administracji publicznej, wydajności pracy we wszystkich sektorach gospodarki, poziomu bezpieczeństwa informacji osoby, społeczeństwa i państwa, stopnia rozwoju informacji i infrastruktury telekomunikacyjnej, w tym w ukraińskim segmencie Internetu; przejście od gospodarki do modelu innowacyjnego oraz rozwoju naukowego i technologicznego, w celu zwiększenia udziału produktów wysokiej technologii, promowanie jakości i dostępności edukacji, nauki, kultury, zdrowia poprzez IT; dawanie ludziom dostępu do krajowych i światowych zasobów informacji w formie elektronicznej; tworzenie miejsc pracy, polepszenie

[11] Ibid.

warunków pracy i życia; pogłębienie wdrażania ram regulacyjnych i prawnych społeczeństwa informacyjnego.

Jednak trudna sytuacja polityczna i gospodarcza, a także szereg innych czynników, takich jak: brak wyraźnego rozgraniczenia kompetencji władz publicznych i samorządów we wdrażaniu IT w systemie administracji publicznej oraz koordynowania działań w tym obszarze; niewystarczające zapewnienie dostępności usług administracyjnych wysokiej jakości dla wszystkich podmiotów społeczeństwa informacyjnego oraz gwarantowanie ich zgodności z przyjętymi wymogami państwowymi; niewystarczające uwzględnienie międzynarodowych doświadczeń w zakresie rozwoju społeczeństwa informacyjnego; rozpowszechniona praktyka delegowania kompetencji władzy państwowej, jej uprawnień dotyczących usług administracyjnych pod pretekstem niezbędności eksploatacji systemów informatycznych i kompleksów, co powoduje utratę kontroli nad kosztami administracyjnymi usług i nad opłatami na takie usługi itp. - doprowadziły do niewykonania na Ukrainie szeregu przepisów tej Ustawy i środków, zaplanowanych przez Radę Ministrów na jego realizację.

O niskim tempie rozwoju informacyjnego społeczeństwa świadczy również indeks sieciowej gotowości (Networked Readiness Index), który określa poziom rozwoju technologii informacyjno-komunikacyjnych na świecie. Składa się on z czterech subindeksów – warunki dla rozwoju IT; gotowość; stosowanie i wpływ, wprowadzane przez składniki (wskaźniki), które opisują rolę rządu, biznesu i społeczeństwa w kształtowaniu środowiska dla rozwoju IT. Według „Globalnego raportu rozwoju technologii informacyjnych – 2015" (The Global Information Technology Report), który od 2002 roku corocznie jest publikowany przez Światowe Forum Ekonomiczne (World Economic Forum), Ukraina w roku 2016 zajmowala 64 pozycję, a w 2015 – 71 pozycję wśród 143 krajów w rankingu w zakresie technologii informacyjnych i komunikacyjnych. Najwyższą pozycję przyznał Networked Readiness Index, kiedy przedstawił Ukrainę w 2009 roku (62 miejsce). Następnie, w ciągu kolejnych dwóch lat nasz kraj stracił 28 punktów, tak że w 2011 roku znalazł się na pozycji 90 wśród 138 krajów. W ostatnich latach, ze względu na rozszerzenie listy krajów uczestniczących w rankingu, Ukraina jest w siódmej dziesiątce i ustępuje dziesiątce państw WNP i Europy Wschodniej. Powodem jest dość niska pozycja Ukrainy

w światowych rankingach. W tym roku decydują elementy, które charakteryzują środowisko polityczne i regulacyjne – 122 i niskie wykorzystanie IT przez rząd – pozycja 124[12].

Na wszystkich wspomnianych etapach, miało miejsce podejście sytuacyjne do tworzenia przepisów prawnych w obszarze informacyjnym, co doprowadziło do do wielu problemów w zakresie regulacji prawnych stosunków informacyjnych.

Ilość ustaw w sektorze informacyjnym, niestety, nie przeradza się w jakość. Krasnostup G. zauważa, że „nie ma potrzeby tworzenia nowych przepisów, lecz trzeba systematyzować już istniejące, wyznaczając ich prawne hiperzwiązki w celu późniejszej ich kodyfikacji na poziomie Kodeksu Ukrainy o informacji[13]. Jednak obszar informacyjny rozwija się dzisiaj szybciej niż każdy inny. To przewiduje stałą konieczność regulacji nowych stosunków społecznych w tym obszarze.

