DOI: 10.52694/ThPSR.124.9

Monika Majchrzak

Wpływ strategii informacyjnej w więziennictwie na bezpieczeństwo państwa

The Impact of Prison Information Strategy on National Security

W obecnym świecie model funkcjonowania państwa kształtowany jest nie tylko przez zasoby finansowe, rzeczowe, społeczne, militarne, ale także przez politykę informacyjną w więziennictwie. Stopień wykorzystywania i angażowania informacji w realizację strategicznych celów państwa wymaga stałego utrzymywania jej tajności i zapewnienia skutecznej jej ochrony przed niepowołanymi osobami. Takie działania wymagają jednak skonkretyzowanego zakresu niezbędnych czynności oraz bezwzględnej dyscypliny w ich implementacji w ośrodkach penitencjarnych.

Celem artykułu jest zaprezentowanie wpływu polityki informacyjnej w więziennictwie na problemy bezpieczeństwa państwa. Problem ten został zawarty w pytaniu o zagrożenia, jakie mogą się pojawić w sytuacji, gdy organy państwa, realizując swoje zadania wobec społeczeństwa, pominą lub zaniedbają albo chociażby niewłaściwie realizują politykę informacyjną w systemie penitencjarnym.

W artykule wykorzystano następujące metody badawcze: analizę, syntezę, porównanie i wnioskowania.

Ze względu na wagę problemu polegającego na prowadzeniu przez państwo właściwej polityki bezpieczeństwa w obszarze informacyjnym w więziennictwie zaprezentowano wraz z wnioskami skalę incydentów, przedstawioną w raporcie rocznym z działalności CERT Polska za lata 2021–2022. Obraz wynikający z tego raportu powinien w sposób ciągły mobilizować organy państwa do wdrażania i prowadzenia polityki informacyjnej w sposób skutecznie zabezpieczający informacje, którymi wymieniają się przedstawiciele państwa ze służbą więzienną i społeczeństwem.

Słowa kluczowe: polityka, polityka informacyjna, polityka bezpieczeństwa, bezpieczeństwo państwa, zagrożenia, bezpieczeństwo systemu informacyjnego, więziennictwo, system penitencjarny

In the current world, the state's operating model is shaped not only by financial, material, social, military resources, but also by information policy in the prison system. The degree of use and involvement of information in the implementation of the strategic objectives of the state requires that its secrecy be maintained at all times and that it be effectively protected from unauthorized persons. Such measures, however, require a concretized scope of necessary activities and absolute discipline in their implementation in penitentiary facilities.

The purpose of the article is to present the impact of information policy in the penitentiary system on state security problems. The problem was included in the question of the dangers that may arise in the situation when the state bodies, while carrying out their tasks to society, omit or neglect, or at least improperly implement the information policy in the penitentiary system.

The article uses the following research methods: analysis, synthesis, comparison and inference.

Due to the importance of the problem of how the state conducts a proper security policy in the information area in the prison sector, the scale of incidents presented in the annual report on the activities of CERT Poland for 2021-2022 is presented with conclusions. The picture resulting from this report should continuously mobilize state bodies to implement and conduct information policy in a way that effectively secures the information exchanged by state representatives with the prison service and the public.

Key words: politics, information policy, security policy, state security, threats, information system security, prisons, penitentiary system

Wprowadzenie

Informacja, która wypełniła całą cyberprzestrzeń, jest wykorzystywana w więziennictwie do komunikacji, a przez to stymuluje zachowania ludzi oraz kształtuje procesy decyzyjne w państwie. W związku z tym stała

się ona przedmiotem zainteresowania i pożądania służb wywiadowczych i środowisk przestępczych. Mnogość informacji w sieci oraz poczucie anonimowości stanowią potencjalne zagrożenie dla środowisk penitencjarnych, które są odbiorcami informacji. Zjawisko cyberprzestępstw nieustannie potęguje się między innymi z tego powodu, że użytkownicy sieci często z powodów rutynowych pomijają zabezpieczenia systemowe.

Sfera cyfryzacji podlega ciągłej ewolucji, wkracza w kolejne obszary życia społecznego i powoduje tworzenie społeczeństwa informacyjnego, także w więziennictwie. Jest to środowisko zdominowane przez osoby posiadające kompetencje informatyczne, doskonale odnajdujące się w cyberprzestrzeni gromadzącej w swych zasobach ogromne ilości danych o osobach osadzonych i pracownikach służby więziennej. W obecnej rzeczywistości informacja nabrała szczególnego znaczenia zarówno w sferze obronności państwa, ale także w sferze polityczno-prawnej, ekonomicznej, technologicznej czy społeczno-kulturalnej, a także penitencjarnej.

Celem artykułu jest zaprezentowanie wpływu polityki informacyjnej w więziennictwie na problemy bezpieczeństwa państwa. Realizacja tego celu wymaga rozwiązania problemu badawczego zawartego w następującym pytaniu: jakie zagrożenia mogą się pojawić w sytuacji, gdy organy państwa, realizując swoje zadania wobec społeczeństwa, pominą lub zaniedbają albo chociażby niewłaściwie realizują politykę informacyjną w systemie penitencjarnym.

W artykule przyjęto hipotezę, że organy władzy państwowej w procesie podejmowania decyzji narażone są na niebezpieczeństwa związane z korzystaniem z ogromnej ilości informacji w więziennictwie. W tej sytuacji służba więzienna powinna realizować politykę bezpieczeństwa informacyjnego w celu eliminowania mogących pojawiać się poważnych zagrożeń dla organów państwa, ale także dla społeczeństwa, wynikających z wykorzystania w procesie decyzyjnym niewłaściwych i błędnych decyzji wobec osadzonych.

