publisher.agency
Norway

October, 2022
№ 1

Oslo, Norway
04-06.10.2022

International Scientific Conference

Theoretical Hypotheses and Empirical Results

UDC 001.1
P 97

Publisher.agency (1): Proceedings of the 1st International Scientific Conference «Theoretical Hypotheses and Empirical results» (October 04-06, 2022). Oslo, Norway, 2022. 290p

ISBN 978-7-9759-6275-5

DOI 10.5281/zenodo.7153556

editor@publisher.agency

https://publisher.agency/

Social Sciences

THE EMERGENCE OF GENDER STUDIES IN AZERBAIJAN 227
ADIGEZALOVA SVETLANA

Physical and Mathematical Sciences

STUDY OF SCATTERING RELATIVISTIC ELECTRONS IN ATOMS 237
MIRABUTALIBOV MIRTEIMOUR MIRKAZIM
ALIYEVA MINA BEYLER
FINDING SUBOPTIMISTIC SOLUTION BY ESTIMATING THE UNKNOWNS TWO IN THE INTERVAL KNAPSACK PROBLEM..... 241
K.SH MAMMADOV
S.Y.HUSEINOV
I.I.BAKSHALIEVA
A NEW CONJECTURE TO THAT OF RIEMANN 243
PR. AZIZ ARBAI
A NEW WAY OF LOOKING AT COMPLEX NUMBERS 250
PR. AZIZ ARBAI
DR. AMINA BELLEKBIR
HYPOTHESIS DISCUSSION ON THE EXPERIMENTS OF A LARGE SAMPLE OF TOSSING OF THE COIN 258
ABHAY KRISHAN

Political Sciences

CYBERZAGROŻENIA JAKO RODZAJ AGRESJI HYBRYDOWEJ – DOŚWIADCZENIE RZECZYPOSPOLITEJ POLSKIEJ W ZAKRESIE ZAPOBIEGANIA I PRZECIWDZIAŁANIA TAKIM ZJAWISKOM 262
HRANOVSKYI MYKOLA
KARAMYSHEV DMYTRO
FOREIGN POLICY ELITE OF KAZAKHSTAN AND THE EU IN THE TRADE AND ECONOMIC SPHERE: SUCCESSES AND PROSPECTS..... 269
LEILA ABDRAZAKOVA

Chemical Sciences

COMPOSITIONS BASED ON ELASTOMERS (BUTADIENE-NITRILE RUBBER) 280
ABDULLAYEVA IRADA GURBAN
BAKHSHALIYEV ELGUN

Political Sciences

Cyberzagrożenia jako rodzaj agresji hybrydowej – doświadczenie Rzeczypospolitej Polskiej w zakresie zapobiegania i przeciwdziałania takim zjawiskom

Hranovskyi Mykola
student studiów doktoranckich Katedry Nauk Politycznych i Filozofii Instytutu Edukacyjno-Naukowego „Instytut Administracji Publicznej" Charkowskiego Narodowego Uniwersytetu im. V. N. Karazina, Charków, Ukraina
Karamyshev Dmytro
doktor nauk z administracji publicznej, profesor Katedry Polityki Społecznej i Humanitarnej Charkowskiego Narodowego Uniwersytetu im. V. N. Karazina, Charków, Ukraina

Adnotacja. W dzisiejszym świecie istnieje tendencja do znacznego wzrostu liczby cyberataków, które stają się coraz bardziej wyrafinowane i nieprzewidywalne. Kwestia zapewnienia bezpieczeństwa cybernetycznego stała się niezwykle istotna dla krajów świata, ale środki przeciwdziałania wyzwaniom i zagrożeniom w tym obszarze są nadal istotne dla społeczności światowej. W związku z powyższym przedstawiono krótką analizę działań mających na celu zapobieganie i przeciwdziałanie cyberzagrożeniom na przykładzie Rzeczypospolitej Polskiej.