Zatem odpowiednie prawne zabezpieczenie powstaje bezsystemowo i niekonsekwentnie, a więc nie jest zdolne wypełnić swoich funkcji i być skutecznym. Współczesny stan normatywno-prawnego zabezpieczenia bezpieczeństwa informacyjnego Ukrainy charakteryzuje się fragmentarycznym wyborem podmiotów prawnej regulacji, niedostatecznym uzgodnieniem norm prawnych i niskim poziomem koordynacji działalności przedmiotów prawodawczej inicjatywy rozwoju i polepszenia norm prawnych. W związku z tym nie jest w stanie adekwatnie do potrzeb rozwiązywać problemów, które powstają[14].

Znaczącymi wydają się wnioski, które proponuje Maksimenko J. dla polepszenia ukraińskiego ustawodawstwa informacyjnego przez jego kodyfikację. W szczególności, twierdzi, że na poziomie prawnym bezpieczeństwo informacyjne powinno rozpatrywać się w trzech aspektach: 1) jako bezpieczeństwo informacyjno-psychologiczne; 2) bezpieczeństwo informacyjne w zakresie praw i wolności; 3) bezpieczeństwo informacyjno-techniczne. Przy czym, regulacja

[12] http://edclub.com.ua/analityka/riven-rozvytku-informaciyno-komunikaciynyh-tehnologiy-v-ukrayini-ta-sviti

[13] H. Krasnostup, *Orhanizatsiyno-pravovi aspekty neobkhidnosti reformuvannya suchasnoho informatsiynoho zakonodavstva* / H. Krasnostup // „Pravo Ukrayiny". – 2005. – # 9. – s. 81-83, s. 82

[14] R.A. Kalyuzhnyy, O.O. Bayev, Normatyvno-pravove zabezpechennya informatsiynoyi bezpeky Ukrayiny. Pravova informatyka, # 4(24) / 2009, s. 5-11.

prawna bezpieczeństwa informacyjno-psychologicznego i bezpieczeństwa informacyjnego w zakresie praw i wolności de iure odpowiada międzynarodowym i europejskim standardom w tym zakresie, kiedy bezpieczeństwo informacyjno-techniczne jest uregulowane przeważnie podprawomocnymi aktami prawnymi i potrzebuje uzgodnienia ze standardami europejskimi[15].

Wadami czynnego ustawodawstwa bezpieczeństwa informacyjnego rozmycie się norm w licznych aktach prawnych różnej siły prawnej; nieuzgodnienie ich zarówno między sobą, jak też z obowiązującą Konstytucją; deklaratywność znacznej części norm bez wyznaczenia dróg ich realizacji, wskutek czego obserwuje się niski poziom realizacji norm prawa, co reguluje społeczne stosunki w zakresie zabezpieczenia bezpieczeństwa informacyjnego; a także obecność licznych blankietowych czy referencyjnych norm prawa, wielu abstrakcyjnych, subiektywnych pojęć, co potrzebuje oficjalnego tłumaczenia albo wyraźnego objaśnienia, a także nieobecność umocowania fundamentalnych, podstawowych definicji (np. bezpieczeństwa informacyjnego)[16].

Koniecznym jest opracowanie i przyjęcie dla prawnego zapewnienia bezpieczeństwa informacyjnego ustawy «O bezpieczeństwie informacyjnym». Przy czym, w ukraińskiej doktrynie jest dyskusyjnym pytanie o przeciwstawianie cyberbezpieczeństwa i bezpieczeństwa informacyjnego.

Na doktrynalnym poziomie wielokrotnie badano pytanie współzależności cyberbezpieczeństwa i bezpieczeństwa informacyjnego, cyberprzestrzeni i obszaru informacyjnego. Faktycznie, sformułowano dwa podejścia do tego pytania - cyberbezpieczeństwa jako oddzielnego kierunku,[17]

---

[15] Y. Maksymenko, *Teoretyko-pravovi zasady zabezpechennya informatsiynoyi bezpeky Ukrayiny*: dys. … kand. yuryd. nauk: 12.00.01 / Yu. Ye. Maksymenko. – K., 2007. – 186 s.

[16] Y.Maksymenko, *Teoretyko-pravovi zasady zabezpechennya informatsiynoyi bezpeky Ukrayiny*: dys. … kand. yuryd. nauk : 12.00.01 / Yu. Ye. Maksymenko. – K., 2007. – 186 s.

[17] V.L. Buryachok, *Informatsiyna ta kiberbezpeka: sotsiotekhnichnyy aspekt*: pidruchnyk / [V.L. Buryachok, V.B. Tolubko, V. O. Khoroshko, S.V. Tolyupa]; za zah. red. d-ra tekhn. nauk, profesora V.B. Tolubka. – K.: DUT, 2015. – 288 s., Lohinova N.I. *Analiz spivvidnoshennya informatsiynoyi ta kibernetychnoyi bezpeky* // I naukova Internet-konferentsiyi „Vykorystannya suchasnykh informatsiynykh tekhnolohiy v pidhotovtsi ta profesiyniy diyal'nosti pravoznavtsiv Natsional'noho universytetu

również cyberbezpieczeństwo jako składowa informacyjnego bezpieczeństwa,[18] która, według opinii autora, wydaje się bardziej uzasadniona.