W celu potwierdzenia przyjętej hipotezy dokonano prezentacji wybranych rozważań teoretycznych zawartych w literaturze dotyczącej polityki informacyjnej w systemie więziennictwa. W celu potwierdzenia ustaleń teoretycznych dokonano analizy porównawczej i zaprezentowano wnioski wynikające z materiału empirycznego zawartego w Raporcie rocznym z działalności CERT Polska za lata 2021–2022.

Państwo działające za pośrednictwem swoich organów powinno być wzorem w zakresie utrzymania wysokich standardów bezpieczeństwa

informacyjnego, które z kolei przekłada się na bezpieczeństwo całego kraju we wszystkich obszarach jego funkcjonowania, w tym systemu penitencjarnego. Wysoki poziom świadomości zagrożeń i negatywnych skutków naruszeń zasad prowadzenia polityki informacyjnej w więziennictwie pozwala na podejmowanie właściwych decyzji w zakresie bezpieczeństwa narodowego, które powinno uwzględniać problematykę szybkiego rozwoju społeczeństwa informacyjnego. W obecnej rzeczywistości systemy informacyjne w służbie więziennictwa bez niezbędnej kontroli i bieżącego monitorowania mogą okazać się słabą stroną funkcjonowania całego aparatu państwowego.

Artykuł wpisuje się w badania dotyczące szerokiej problematyki bezpieczeństwa w więziennictwie, ze szczególnym uwzględnieniem bezpieczeństwa informacyjnego. Wydaje się, że może być również materiałem wykorzystywanym przez studentów kierunków związanych z bezpieczeństwem.

Rola polityki informacyjnej w więziennictwie

Właściwa polityka informacyjna dotyczy wszystkich obszarów funkcjonowania państwa tzn. między innymi gospodarki, polityki, ochrony środowiska, obrony granic. Do tych sfer funkcjonowania państwa należy również więziennictwo jako obszar z jednej strony specyficzny, ale stanowiący ważny element funkcjonowania państwa. Można więc z pewnością założyć, że wszystkie zjawiska dotyczące polityki informacyjnej mające wpływ na funkcjonowanie państwa dotyczą również więziennictwa.

Znaczenie polityki informacyjnej dla funkcjonowania państwa, a więc również dla więziennictwa jest przedmiotem badań i rozważań, które warunkuje bezpieczeństwo państwa i obywateli.

Dostrzeganie potrzeby uwzględnienia działań w obszarze zabezpieczeń informacji w narastającym „kryzysie" jej bezpieczeństwa sprawia, że stała się dyskursem do wnikliwej analizy zagrożeń, jakie może wywołać dla państwa, jeśli jest niewystarczająco chroniona, zwłaszcza w więziennictwie. Dystrybucja informacji w przekazie nadawcy powinna być wolna od niebezpiecznych *deepfake'ów*, które wprowadzają opinię publiczną w błąd, fałszują strategiczne informacje i w rezultacie zakłócają lub wręcz uniemożliwiają właściwą reakcję na nie przez adresata.

Pełne zrozumienie problemu wymaga dookreślenia, czym jest sama informacja. Jest to czynnik, który zmniejsza skalę niewiedzy o danym zjawisku oraz umożliwia podjęcie właściwej decyzji lub sprawniejsze działanie państwa[1]. Niekwestowana rola informacji w więziennictwie w procesie decyzyjnym państwa przybiera charakter strategiczny. Informacja jest źródłem wiedzy, której odpowiednie wykorzystanie daje władzę. Im bardziej wiarygodna informacja i im więcej jej jest, tym bardziej wzrastają szanse na optymalną decyzję[2].

Polityka informacyjna tworzy więc warunki, w których podejmowane są wszystkie decyzje, w ramach których toczy się dyskurs publiczny i polityczna działalność. Przez długi czas była uważana za „niską politykę" o relatywnie niewielkim znaczeniu, względnie nieistotną. Koncepcja krajowej polityki informacyjnej stała się możliwa tylko dlatego, że przywódcy polityczni na całym świecie uznali, że w rzeczywistości przepisy i regulacje dotyczące informacji są kwestiami „wysokiej polityki" o nadrzędnym znaczeniu strategicznym[3].

Podsumowując, zwyczajowo polityka informacyjna powinna być kreowana przez organy państwa przy wsparciu osób odpowiedzialnych za ochronę informacji znajdujących się w gestii każdego podmiotu[4]. Więzienie jest miejscem, gdzie informacja jest w dyspozycji służby więziennej oraz osadzonych. Każda z tych grup zabiega o informacje, którymi będą mogli skutecznie wpływać na siebie. Służba więzienna oczekuje podporządkowania. Natomiast osadzeni często skupiają swoją uwagę na próbach destabilizacji systemu karnego polegających na utrzymaniu kontaktu z zewnętrznym otoczeniem i mimo ograniczeń wolności wpływaniu na nie.

Zagrożenia dla bezpieczeństwa państwa w więziennictwie

Bez względu na to, jak spojrzymy na kwestię bezpieczeństwa, należy zauważyć, że musi być ono postrzegane jako wartość, do której warto dążyć, o którą warto zabiegać. Nie należy zapominać, że współczesne środowisko

[1] M. Witkowska, K. Cholawo-Soszoch, *Społeczeństwo informacyjne. Istota, rozwój, wyzwania*, Wydawnictwo Akademickie i Profesjonalne, Warszawa 2006, s. 99.
[2] P. Sienkiewicz, *Społeczeństwo informacyjne jako system cybernetyczny,* Uczelniane Wydawnictwo Naukowo-Dydaktyczne, Kraków 2004, s. 23.
[3] S. Braman, *Defining information policy*, „JOURNAL OF INFORMATION POLICY" 2011, Vol. 1, s. 2.
[4] K. Liderman, *Bezpieczeństwo informacyjne*. *Nowe wyzwania*, PWN, Warszawa 2017, s. 129.

bezpieczeństwa charakteryzuje się zacieraniem granic między jego wymiarem wewnętrznym i zewnętrznym, militarnym i pozamilitarnym.