Słowa kluczowe: cyberbezpieczeństwo, cyberatak, obiekty infrastruktury krytycznej państwa, incydent, współpraca międzynarodowa w zakresie ochrony cyberprzestrzeni.

Sformułowanie problemu. Jednym z kluczowych problemów, z jakimi spotykają się państwa świata, jest problem ochrony informacji przed wyzwaniami i zagrożeniami w cyberprzestrzeni. Znaczenie kwestii bezpieczeństwa cybernetycznego jest dziś niewątpliwe, ponieważ każdy współczesny człowiek stoi przed koniecznością korzystania z systemów i technologii informatycznych, od sieci społecznościowych, zamieszczania informacji o swoich danych osobowych w Internecie po korzystanie z banku konta, systemy e-commerce itp.

Analiza najnowszych badań i publikacji. Badanie problematyki bezpieczeństwa cybernetycznego jako elementu ochrony informacji państwa we współczesnych warunkach jest przedmiotem uwagi wielu naukowców: S. Morgana, A. Klimburga, M. Schmidta, M. Gedekera, M. Libitskiego, J. Nye, I. Zubarev, M. Bezkorovainy , P. Olchowska, J. Garbiński, O. Krokovska, D. Dubov, M. Ozhevan, V. Furashev, V. Buryachok, V. Butuzov, V. Tolubko, O. Dovgan, V. O. Khoroshko, S. V. Tolyupa, M. Balyuk, V. Doroshko i inni.
Mimo dużej ilosci opracowań w tym zakresie, kwestia zapewnienia cyberbezpieczeństwa jako integralnego elementu systemu bezpieczeństwa informacji, zwłaszcza w warunkach wojny hybrydowej wciąż pozostaje otwarta.
Ponieważ Polska zajmuje się rozwiązywaniem tego problemu systematycznie i na poziomie krajowym, zwracając szczególną uwagę na zapobieganie i przeciwdziałanie cyberzagrożeniom, sugeruje się zapoznanie się z analizą polskich doświadczeń w rozwiązywaniu istniejących problemów z zakresu prewencji i przeciwdziałanie cyberzagrożeniom.

Celem niniejszego artykułu jest analiza aktualnego stanu zwalczania cyberataków w krajach UE, w szczególności w Rzeczypospolitej Polskiej.

Prezentacja głównego materiału badawczego. 1 sierpnia 2018 r. Prezydent RP podpisał ustawę o Krajowym Systemie Cyberbezpieczeństwa [3]. Ustawa ta wdraża dyrektywę Parlamentu Europejskiego i Rady (UE) 2016/1148 Dyrektywę (UE) 2016/1148 w sprawie środków zapewniających wysoki ogólny poziom

bezpieczeństwa sieci i systemów informatycznych w UE (tzw. Dyrektywa (dyrektywa NIS) (zwana dalej dyrektywą NIS) [2].

Zobowiązuje państwa członkowskie UE do zagwarantowania minimalnego poziomu krajowych zdolności w zakresie cyberbezpieczeństwa poprzez tworzenie właściwych organów i pojedynczych punktów kontaktowych dla cyberbezpieczeństwa, tworzenie zespołów reagowania na incydenty bezpieczeństwa komputerowego (CSIRTs computer security) oraz przyjmowanie krajowych strategii cyberbezpieczeństwa.

Ustawa o krajowym systemie cyberbezpieczeństwa weszła w życie 28 sierpnia 2018 r. Jednak dla pełnego wdrożenia dyrektywy NIS w Polsce konieczne było przyjęcie dodatkowych uchwał Rady Ministrów RP jako aktów wykonawczych w szczególności szereg Uchwał: z dnia 11 września 2018 r. „W sprawie wykazu usług kluczowych oraz progów istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych" z dnia 02.10.2018 r. „W sprawie zakresu działania oraz trybu pracy Kolegium do spraw Cyberbezpieczeństwa", z dnia 16.10.2018 r. „ W sprawie rodzajów dokumentacji dotyczącej cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej ", z dn. 31.10.2018 r. „W zakresie progów uznania incydentu za poważny" [6].