Przez dłuższy czas przeciwstawianie cybernetycznego i informacyjnego bezpieczeństwa miało miejsce w europejskiej i amerykańskiej doktrynach polityczno-prawnych. Jednak, w analitycznym raporcie „Redefining Information Warfare Boundaries for anarmy in a Wireless World"[19] sporządzonym przez korporację „RAND" na zamówienie armii USA (sprawozdanie z 2013 roku, kod sprawozdania po projekcie - RAND10473) zaznaczono, że w praktycznej działalności organów wojskowego zarządzania, podmiotów zabezpieczenia informacyjnego bezpieczeństwa informacyjnego, środowisko koniecznie trzeba rozpatrywać w dwóch wymiarach: ludzkim i technicznym.

Rozpatrywanie informacyjnego obszaru i cyberprzestrzeni (więc informacyjnego bezpieczeństwa i cyberbezpieczeństwa) jako oddzielnych równoległych instytucji (kierunków działania) uznano jako bezpodstawne i sztuczne (czyli uznano jako metodologiczny błąd)[20]. Zatem pozycja, która wielokrotnie jest uzasadniana przez ukraińskich uczonych, że cyberprzestrzeń jest integralną częścią obszaru informacyjnego, a odpowiednio cyberbezpieczeństwa – składową informacyjnego bezpieczeństwo, zaczęła być rozpatrywana jako możliwa również na poziomie międzynarodowym. Jednak w naukowych badaniach i normatywnej regulacji wielu europejskich krajów wciąż figuruje pierwsze podejście, które przeciwstawia bezpieczeństwo informacyjne i cyberbezpieczeństwo.

Olijnyk O. uważa, że wymagania bezpieczeństwa informacyjnego powinny być organiczone do wszystkich poziomów ustawodawstwa, w tym prawa konstytucyjnego, podstawowych ustaw, przepisów co

«Odes'ka yurydychna akademiya»" http://conf.inf.od.ua/doklady-konferentsii/spisok-dokladov-iv-konferentsii-2016-g/106-loginova

[18] Ф V.M. Furashev, *Kiberprostir ta informatsiynyy prostir, kiberbezpeka ta informatsiyna bezpeka: sutnist', vyznachennya, vidminnosti* // /Informatsiya i pravo. - 2(5)/2012. http://ippi.org.ua/journal/85

[19] http://www.rand.org/content/dam/rand/pubs/monographs/MG1100/MG1113/RAND_MG1113.pdf

[20] T. Popova, *Shcho oznachaye «Doktryna informatsiynoyi bezpeky Ukrayiny»*? http://www.radiosvoboda.org/a/28337376.html

do organizacji państwowego systemu zarządzania, specjalnych ustaw, rozporządzeń itp.[21]

Analiza czynnego ukraińskiego ustawodawstwa i prac ojczystych i zagranicznych naukowcow pozwala wyciągnąć następujące wnioski. Różnorodność podejść do definicji bezpieczeństwa informacyjnego świadczy, że jest ono jedną z ważnych wieloaspektowych koncepcji w nauce i innych dziedzinach działalności człowieka. Istota i złożoność tej koncepcji jest również cechą współczesnego społeczeństwa informacyjnego. Analiza różnych podejść do określenia znaczenia bezpieczeństwa informacyjnego pozwala wywnioskować niecelowość ścisłego przestrzegania jednej pozycji. Najbardziej odpowiednim jest integralne podejście, zgodnie z którym bezpieczeństwo informacyjne jest określane za pomocą jego podstawowych cech, biorąc pod uwagę stałą dynamikę systemów informacyjnych i socjalnych. Doktryna prawnego zabezpieczenia bezpieczeństwa informacyjnego, naszym zdaniem, powinna odzwierciedlać złożoność tego obszaru, więc, jednoczyć zabezpieczenie prawnych interesów człowieka, społeczeństwa i państwa w obszarze informacyjnym; subiektywnych praw informacyjnych człowieka i obywatela; systemów organów i instytucji, odpowiedzialnych za zapewnienie informacyjnego bezpieczeństwa oraz zapewniać udział społeczeństwa obywatelskiego w tym procesie.