Globalizacja i rosnąca współzależność często skutkują nieprzewidywalnością zjawisk, których zasięg nie jest już ograniczony barierami geograficznymi, systemami politycznymi i gospodarczymi. We współczesnych skłonnościach do wielosektorowego postrzegania bezpieczeństwa, nabiera ono szczególnego znaczenia. Tworzy złożony i dynamiczny wskaźnik sprawności organizacyjnej państwa, umożliwiając zjednoczenie obywateli wokół ważnego celu, jakim jest przeciwdziałanie zagrożeniom i budowanie społecznego poparcia dla decyzji podejmowanych przez kierownictwo[5].

Bezpieczeństwo państwa jest poddawane ciągłym przemianom, które wynikają z implementacji nowych rozwiązań dotyczących rządzenia państwem z uwzględnieniem więziennictwa. Dotychczasowa rola państwa w zapewnieniu obrony narodowej skupiała się jedynie na wojskowo-politycznej płaszczyźnie. Jednak postępująca cyfryzacja, w ramach której nieustannie dokonuje się szereg przemian organizacyjnych, technicznych, technologicznych, ekonomicznych, społecznych, ekologicznych, kulturowych itp. wymusiła poszerzenie tej problematyki o nowe płaszczyzny. Wśród tych płaszczyzn na przełomie XX i XXI w. bezpieczeństwo informacyjne łącznie z bezpieczeństwem ekonomicznym zostało uznane za priorytetową dziedzinę bezpieczeństwa narodowego[6].

Bezpieczeństwo systemów informacyjnych państwa polskiego w erze globalizacji informacji jest nieustannym obiektem cyberataków, stąd wymaga nie tylko odpowiedniego systemu zabezpieczeń poprzez system teleinformatyczny, ale również ochrony prawnej. Uregulowania prawne w połączeniu z właściwym systemem informacyjnym i szeroko zakrojoną kampanią uświadamiającą w społeczeństwie ich podatność na utratę bezpieczeństwa są w stanie ograniczyć zagrożenia w strefie informacji do poziomu akceptowalnego. Skuteczna ochrona systemu informacyjnego w więziennictwie wymaga permanentnego monitoringu otoczenia wewnętrznego i zewnętrznego państwa polskiego. Galopująca skala przestępstw w obszarze informacji i trudności w identyfikacji cyberprzestępców stanowią o istności podejmowanej problematyki. Państwo polskie często jest poddawane próbom ataków, które są wymierzone w przejęcie

[5] T. Kośmider, *Determinants of the process of creating national security*, „JOURNAL OF SECURITY AND SUSTAINABILITY ISSUES" 2021, Vol. 11, s. 297.

[6] J. Janczak, A. Nowak, *Bezpieczeństwo informacyjne. Wybrane problemy*, Akademia Obrony Narodowej, Warszawa 2013, s. 12.

informacji. Incydenty te zakłócają prawidłowe działanie i umniejszają ochronę aktywów, jakimi są informacje. Jak wynika z danych CERT Polska, intensyfikacja tych działań przestępczych nastąpiła po inwazji 24 lutego 2022 r. Federacji Rosyjskiej na Ukrainę.

Zmiany w ilości incydentów obsłużonych przez CERT Polska w latach 2021 r. i 2022 r. w podziale na kategorie wg taksonomii eCSIRT.net mkVI[7] przedstawia Tabela nr 1.

Tabela 1. Dynamika zmian w ilości obsłużonych incydentów przez CERT Polska w latach 2021–2022

Lp.	Typy incydentów	2021	2022	2022/2021 (%)
I.	Obraźliwe i nielegalne treści	311	308	99,04
	Spam	262	239	91,22
	Dyskredytacja, obrażanie	9	6	66,66
	Pornografia dziecięca, przemoc	4	0	0,00
	Niesklasyfikowane	36	63	175,00
II.	Złośliwe oprogramowanie	2 847	3 409	119,74
	Wirus	1	0	0,00
	Robak sieciowy	0	0	0,00
	Koń trojański	9	20	222,22
	Oprogramowanie szpiegowskie	0	1	0,00
	Dialer	0	0	0,00
	Rootkit	1	0	0,00
	Niesklasyfikowane	2 836	3 388	119,46
III.	Gromadzenie informacji	27	31	114,81
IV.	Próby włamań	127	121	95,28
V.	Włamania	247	354	143,32
VI.	Dostępność zasobów	148	175	118,24
VII.	Atak na bezpieczeństwo informacji	55	39	70,91
VIII.	Oszustwa komputerowe	25 472	35 009	137,44
	Nieuprawnione wykorzystanie zasobów	3	1	33,33
	Naruszenie praw autorskich	1	2	200,00
	Kradzież tożsamości, podszycie się	12	28	233,33
	Phishing	22 575	25 625	113,51
	Niesklasyfikowane	2 881	9 353	324,64
IX.	Podatne usługi	216	188	87,04
X.	Inne	33	49	148,50
RAZEM		**29 483**	**39 683**	**134,30**

Źródło: opracowanie własne na podstawie Raportu rocznego z działalności CERT Polska za lata 2021 i 2022, https://cert.pl/uploads/docs/Raport_CP_2021.pdf, ttps://cert.pl/uploads/docs/Raport_CP_2022.pdf, (24.05.2024), s.23-24, 38-39.

[7] https://www.trusted-introducer.org/Incident-Classification-Taxonomy.pdf (dostęp: 24.05.2024).