Dyrektywa NIS zobowiązuje do zapewnienia cyberbezpieczeństwa w obszarach usług, które mają kluczowe znaczenie dla wspierania krytycznych działań społeczno-gospodarczych państwa.

Sektory te obejmują: energetykę, transport, bankowość, instytucje finansowe, opiekę zdrowotną, infrastrukturę wodną i cyfrową. Ustawa wprowadziła koncepcję systemu cyberbezpieczeństwa, który ma na celu zapewnienie cyberbezpieczeństwa oraz zapobieganie i przeciwdziałanie cyberzagrożeniom [4] na poziomie krajowym, w tym nieprzerwane świadczenie usług kluczowych i usług cyfrowych, poprzez osiągnięcie odpowiedniego poziomu bezpieczeństwa systemów informatycznych służących do świadczenia tych usług oraz zapewniających obsługę incydentów. Podmioty wchodzące w skład Krajowego Systemu Cyberbezpieczeństwa (NSC):

- kluczowi operatorzy;
- dostawcy usług cyfrowych;
- instytucje państwowe;
- Kompetentne władze;
- CSIRT na poziomie krajowym,
- Pojedynczy punkt kontaktowy w kwestiach bezpieczeństwa cybernetycznego;
- Podmioty świadczące usługi w zakresie cyberbezpieczeństwa.

Dzięki nowemu prawu pojawiły się również nowe pojęcia: incydenty (krytyczne, poważne, znaczące, w strukturze państwa), usługi (kluczowe i cyfrowe), zarządzanie podatnością czy incydentami.

Incydent to zdarzenie, które ma lub może mieć negatywny wpływ na cyberbezpieczeństwo. Kilka ich typów zostało zidentyfikowanych przez prawo. Incydent krytyczny – prowadzi do naruszenia bezpieczeństwa lub porządku publicznego, interesów międzynarodowych lub gospodarczych, funkcjonowania instytucji publicznych, praw i wolności obywatelskich, zdrowia lub życia ludzi. Takie przypadki są klasyfikowane przez odpowiednie zespoły CSIRT – omówione poniżej. Poważny incydent – może to spowodować znaczne obniżenie jakości lub przerwę w ciągłości usługi klucza. Incydent istotny – istotnie wpływa na świadczenie usługi cyfrowej. Incydent w strukturze państwa może spowodować obniżenie jakości lub przerwanie zadania publicznego realizowanego przez organ państwowy.

Wystąpienie incydentu może zakłócić działanie usługi cyfrowej – świadczonej drogą elektroniczną oraz usługi kluczowej – ważnej dla wspierania krytycznych działań społecznych lub gospodarczych. Lista usług kluczowych zawarta jest w Rozporządzeniu Rady Ministrów RP z dnia 11 września 2018 r. w sprawie wykazu usług kluczowych oraz progów znaczenia destrukcyjnego skutku zdarzenia dla świadczenia usług kluczowych.

W związku z nowymi aktami prawnymi operatorzy usług kluczowych również zostają rozdzieleni (załącznik nr 1 do Ustawy) i nakładają na nich obowiązki, w tym:

- systematyczna ocena ryzyka i zarządzanie incydentami, wdrażanie odpowiednich środków technicznych i organizacyjnych, zbieranie informacji o zagrożeniach cyberbezpieczeństwa i podatności na incydenty, zarządzanie incydentami oraz stosowanie środków zapobiegania i ograniczania wpływu incydentów na bezpieczeństwo systemów informatycznych;
- opracowanie, zastosowanie i aktualizacja dokumentacji dotyczącej cyberbezpieczeństwa systemu informatycznego służącego do świadczenia usługi kluczowej oraz ustanowienie nadzoru nad tą dokumentacją;

• tworzenie wewnętrznych struktur odpowiedzialnych za cyberbezpieczeństwo lub zawarcie umowy z podmiotem gospodarczym świadczącym usługi cyberbezpieczeństwa;

• zapewnienie audytu bezpieczeństwa systemu informatycznego co najmniej raz na 2 lata.