Bibliografia

Zolotar O.O. *Pravova okhorona yak skladova informatsiynoyi bezpeky: monohrafiya*., K.: TOV «PanTot», 2011, 100 s.

Zolotar O.O. *Geneza okhorony i zakhystu informatsiyi v Ukrayini: istoryko-pravovyy aspekt //Derzhavna polityka tsyvil'noyi aviatsiyi KhKhI st.: ekonomichni i stratehichni mozhlyvosti Ukrayiny:* Materialy naukovo-praktychnoyi konferentsiyi, Kyyiv, 19-20 lyutoho 2009 r., K.: Vyd-vo Yevrop. Un-tu, 2009, S. 118-129

Kalyuzhnyy R.A., Bayev O.O. „Normatyvno-pravove zabezpechennya informatsiynoyi bezpeky Ukrayiny. Pravova informatyka", # 4(24) / 2009, s. 5-11.

[21] Oliynyk O.V. *Normatyvno-pravove zabezpechennya informatsiynoyi bezpeky v Ukrayini.* // „Pravo i suspil'stvo" # 3 / 2012, 132-137, s. 137

Liderman, K. *Bezpieczeństwo informacyjne*. Warszawa, PWN, 2012, s. 12.

Pro Osnovni zasady rozvytku informatsiynoho suspil'stva v Ukrayini na 2007-2015 roky: Zakon Ukrayiny vid 09.01.2007 # 537-V // Vidomosti Verkhovnoyi Rady Ukrayiny, 2007, # 12, St. 102.

Zima I.I. *Informatsiyna viyna ta informatsiyna bezpeka: ohlyad dumok zarubizhnykh politolohiv ta voyennykh spetsialistiv* // „Nauka i oborona", 1998, # 1, ts. 56-58.

Pro osnovni zasady rozvytku informatsiynoho suspil'stva v Ukrayini na 2007-2015 roky: Zakon Ukrayiny // Uryadovyy kur"yer, 2007, 14 lyut.

Riven' rozvytku informatsiyno-komunikatsiynykh tekhnolohiy v Ukrayini ta sviti Pobrano: 23 marzets 2017, źródło: http://edtslub.tsom.ua/analityka/riven-rozvytku-informatsiyno-komunikatsiynyh-tehnologiy-v-ukrayini-ta-sviti

Krasnostup H. *Orhanizatsiyno-pravovi aspekty neobkhidnosti reformuvannya suchasnoho informatsiynoho zakonodavstva* / H. Krasnostup // „Pravo Ukrayiny", 2005, # 9, s. 81-83.

Maksymenko Yu. Ye. *Teoretyko-pravovi zasady zabezpechennya informatsiynoyi bezpeky Ukrayiny*: dys. … kand. yuryd. nauk: 12.00.01 / Yu. Ye. Maksymenko. – K., 2007. – 186 s.

Buryachok, V.L. *Informatsiyna ta kiberbezpeka: sotsiotekhnichnyy aspekt*: pidruchnyk / [V.L. Buryachok, V.B. Tolubko, V.O. Khoroshko, S.V. Tolyupa]; za zah. red. d-ra tekhn. nauk, profesora V.B. Tolubka. – K.: DUT, 2015. – 288 s.

Lohinova N.I. *Analiz spivvidnoshennya informatsiynoyi ta kibernetychnoyi bezpeky // I naukova Internet-konferentsiyi "Vykorystannya suchasnykh informatsiynykh tekhnolohiy v pidhotovtsi ta profesiyniy diyal'nosti pravoznavtsiv Natsional'noho universytetu «Odes'ka yurydychna akademiya»*. Pobrano: 24 marzets 2017, źródło: http://tsonf.inf.od.ua/doklady-konferentsii/spisok-dokladov-iv-konferentsii-2016-g/106-loginova

Furashev V.M., *Kiberprostir ta informatsiynyy prostir, kiberbezpeka ta informatsiyna bezpeka: sutnist', vyznachennya, vidminnosti* // /„Informatsiya i pravo", 2(5)/2012. Pobrano: 24 marzets 2017, źródło: http://ippi.org.ua/journal/85

22. *Redefining information warfare boundaries for an Army in a wireless world* / Isaac R. Porche III, Christopher P., M. York, C. Serena, J.M. Sollinger, E. Axelband, E.Y. Min, B.J. Held. Pobrano: 24 marzec 2017, źródło: http://www.rand.org/content/dam/rand/pubs/monographs/MG1100/MG1113/RAND_MG1113.pdf

23. Popova T. *Shcho oznachaye «Doktryna informatsiynoyi bezpeky Ukrayiny»*? Pobrano: 24 marzets 2017, źródło: http://www.radiosvoboda.org/a/28337376.html