Z przedstawionego w Tabeli 1 materiału liczbowego wynika, że tylko w jednym roku liczba incydentów obsłużonych przez CERT Polska wzrosła o 10 200, to jest o 34,30%. Na wzrost ten zasadnicze znaczenie miały zdarzenia zakwalifikowane jako Oszustwa komputerowe, których liczba zwiększyła się o 37,44%. W grupie tej natomiast dominują ilościowo incydenty zakwalifikowane jako Phishing (wzrost o 13,51%). Należy ponadto zwrócić uwagę na wyjątkowo wysoki wzrost liczby incydentów niesklasyfikowanych. Ich ilość zwiększyła się o 224,64%. Niepokój budzi nie tylko poważny wzrost tych zdarzeń, ale ich charakter mogący sugerować, że są to incydenty nowego charakteru, których identyfikacja i w konsekwencji walka z nimi może być szczególnie utrudniona.

Z przedstawionego zestawienia liczbowego w Tabeli 1 wynika ponadto, że liczba niektórych rodzajów incydentów zmniejszyła się. Są to jednak incydenty, których znaczenie w liczbach bezwzględnych jest niewielkie, a niejednokrotnie dotyczą zaledwie jednostkowych przypadków. O rozmiarach ogólnej tendencji wzrostowej nie decyduje bowiem w żaden sposób spadek nieuprawnionego korzystania z zasobów o prawie 70% czy zmniejszenie ilości dyskredytacji i obrażania o ponad 30%.

W tej sytuacji jest oczywiste, że o ogólnej liczbie incydentów oraz o ich wzroście decydują oszustwa komputerowe.

Zmiana ilości incydentów w wartościach bezwzględnych miała również wpływ na ich strukturę, którą przedstawiono w Tabeli 2.

Wśród zaprezentowanych w Tabeli 2 incydentów dominują oszustwa komputerowe, które w roku 2021 stanowiły 86,40% wszystkich incydentów, a w roku 2022 już 88,22% w tej grupie. Na taki zasadniczy udział największy wpływ miały zdarzenia zakwalifikowane do grupy: Phishing, choć ich udział w ogólnej liczbie incydentów uległ relatywnemu zmniejszeniu.

Wzrost liczby niesklasyfikowanych oszustw komputerowych spowodował szczególnie dynamiczne zwiększenie ich udziału w ogólnej liczbie incydentów, to znaczy z niecałych 10% w roku 2021 do ponad 23% w 2022 r.

Tabela 2. Struktura incydentów obsłużonych przez CERT Polska w latach 2021 r. i 2022 r. w podziale na kategorie wg taksonomii eCSIRT.net mkVI[8]

Lp.	Typy incydentów	Liczba incydentów w 2021 r.	% w 2021 r.	Liczba incydentów w 2022 r.	% w 2022 r.
I.	Obraźliwe i nielegalne treści	311	1,05	308	0,78
	Spam	262	0,89	239	0,60
	Dyskredytacja, obrażanie	9	0,03	6	0,02
	Pornografia dziecięca, przemoc	4	0,01	0	0,00
	Niesklasyfikowane	36	0,12	63	0,16
II.	Złośliwe oprogramowanie	2 847	9,66	3 409	8,59
	Wirus	1	0,00	0	0,00
	Robak sieciowy	0	0,00	0	0,00
	Koń trojański	9	0,03	20	0,05
	Oprogramowanie szpiegowskie	0	0,00	1	0,00
	Dialer	0	0,00	0	0,00
	Rootkit	1	0,00	0	0,00
	Niesklasyfikowane	2 836	9,62	3 388	8,54
III.	Gromadzenie informacji	27	0,09	31	0,08
IV.	Próby włamań	127	0,43	121	0,30
V.	Włamania	247	0,84	354	0,89
VI.	Dostępność zasobów	148	0,50	175	0,44
VII.	Atak na bezpieczeństwo informacji	55	0,19	39	0,10
VIII.	Oszustwa komputerowe	25 472	86,40	35 009	88,22
	Nieuprawnione wykorzystanie zasobów	3	0,01	1	0,00
	Naruszenie praw autorskich	1	0,00	2	0,01
	Kradzież tożsamości, podszycie się	12	0,04	28	0,07
	Phishing	22 575	76,57	25 625	64,57
	Niesklasyfikowane	2 881	9,77	9 353	23,57
IX.	Podatne usługi	216	0,73	188	0,47
X.	Inne	33	0,11	49	0,12
RAZEM		**29 483**	**100,00**	**39 683**	**100,00**

Źródło: Raport roczny z działalności CERT Polska za lata 2021 i 2022, https://cert.pl/uploads/docs/Raport_CP_2021.pdf, ttps://cert.pl/uploads/docs/Raport_CP_2022.pdf, (24.05.2024), s. 23-24, 38-39.

[8] https://www.trusted-introducer.org/Incident-Classification-Taxonomy.pdf (dostęp: 24.05.2024).

Analizując strukturę incydentów, należy zwrócić uwagę, że oprócz oszustw komputerowych zauważalne znaczenie posiadają incydenty zakwalifikowane do grupy: Złośliwe oprogramowanie. Chociaż ich udział w ogólnej liczbie zdarzeń jest w 2022 r. mniejszy niż w 2021 r., to jednak mieści się on w przedziale od 9,62% w 2021 r. do 8,54% w 2022 r. Po raz kolejny niepokoją niesklasyfikowane elementy złośliwego oprogramowania, które w zasadzie w całości wypełniają tą grupę incydentów.

Szczegółowa analiza wykazała, że są również incydenty, które zapewne wystąpiły, ale nie zostały zgłoszone, a więc w strukturze występują jako zjawiska o wymiarze 0,00%. Dotyczy to grup złośliwego oprogramowania, takich jak: Robak sieciowy oraz Dialer.