W przypadku awarii, zgodnie z prawem, należy go serwisować. Odnosi się to do czynności polegającej na wykrywaniu, rejestrowaniu, analizowaniu, klasyfikowaniu, ustalaniu priorytetów, podejmowaniu działań naprawczych i ograniczaniu konsekwencji incydentu. Ustawa określa trzy organy na poziomie krajowym, które zajmują się reagowaniem na incydenty komputerowe i zarządzaniem nimi. Zgodnie z terminologią przyjętą w dyrektywie NIS 2016/1148 nazywane są CSIRT. W Polsce są to „CSIRT GOV", „CSIRT MON", „CSIRT NASK".

CSIRT GOV, czyli Rządowy Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego pod przewodnictwem funkcjonariusza na poziomie Szefa Agencji Bezpieczeństwa Wewnętrznego – którego zadaniem jest opracowywanie i koordynowanie przeglądu incydentów zgłaszanych przez kluczowe podmioty sektora publicznego w sektorze finansów publicznych, jednostki zgłaszające się do i nadzorowane przez Prezesa Rady Ministrów (m.in. RCB), KNF, UZP, URE, PGRP, Narodowy Bank Polski, Bank Gospodarki Narodowej (Bank Gospodarstwa Krajowego) oraz podmioty objęte ustawą o zarządzaniu kryzysowym, czyli podmioty, których systemy teleinformatyczne (ICT) lub sieci teleinformatyczne są ujęte w jednolitym wykazie obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej,

CSIRT MON to System Reagowania na Incydenty Komputerowe Ministerstwa Obrony Narodowej RP. Określona struktura koordynuje rozpatrywanie incydentów zgłaszanych przez podmioty podległe lub podlegające Ministrowi Obrony Narodowej oraz przedsiębiorców o szczególnym znaczeniu gospodarczym i obronnym.

CSIRT NASK zarządzany jest przez Naukową i Akademicką Sieć Komputerową i reaguje na incydenty zgłaszane przez instytuty badawcze, Polską Agencję Żeglugi Powietrznej (PAŻP) lub osoby fizyczne.

CSIRT zapewniają spójny i kompletny system zarządzania ryzykiem na poziomie krajowym, realizując zadania przeciwdziałania zagrożeniom cyberbezpieczeństwa o charakterze międzysektorowym i transgranicznym – znajdują się w europejskiej sieci CSIRT i przekazują informacje o incydentach innym państwom oraz inne punkty kontaktowe. Zespoły realizują te zadania we współpracy ze sobą, z organami właściwymi do spraw cyberbezpieczeństwa, ministrem właściwym do spraw IT oraz pełnomocnikami. Monitorują zagrożenia i incydenty cyberbezpieczeństwa na poziomie krajowym oraz oceniają związane z nimi ryzyko. Mogą również wysyłać powiadomienia o wykrytych zagrożeniach.

Zespoły CSIRT są zobowiązane do informowania siebie nawzajem oraz Rządowego Centrum Bezpieczeństwa o krytycznym incydencie, który może spowodować kryzys bezpieczeństwa lub porządku publicznego. Zespoły wspólnie opracowują podstawowe elementy procedur obsługi incydentów, w których współpracują ze sobą.

Ustawa wprowadza również pojęcie grupy branżowej ds. cyberbezpieczeństwa, czyli zespołu utworzonego przez organ właściwy dla danego sektora lub podsektora. Zespół ten jest odpowiedzialny za obsługę lub wspieranie obsługi incydentów w swoim sektorze lub podsektorze.