Zespoły CERT Polska (CSIRT NASK) oraz CSIRT MON zaobserwowały w ostatnim czasie szeroko zakrojoną kampanię szkodliwego oprogramowania wymierzoną w polskie instytucje rządowe. Na podstawie wskaźników technicznych i podobieństwa do ataków z przeszłości (m.in. na podmioty ukraińskie) można powiązać tę kampanię ze zbiorem aktywności APT28, który jest kojarzony z Głównym Zarządem Wywiadowczym Sztabu Generalnego Sił Zbrojnych Federacji Rosyjskiej (GRU)[9].

Kolejnym istotnym aspektem bezpieczeństwa systemu informacyjnego w więziennictwie jest obszerna skala zagrożeń oraz rażące w skutkach próby osłabienia, zniszczenia, a nawet przejęcia informacji o strategicznym dla państwa znaczeniu przez środowiska cyberprzestępców, konkurencji, czy wywiadu obcych państw itp.

Gdy polityka informacyjna w państwie jest niewystarczająca, mogą pojawić się następujące zagrożenia:

- skuteczne odwrócenie uwagi służb więziennictwa od innych zagrożeń, które w tym czasie mogą zaistnieć;
- wywołanie destabilizacji funkcjonowania ośrodków penitencjarnych i państwa;
- wprowadzenie dezorientacji wszystkich pracowników administracji państwowej, a także organów prowadzących jak i sprawujących nadzór i kontrolę w publicznych jednostkach, w tym w ośrodkach penitencjarnych;
- znaczące umniejszenie poczucia bezpieczeństwa wśród rządzących i obywateli;

[9] Kampania APT28 skierowana przeciwko polskim instytucjom rządowym, https://cert.pl/posts/2024/05/apt28-kampania/ (24.05.2024).

- absorbowanie zwiększonej ilości służb mundurowych i służb medycznych;
- zwiększone wydatkowanie środków finansowych państwa;
- ryzyko wyjścia na wolność osób skrajnie niebezpiecznych dla otoczenia;
- wprowadzenie zamieszania, popłochu, strachu, niepewności wśród obywateli;
- nadmierne koncentrowanie uwagi mediów;
- dezorganizacja całego aparatu państwowego;
- uderzenie w społeczeństwo zakłócając dalszy rozwój, kształcenie, zatrudnienie;
- postawienie państwa w stan podwyższonej gotowości.

W globalnej kulturze polityki i prawa wszystko jest informacją, w tym również sam człowiek sprowadzany jest do obiektu w systemie teleinformatycznym[10].

Skuteczna polityka informacyjna w służbie więziennej mająca na celu zapewnienie bezpieczeństwa państwa powinna zatem obejmować takie elementy, jak:

- ochronę informacji niejawnych;
- zasady ochrony danych osobowych;
- politykę bezpieczeństwa systemu teleinformatycznego;
- zasady ochrony tajemnic państwowych;
- zapobieganie przestępstwom na szkodę państwa, szczególnie fałszerstwom i oszustom;
- zasady ochrony fizycznej i technicznej systemów informacyjnych w więziennictwie;
- utrzymanie ciągłości przekazu informacji w zakładach karnych;
- inne związane z bezpieczeństwem w ośrodkach penitencjarnych[11].

Wnioskując, polityka informacyjna w więziennictwie, czyli sposób działania, powinna opierać się o przyjęte strategie warunkujące stabilność państwa i możliwość realizacji przyjętych celów. Powszechność stosowania informacji w więzieniu nie jest elementem, który może pozostać bez kontroli. Swoboda użytkowników musi być permanentnie nadzorowana i weryfikowana z uwagi na zagrożenia kluczowych interesów państwa.

[10] J. Jankowski, *Cyberkultura prawa. Współczesne problemy filozofii i informatyki prawa*, *Globalna cyberkultura polityki i prawa,* Warszawa 2012, s. 315.
[11] J. Wójcik, *Kryminologiczne i kryminalistyczne problemy funkcjonowania wywiadu gospodarczego*, [w:] R. Borowiecki, M. Romanowska (red.), *System informacji strategicznej*, Warszawa 2021, s. 352–353.

Dane z baz CERT Polska (CSIRT NASK) oraz CSIRT MON powinny natomiast wskazywać organom władzy państwowej kierunki doskonalenia bezpieczeństwa informacyjnego w systemach penitencjarnych poprzez definiowanie zagrożenia dla państwa polskiego.

Znaczenie i sposoby realizacji polityki informacyjnej w więziennictwie dla bezpieczeństwa państwa

Każde państwo i jego naród w tym więziennictwo funkcjonuje w zmiennym otoczeniu, które posiada następujące właściwości:

- coraz większa liczba nowych, nieznanych zmian – oznacza to, że w otoczeniu, w którym funkcjonuje człowiek występuje coraz więcej nowszych i niespotykanych do danej chwili zmian, względem których nie wypracowano rozwiązań i względem których nie zostały zgromadzone żadne doświadczenia;
- wzrost intensywności otoczenia – oznaczający coraz większy wpływ elementów znajdujących się w otoczeniu na funkcjonujące w nim organizacje oraz, co jest z tym ściśle związane, na ludzi;
- szybsze tempo zmian zachodzących w otoczeniu – oznacza skrócenie czasu niezbędnego na wprowadzenie zmian;
- złożoność otoczenia – wskazująca na zwiększanie się liczby różnych elementów funkcjonujących w otoczeniu. Szybkie tempo przyrostu powoduje, że wpływ tych elementów na bezpieczeństwo państwa staje się bardzo trudny do przewidzenia[12].