Innym organem utworzonym przez nowe prawo jest Zespół ds. Incydentów Krytycznych, który pełni rolę wspierającą w radzeniu sobie z incydentami krytycznymi zgłaszanymi przez sieć CSIRT. W skład zespołu wchodzą przedstawiciele Rządowego Centrum Bezpieczeństwa, a także CSIRT MON, CSIRT NASK oraz szef Agencji Bezpieczeństwa Wewnętrznego. Na jej czele stoi dyrektor rządowego centrum bezpieczeństwa.

Zgodnie z dyrektywą europejską utworzono Pojedynczy Punkt Kontaktowy, który podlega Ministerstwu Cyfryzacji i odpowiada za:

• stworzenie ram prawnych funkcjonowania strefy cyberbezpieczeństwa RP, w tym zapewnienie ich spójności;

• pełnienie funkcji komunikacyjnej w celu zapewnienia współpracy z podmiotami odpowiedzialnymi za cyberbezpieczeństwo;

• gromadzenie i przetwarzanie informacji otrzymywanych m.in. przez kluczowych operatorów usług;

• kontrola przestrzegania wymagań organizacyjnych i technicznych przez podmioty świadczące usługi cyberbezpieczeństwa;

• przekazywanie, na żądanie odpowiedniego CSIRT, powiadomienia o poważnym incydencie lub istotnym incydencie z udziałem co najmniej dwóch państw członkowskich UE do pojedynczych punktów kontaktowych innych państw członkowskich UE;

• zapewnienie udziału przedstawiciela RP w Grupie Współpracy;
• zapewnienie współpracy z Komisją Europejską w zakresie cyberbezpieczeństwa;
• koordynacja współpracy organów właściwych w sprawach cyberbezpieczeństwa RP z właściwymi organami państw członkowskich UE;
• współpraca z innymi organami, na przykład organami ścigania i właściwym organem w kwestiach ochrony danych [5].

Podmiotem odpowiedzialnym za koordynację działań i realizację polityki rządu w zakresie zapewnienia cyberbezpieczeństwa w RP jest Pełnomocnik Rządu ds. Cyberbezpieczeństwa (jego funkcje pełni Sekretarz Stanu Ministerstwa Cyfryzacji RP Polski). Do głównych zadań Rzecznika Rządu należy w szczególności analiza i ocena funkcjonowania krajowego systemu cyberbezpieczeństwa, kontrola procesu zarządzania ryzykiem krajowego systemu cyberbezpieczeństwa, wydawanie wniosków dotyczących projektów rozporządzeń i innych dokumentów rządowych mających wpływ na realizację zadań z zakresu cyberbezpieczeństwa, wydawanie zaleceń i inicjowanie krajowych ćwiczeń z zakresu cyberbezpieczeństwa. Pełnomocnik ma obowiązek przedłożyć Radzie Ministrów sprawozdanie za poprzedni rok kalendarzowy, zawierające informacje o bieżących działaniach w zakresie cyberbezpieczeństwa w kraju, do dnia 31 marca każdego roku. Rada ds. Bezpieczeństwa Cybernetycznego została powołana przy Radzie Ministrów. Jest to organ doradczy i konsultacyjny zajmujący się planowaniem, nadzorem i koordynacją zespołów CSIRT, grup branżowych zajmujących się cyberbezpieczeństwem oraz właściwych organów. Powołanie Rady miało na celu wspieranie większej spójności systemowej i przejrzystości, a także nadanie odpowiedniej rangi kwestiom cyberbezpieczeństwa, a także zapewnienie formułowania spójnych instrukcji i planów przeciwdziałania zagrożeniom cyberbezpieczeństwa. Natomiast art. 90 określa w drodze uchwały termin realizacji Strategii do 31 października 2019 r. Dokument określa cele strategiczne i odpowiadające im działania polityczne mające na celu osiągnięcie i utrzymanie wysokiego poziomu bezpieczeństwa cybernetycznego RP. Zaistniała potrzeba oceny i rewizji obowiązującego dokumentu strategicznego na rok 2019, tj. Krajowych Ram Polityki Cyberbezpieczeństwa RP na lata 2017-2022, przyjętych Uchwałą nr 52/2017 Rady Ministrów z dnia 27 kwietnia , 2017 oraz odpowiedni Plan Działań na rzecz wdrażania Krajowych Ram Polityki Cyberbezpieczeństwa RP na lata 2017-2022. Stale zmieniające się warunki związane z bezpieczeństwem, zwłaszcza w cyberprzestrzeni, wymagają szybkiej i zdecydowanej reakcji agencji rządowych. Zdaniem Kancelarii Premiera: projekt uchwały ma na celu stworzenie strategii cyberbezpieczeństwa. Strategia ma charakter polityczno-strategiczny, natomiast na poziomie operacyjnym jej realizacja zapewni szczegółowy plan działania. Plan działań opisuje podmioty zaangażowane w realizację Strategii oraz środki jej realizacji. Przy opracowywaniu Strategii wykorzystano najlepsze praktyki i rozwiązania zaproponowane przez Międzynarodowy Związek Telekomunikacyjny oraz doświadczenia innych krajów [1].

Działalność Ministerstwa Cyfryzacji RP

Celem Ustawy o Krajowym Systemie Cyberbezpieczeństwa, przygotowanej przez Ministerstwo Cyfryzacji RP, było opracowanie ustawodawstwa, które pozwoliłoby na implementację Dyrektywy NIS i stworzenie skutecznego systemu bezpieczeństwa teleinformatycznego na poziomie krajowym. W celu realizacji określonych aktów normatywnych Rzecznik Rządu współdziała z różnymi wyspecjalizowanymi strukturami, np.:

- z kompetentnymi organami w zakresie szkolenia personelu;
- z CSIRT w sprawie wytycznych;
- z organami samorządu lokalnego w dziedzinie edukacji i e-learningu;
- z partnerami technologicznymi w zakresie wymiany informacji o nowych zagrożeniach i technologiach.

Naukowo-akademicka sieć komputerowa – Państwowy Instytut Badawczy (Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy (NASK) zlecił działania mające na celu podniesienie poziomu świadomości w zakresie cyberzagrożeń wśród pracowników administracji państwowej. Przewiduje się realizację dwóch zadań:

1. Budowa platformy szkoleń elektronicznych (e-CTP - CyberTrainingPlatform) dla pracowników administracji publicznej, w tym jednostek samorządu terytorialnego.

Testy platformy powinny odbyć się do końca tego roku w urzędach państwowych, a platforma zostanie w pełni uruchomiona w 2020 roku. Urzędy zostaną zaproszone do konsekwentnego korzystania z e-learningu zgodnie z ustalonym harmonogramem. Planuje się, że platforma będzie tymczasowo dostępna dla konkretnej administracji państwowej i w tym czasie nie będzie dostępna dla innych. Podjęto również decyzję o stworzeniu call center, które będzie obsługiwać wspomnianą platformę.

2. Prowadzenie specjalistycznych szkoleń w regionach dla przedstawicieli poszczególnych pododdziałów strukturalnych organów państwowych i samorządowych w ramach ustawy o Krajowym Systemie Cyberbezpieczeństwa (NSC).

Celem szkoleń jest podniesienie poziomu bezpieczeństwa w organach administracji państwowej i samorządu terytorialnego poprzez podniesienie poziomu świadomości i budowanie kompetencji w zakresie cyberbezpieczeństwa. Planowana jest organizacja czterech spotkań informacyjnych (organizowanych na bazie czterech wybranych/gotowych do współpracy lokalnych administracji państwowych), które obejmą łącznie około czterystu urzędników szczebla regionalnego odpowiedzialnych za cyberbezpieczeństwo. Oba zadania projektowe wspierane przez trzy zespoły NASK: Akademię NASK, Szkołę Informatyczną oraz NASK CSIRT. Koordynację zapewni departament cyberbezpieczeństwa Ministerstwa Cyfryzacji.