Kluczowym aspektem zarządzania jest w szczególności formułowanie celów działalności, planowanie lub organizowanie przebiegu działań, pozyskiwanie i dystrybucja zasobów (zarówno ludzkich, jak i materialnych), czyli organizacja struktur i kontrola realizacji celów[13].

Poczucie bezpieczeństwa rozpatrywane w kontekście bezpieczeństwa informacji w więziennictwie, stanowi podstawę każdego autonomicznego państwa, które w dążeniu do zapewnienia stabilnej i silnej pozycji na arenie międzynarodowej chroni swych obywateli oraz zasoby przed

[12] A. Rychły-Lipińska, *Model bezpieczeństwa jednostki we współczesnym zmieniającym się otoczeniu – wstępne rozważania*, „Studia nad bezpieczeństwem" 2017, t. 2, s. 42.
[13] J. Frąszczak, *Method of Management of Personal Income Tax Changes Implemented by the Polish Deal*, „EUROPEAN RESEARCH STUDIES JOURNAL" 2022, Vol. XXV, Special Issue 3, s. 146.

zagrożeniami. Wśród tych zasobów są między innymi informacje i systemy informacyjne. Dzisiejszy obraz cyberprzestrzeni wskazuje na konieczność traktowania tej sfery jako jednej ze strategicznych z punktu widzenia obronności kraju[14].

Państwo stanowi podstawę rozwoju społeczeństwa i jest generatorem licznych informacji, które wymagają właściwej ochrony z uwagi na dobro wszystkich użytkowników całego systemu informacyjnego w więziennictwie, występującego w państwie. Ponadto, zapewnienie bezpieczeństwa informacyjnego w państwie ma również przełożenie na ogólne bezpieczeństwo jego wewnętrznych i zewnętrznych interesariuszy, co jest bardzo istotne w polityce międzynarodowej. Bezpieczeństwo informacyjne nabiera jeszcze większego znaczenia, gdy w Ukrainie toczy się wojna z Federacją Rosyjską.

Bezpieczeństwo narodowe obejmuje problematykę przeciwstawiania się wszelkim zagrożeniom zewnętrznym oraz wewnętrznym dla istnienia narodu i państwa. Polityką państwa polskiego, jaką prowadzi w trosce o własne bezpieczeństwo, jest ustalenie zbioru wartości wewnętrznych, które powinny być chronione przed zagrożeniami. Należą do nich:

- przetrwanie (biologiczne przeżycie ludzkości, narodu, jako grupy etnicznej oraz państwa, jako nielicznej jednostki politycznej);
- integralność terytorialna;
- niezależność polityczna (w sensie ustrojowym, samowładności i swobody afiliacji);
- jakość życia, na którą składają się: standard życia, szczebel rozwoju społeczno-gospodarczego, zakres praw i swobód obywatelskich, system kulturalny, stan środowiska naturalnego, możliwości i perspektywy dalszego rozwoju[15].

Jednym z kluczowych elementów, mających negatywny wpływ na bezpieczeństwo jest oczywiście dezinformacja i propaganda. Są to działania zaplanowane, rozłożone w czasie. Dezinformacja jest ukierunkowana na budowanie fałszywego obrazu rzeczywistości, z kolei propaganda

[14] A. Nowak, *Cyberprzestrzeń jako nowa jakość zagrożeń. Bezpieczeństwo Narodowe*, „Zeszyty Naukowe AON, t. 3 (92), s. 5.

[15] K. Liedel, *Bezpieczeństwo informacyjne w dobie terrorystycznych i innych zagrożeń bezpieczeństwa narodowego*, PWN, Toruń 2005, s. 12.

– na emocje. Chodzi o to, by sterować emocjami i zachowaniem danej populacji w konkretnej chwili[16].

W zależności od katalogu pojawiających się zagrożeń, bezpieczeństwo przyjmuje różne wymiary np. bezpieczeństwo informacyjne, ekonomiczne, polityczne, militarne, społeczne, ekologiczne, ideologiczne, kosmiczne. Wieloaspektowość zagrożeń bezpieczeństwa wymaga od państwa całościowego działania, we wszystkich obszarach z uwagi na jego istotę i niepodzielny charakter. Polityka bezpieczeństwa narodowego jest uwarunkowana postępem cywilizacyjnym, a wraz nim możliwościami technicznymi i technologicznymi, które ewoluują również w obszarze organizacyjnym ośrodków penitencjarnych.

W społeczeństwie informacyjnym, jak określa A. Toffler, „naczelnym czynnikiem wytwórczości i władzy człowieka" jest przepływ i wymiana informacji, które stały się fundamentem dla sprawnego funkcjonowania podmiotów, administracji wszystkich szczebli oraz życia jednostek. Fakt ten stanowi istotne wyzwanie dla bezpieczeństwa narodowego, a nowa technika to nowy obszar potencjalnego rozpoznania, walki interesów, a nawet otwartego konfliktu, zmuszające do posiadania skutecznej polityki bezpieczeństwa informacyjnego[17].

Papież Jan Paweł II w encyklice *Redemptor hominis* zwracał uwagę na fundamentalny charakter godności: „Przyjmując, iż podstawową zasadą jest stwierdzenie, że wartość godności ludzkiej jest najwyższym dobrem, do którego należy zmierzać w porządku moralnym, i że musi ono znajdować wyraz w prawodawstwie, należy przede wszystkim jasno i precyzyjnie zdefiniować prawa człowieka i nadać im kształt prawny"[18].