Kolejnym aspektem rozwojowej działalności NPP jest współpraca technologiczna. Jest to szczególnie ważne ze względu na umowy dwustronne z partnerami technologicznymi oraz wymianę informacji (podatności, zagrożeń, narzędzi monitorowania cyberbezpieczeństwa). To jednak nie wszystkie wysiłki na rzecz stworzenia potężnego systemu cyberbezpieczeństwa w Polsce.

W ramach projektu badawczego powstała Krajowa Platforma Cyfrowa, która przewiduje stworzenie prototypu złożonego, zintegrowanego systemu monitorowania, obrazowania i ostrzeżeń o zagrożeniach cyberprzestrzeni państwa, oceny potencjalnych skutków i skoordynowanego reagowania do incydentów komputerowych na poziomie krajowym. Przy pomocy tego projektu Minister Cyfryzacji zapewnia rozwój lub utrzymanie systemu teleinformatycznego obsługującego:

- wymianę informacji w celu współpracy podmiotów wchodzących w skład krajowego systemu cyberbezpieczeństwa;
- tworzenie i przyjmowanie rekomendacji dotyczących działań podnoszących poziom cyberbezpieczeństwa;
- zgłaszanie i obsługa incydentów, ocena ryzyka na poziomie krajowym;
- ostrzeżenia o zagrożeniach cyberbezpieczeństwa.

Ponadto NASK opracowuje podręczniki obejmujące tematykę organizacji NASK, zasad zgłaszania spraw oraz ochrony danych osobowych. Publikowane są również na stronach internetowych MC i mają na celu szerokie rozpowszechnianie wiedzy i budowanie kompetencji.

Kolejną inicjatywą jest „Partnerstwo na rzecz cyberbezpieczeństwa" – narzędzie dobrowolnej współpracy i wymiany doświadczeń oraz informacji o zagrożeniach i incydentach w cyberbezpieczeństwie. Głównym narzędziem partnerstwa jest: wymiana informacji z zakresu cyberbezpieczeństwa, o incydentach i istotnych zagrożeniach, które wychodzą (wg informacji Partnera) poza zdarzenia wewnętrzne,

zapewniając odpowiednią reakcję i postępowanie w rozwiązywaniu problemów. W ramach udziału w programie uczestnicy mogą:

• przekazywać informacje o incydentach NASK;
• informować koordynatora programu (NASK) o zaobserwowanych zagrożeniach;
• dzielić się wiedzą z zakresu cyberbezpieczeństwa;
• zainicjować tworzenie grupy docelowej.

W ramach programu, na który obecnie składa się ponad pięćdziesiąt umów trójstronnych, podpisano siedem umów z jednostkami samorządu terytorialnego na szczeblu wojewódzkim (lokalnej administracji państwowej).

Wnioski. Cyberprzestrzeń jest uważana za piątą sferę działań wojennych, równie krytyczną dla operacji wojskowych jak ląd, morze, powietrze i przestrzeń kosmiczna. To sfera obejmująca wszystko: od sieci informacyjno-telekomunikacyjnych, infrastruktury i danych przez nie obsługiwanych po systemy komputerowe, procesory i urządzenia do sterowania.

Zapewnienie cyberbezpieczeństwa w Polsce i budowanie jej zrównoważonego systemu to proces ciągły. Warto zauważyć, że pomimo pojawiających się wyzwań i trudności staje się bardziej świadomy i zaplanowany. Oprócz tych wskazanych po audycie Wyższej Izby Kontroli (HCC) możemy również mówić o braku dostatecznej liczby ekspertów na rynku, trudnościach w harmonizacji aktów regulacyjnych i prawnych związanych z różnorodnością sektorów, różnych interpretacjach prawa i ustalonych wymagań. Niemniej realizacja Strategii jesienią tego roku oraz działania Ministerstwa Cyfryzacji mogą przyspieszyć wypracowanie odpowiednich mechanizmów zapewnienia cyberbezpieczeństwa w RP.