Aspekty bezpieczeństwa informacyjnego i cyberbezpieczeństwa zostały uwzględnione wśród działań państwa polskiego *zgodnie ze Strategią Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024*. Swym zakresem obejmuje ona działania w obrębie systemów teleinformatycznych operatorów infrastruktury krytycznej oraz uwzględnia potrzeby zapewnienia zdolności Siłom Zbrojnym Rzeczypospolitej Polskiej w układzie krajowym, sojuszniczym i koalicyjnym do prowadzenia działań militarnych w przypadku zagrożenia cyberbezpieczeństwa powodującego

[16] P. Dela, *Bankowość i Finanse. Technologie. Obawy, entuzjazm czy zwyczajnie nowa norma?*, Miesięcznik Finansowy BANK, https://bank.pl/bankowosc-i-finanse-technologie-obawy-entuzjazm-czy-zwyczajnie-nowa-norma/ (dostęp: 27.05.2024).

[17] K. Liedel, *Bezpieczeństwo informacyjne…,* s. 17.

[18] J. Paweł II, *Redemptor hominis*, https://www.vatican.va/content/john-paul-ii/pl/encyclicals/documents/hf_jp-ii_enc_04031979_redemptor-hominis.html (dostęp: 27.05.2024).

konieczność działań obronnych. Realizując *Strategię Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024*, rząd stara sie w pełni gwarantować prawo do prywatności oraz staje na stanowisku, że wolny i otwarty Internet jest istotnym elementem funkcjonowania współczesnego społeczeństwa[19].

Utrzymanie bezpieczeństwa narodowego w aspekcie informacyjnym może być realizowane według koncepcji realistycznej lub liberalnej. Koncepcja realistyczna oparta jest na następujących przesłankach:

- zwiększanie ochrony własnych systemów informacyjnych;
- stała ocena słabości systemów informacyjnych potencjalnych przeciwników, w tym takie działania, jak tworzenie możliwości wtargnięcia do ich systemów;
- przygotowanie możliwych form odpowiedzi na atak, w tym z wykorzystaniem informacyjnych, jak i konwencjonalnych wojskowych środków rażenia;
- rozwijanie metod szacowania poniesionych i/lub zadanych zniszczeń (strat informacyjnych).

W przypadku zastosowania teorii liberalnej bezpieczeństwa narodowego ochrona systemów informacyjnych polega na:

- zwiększaniu poziomu powiązań i współzależności systemów informacyjnych różnych państw w celu przeciwdziałania zagrożeniom;
- tworzeniu globalnych instytucji i porozumień zapobiegających wojnie informacyjnej[20].

Wprowadzenie równowagi pomiędzy realistyczną teorią bezpieczeństwa narodowego a teorią liberalną wymaga powołania globalnych instytucji i porozumień przeciwko działaniom wojennym oraz dbałości o ciągłą świadomość własnych słabych stron i zwiększania poziomu ochrony systemów informacyjnych[21].

K. Liedel stwierdza, że niezbędne dla bezpieczeństwa państwa jest wprowadzenie polityki informacyjnej zapewniającej ochronę istniejących systemów, ale również gwarantującej państwu i podmiotom, które chroni posiadanie, przetrwanie, i swobodę rozwoju społeczeństwa

[19] *Uchwała Rady Ministrów z 22 października 2019 r. w sprawie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024*, s. 6.

[20] T. Jemioło, P. Sienkiewicz, *Zagrożenia dla bezpieczeństwa informacyjnego państwa (identyfikacja, analiza zagrożeń i ryzyka)*, „Raport z badań AON" 2004, t. 2, s. 109.

[21] K. Liedel, *Bezpieczeństwo informacyjne…*, s. 21.

informacyjnego. Zatem pozytywne środki polityki bezpieczeństwa muszą uwzględniać to, że:

- informacja stanowi zasób strategiczny państw i organizacji XXI w.;
- informacja i wynikająca z niej wiedza oraz technologie informatyczne są podstawowym czynnikiem wytwórczym;
- większość dochodu państwa zostanie uzyskana z szeroko rozumianego sektora informacyjnego;
- procesy decyzyjne w innych sektorach gospodarki i życia społecznego uzależnione będą od systemów przetwarzania i przesyłania informacji;
- zakłócenie prawidłowości działania systemów informacyjno-sterujących nie wymaga wysokich nakładów materialnych;
- rywalizacja pomiędzy przeciwnikami przeniesie się na inną płaszczyznę walki informacyjnej.

Konkludując, obecnie walka informacyjna jest substytutem wojny. Przemawia za tym jej strategiczna rola w obecnym świecie oraz wzrastająca informatyzacja sił zbrojnych, a także zwiększające się nieustannie możliwości systemów łączności, ze wzrastającym nasyceniem wojsk nowymi technikami walki – w tym szczególnie bronią precyzyjnego rażenia[22]. Zasoby informacyjne w więziennictwie z punktu widzenia bezpieczeństwa narodowego stanowią elementy wrażliwe, a więc takie, których naruszenie zakłóca w różnym stopniu normalne funkcjonowanie państwa i tworzy zagrożenia dla jego bezpieczeństwa[23].

Podsumowanie

Reasumując, informacje zawarte w artykule i przeprowadzone analizy potwierdzają celowość i niezbędność prowadzenia przez państwo właściwej polityki informacyjnej w więziennictwie. Jest ona bowiem podstawą bezpieczeństwa państwa, utrzymania stabilizacji i społecznego spokoju. Obce służby wywiadowcze i hakerzy prześcigają się w rozpracowywaniu systemów informacyjnych w więziennictwie, a w konsekwencji zamierzają wywierać wpływ na gospodarkę, politykę, obronę granic państwa, ochronę środowiska i inne sfery życia społecznego. Stosowanie odpowiednich zabezpieczeń systemowych, wdrażanie restrykcyjnych procedur

[22] Ibidem, s. 31.
[23] K. Liedel, P. Piasecka, T. R. Aleksandrowicz, *Analiza informacji. Teoria i praktyka zarządzanie bezpieczeństwem,* Difin, Warszawa 2012, s. 28.

dostępu i użytkowania, propagowanie wiedzy na temat zagrożeń oraz natychmiastowe reagowanie na incydenty znacznie podwyższają stopień bezpieczeństwa informacyjnego.

Z przeprowadzonej analizy i oceny informacji wynikających z raportu CERT Polska wynika, że występujące obecnie zagrożenia znacząco podwyższają poziom ryzyka w obszarze bezpieczeństwa informacji. W dniu 31 maja bieżącego roku Minister Obrony Narodowej poinformował za pośrednictwem mediów, że w 2023 r. miało miejsce ponad 80 000 cyberataków. Przewiduje się, że w 2024 r. liczba ta może ulec podwojeniu. Na uwagę zasługuje ponadto spektakularny atak w ostatnim okresie na Polską Agencję Prasową, za pośrednictwem której poinformowano polskie społeczeństwo o mobilizacji, która ma nastąpić od 01 lipca br. Wiadomość jest oczywiście fałszywa, ale związki cyberataków z wojną w Ukrainie i destabilizującymi działaniami w tym zakresie Federacji Rosyjskiej są coraz bardziej widoczne.

Zjawiska związane z problematyką bezpieczeństwa informacyjnego w więziennictwie, opisywane w naukowych publikacjach i wykazane w przytoczonym w artykule materiale empirycznym potwierdzają, że w sprawowaniu władzy organy państwa nie mogą pomijać prowadzenia rzetelnej i nieustannie monitorowanej polityki informacyjnej. Zaprezentowany materiał empiryczny potwierdził, że przyjęta zaprezentowana we wstępie hipoteza o narażeniu państwa w procesie sprawowania władzy na niebezpieczeństwa związane z informacją, w pełni potwierdziła się. Dbałość o systemowe zabezpieczenia, ujawnianie cyberataków i zwalczenie przestępstw w środowisku informacyjnym w więziennictwie to działania, które stały się trwałym elementem obecnej rzeczywistości.

Bibliografia

Braman S., *Defining information policy*, „JOURNAL OF INFORMATION POLICY" 2011, Vol. 1.

Dela P., *Bankowość i Finanse. Technologie. Obawy, entuzjazm czy zwyczajnie nowa norma?*, Miesięcznik Finansowy BANK, https://bank.pl/bankowosc-i-finanse-technologie-obawy-entuzjazm-czy-zwyczajnie-nowa-norma/ (dostęp: 27.05.2024).

Frąszczak J., *Method of Management of Personal Income Tax Changes Implemented by the Polish Deal*, „EUROPEAN RESEARCH STUDIES JOURNAL" 2022, Vol. XXV, Special Issue 3.

Janczak J., Nowak A., *Bezpieczeństwo informacyjne. Wybrane problemy*, Akademia Obrony Narodowej, Warszawa 2013.

Jankowski J., *Cyberkultura prawa. Współczesne problemy filozofii i informatyki prawa*, *Globalna cyberkultura polityki i prawa*, Warszawa 2012.

Jemioło T., Sienkiewicz P., *Zagrożenia dla bezpieczeństwa informacyjnego państwa (identyfikacja, analiza zagrożeń i ryzyka)*, „Raport z badań AON" 2004, t. 2.

Kośmider T., *Determinants of the process of creating national security*, „JOURNAL OF SECURITY AND SUSTAINABILITY ISSUES" 2021, Vol. 11.

Liderman K., *Bezpieczeństwo informacyjne*. *Nowe wyzwania*, PWN, Warszawa 2017.

Liedel K., *Bezpieczeństwo informacyjne w dobie terrorystycznych i innych zagrożeń bezpieczeństwa narodowego*, Toruń 2005.

Liedel K., Piasecka P., Aleksandrowicz T.R., *Analiza informacji. Teoria i praktyka zarządzanie bezpieczeństwem*, Warszawa 2012.

Nowak A., *Cyberprzestrzeń jako nowa jakość zagrożeń. Bezpieczeństwo Narodowe*, „Zeszyty Naukowe AON, t. 3 (92).

Rychły-Lipińska A., *Model bezpieczeństwa jednostki we współczesnym zmieniającym się otoczeniu – wstępne rozważania*, „Studia nad bezpieczeństwem" 2017, t. 2.

Sienkiewicz P., *Społeczeństwo informacyjne jako system cybernetyczny*, Kraków 2004.

Witkowska M., Cholawo-Soszoch K., *Społeczeństwo informacyjne. Istota, rozwój, wyzwania*, Warszawa 2006.

Wójcik J., *Kryminologiczne i kryminalistyczne problemy funkcjonowania wywiadu gospodarczego*, [w:] Borowiecki R., Romanowska M. (red.), *System informacji strategicznej*, Warszawa 2021.

Akty prawne:

Uchwała Rady Ministrów z 22 października 2019 r. w sprawie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024.

Netografia:

https://www.trusted-introducer.org/Incident-Classification-Taxonomy.pdf (24.05.2024).

Jan Paweł II, *Redemptor hominis*, https://www.vatican.va/content/john-paul-ii/pl/encyclicals/ documents/hf_jp-ii_enc_04031979_redemptor-hominis.html (27.05.2024).

Kampania APT28 skierowana przeciwko polskim instytucjom rządowym, https://cert.pl/posts/2024/05/apt28-kampania/ (dostęp: 24.05.2024).

Raport roczny z działalności CERT Polska za lata 2021, https://cert.pl/uploads/docs/Raport_CP_2021.pdf (dostęp: 24.05.2024).

Raport roczny z działalności CERT Polska za lata 2022, https://cert.pl/uploads/docs/Raport_CP_2022.pdf (dostęp: 24.05.2024).