Zapewnienie cyberbezpieczeństwa w Europie, w szczególności w Polsce, oraz zbudowanie skutecznego systemu zwalczania cyberzagrożeń to długi i systematyczny proces, dolaczenie sie do którego na zasadach partnerskich, było by warto dla krajów, które w dalszym ciągu są celem cyberataków.

W nowoczesnych warunkach komponent informacyjny nabiera coraz większego znaczenia i staje się jednym z najważniejszych elementów zapewnienia bezpieczeństwa narodowego państwa.

BIBLIOGRAFIA:

1.BIULETYN INFORMACJI PUBLICZNEJ KANCELARII PREZESA RADY MIBISTRÓW RP.URL:HTTPS://BIP.KPRM.GOV.PL/KPR/WYKAZ/R953654207552,PROJEKT-UCHWALY-RADY-MINISTROW-W-SPRAWIE-STRATEGII-CYBERBEZPIECZENSTWA-RZECZYPOS.HTML

2. DYREKTYWA PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2016/1148 Z DNIA 6 LIPCA 2016 R. W SPRAWIE ŚRODKÓW NA RZECZ WYSOKIEGO WSPÓLNEGO POZIOMU BEZPIECZEŃSTWA SIECI I SYSTEMÓW INFORMATYCZNYCH NA TERYTORIUM UNII. URL: HTTPS://EUR-LEX.EUROPA.EU/LEGAL-CONTENT/PL/TXT/PDF/?URI=CELEX:32016L1148&FROM=PL

3. DZIENNIK USTAW RP 2018 ROK. URL:HTTP://WWW.DZIENNIKUSTAW.GOV.PL/DU/2018

4. ENCYKLOPEDIA ZARZĄDZANIA. URL:HTTPS://MFILES.PL/PL/INDEX.PHP/CYBERBEZPIECZEŃSTWO

5. STRONA INTERNETOWA MINISTERSTWA CYFRYZACJI RP.
URL: HTTPS://WWW.GOV.PL/WEB/CYFRYZACJA/KRAJOWY-SYSTEM-CYBERBEZPIECZENSTWA-

6. USTAWA Z 5 LIPCA 2018 R. «O KRAJOWYM SYSTEMIE CYBERBEZPIECZEŃSTWA».
URL:HTTP://PRAWO.SEJM.GOV.PL/ISAP.NSF/DOWNLOAD.XSP/WDU20180001560/T/D20181560L.PDF

Mykola Hranovskyi – graduate student of the Department of Political Science and Philosophy of the Educational and Scientific Institute "Institute of Public Administration" of Kharkiv National University named after V. N. Karazin, Kharkiv, Ukraine.

Dmytro Karamyshev – Doctor of Science of Public Administration, Professor of the Department of Social and Humanitarian Policy of Kharkiv National University named after V. N. Karazin, Kharkiv, Ukraine.

Cyber threats as a kind of hybrid aggression - the experience of the Republic of Poland in preventing and counteracting such phenomena.

Annotation. *In today's world, there is a tendency to significantly increase the number of cyber attacks, which are becoming more and more sophisticated and unpredictable. The issue of ensuring cybersecurity has become extremely important for the countries of the world, but measures to counter the challenges and threats in this area are still important for the global community. Therefore, a short analysis of activities aimed at preventing and counteracting cyber threats, based on the example of the Republic of Poland, is presented.*

Key words: *cybersecurity, cyber attack, critical objects of state infrastructure, international cooperation in the field of cyberspace protection.*

Proceedings of the 1st International Scientific Conference
«Theoretical Hypotheses and Empirical results» (October 04-06, 2022).
Oslo, Norway, 2022. 290p

editor@publisher.agency

https://publisher.agency

University of Norway

PO Box 1012 Blindern

0224 Oslo