



Przedsiębiorcza Uczelnia

Wyższa Szkoła Pedagogiczna TWP w Warszawie



**WYŻSZA SZKOŁA PEDAGOGICZNA
TOWARZYSTWA WIEDZY Powszechniej
WYDZIAŁ NAUK SPOŁECZNYCH W WARSZAWIE**

Kierunek: politologia

Specjalność: nowe zarządzanie – public governance

Jarosław Talarowski

„Zarządzanie informacją uzyskaną w trakcie kontroli operacyjnej”

*Praca dyplomowa
napisana pod kierunkiem
dr. Marcina Bąkiewicza*

Warszawa 2010



KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY



Projekt współfinansowany ze środków Unii Europejskiej
w ramach Europejskiego Funduszu Społecznego

SPIS TREŚCI

Wstęp

Rozdział I	Informacja w organizacji.
I.1.	Informacja. Pojęcie i podział.
I. 2.	Tajemnica przedsiębiorstwa, informacja niejawna, informacja wrażliwa.
Rozdział II	Kontrola operacyjna
II.1.	Pojęcie kontroli operacyjnej.
II.2.	Zakres zastosowania kontroli operacyjnej.
II.3.	Uwarunkowania prawne kontroli operacyjnej.
Rozdział III	Zarządzanie informacją w organizacji.
III.1.	Podstawowe definicje.
III.2.	Koncepcje zarządzania informacją.
III.3.	Systemy zarządzania informacją.
Rozdział IV	Zarządzanie informacją uzyskaną w trakcie kontroli operacyjnej.
IV.1.	System zarządzania.
IV.2.	Metody weryfikacji informacji.
Zakończenie	
Bibliografia	

Wstęp

W dzisiejszej rzeczywistości globalnej, wiedza o faktycznej sytuacji organizacji jak i sytuacji jej członków, wiedza o planowanych lub nie, zdarzeniach i działaniach w bliższej lub dalszej przyszłości, pozwala na skuteczne kierowanie organizacją i ma istotne znaczenie dla jej rozwoju. Wiedza ta, mimo iż niewymierna materialnie, stanowi istotny potencjał organizacji, często jako zasób o znaczeniu strategicznym.

Źródłem tej wiedzy, są gromadzone dane, które obrazują zachodzące zjawiska i wydarzenia. Porządkowanie i analizowanie takich zbiorów pozwala na uzyskanie informacji tj. rzeczywistej wiedzy o konkretnym fakcie bądź stanie rzeczy.

Zarządzanie organizacją nierozzerwalnie związane jest z pozyskiwaniem, gromadzeniem, analizą i wykorzystaniem informacji w procesie kierowania nią samą.

Celem niniejszego opracowania jest wskazanie możliwości zastosowania zasad i metod związanych z zarządzaniem informacją w organizacji, a ściślej mówiąc w przedsiębiorstwie, w zarządzaniu informacją dotyczącą delikatnej sfery ludzkiej prywatności oraz elementarnych praw konstytucyjnych, pozyskiwaną przez uprawnione organy władzy publicznej, w celu realizacji wyłącznie zadań nałożonych na te podmioty przez powszechnie obowiązujące przepisy prawa. Pozyskiwanie, gromadzenie, analizowanie i przetwarzanie oraz wykorzystanie informacji o tak szczególnym charakterze wymaga, zarówno właściwych uregulowań formalno-prawnych jak i uregulowań czysto zarządczych, pozwalających na zgodne z prawem pozyskanie i wykorzystanie uzyskanej wiedzy.

Zasadnym jest, przybliżenie czytelnikowi, zasad i metod pozyskiwania przez organy władzy publicznej informacji o faktach i zdarzeniach oraz o zachowaniach obywateli bądź osób trzecich w szczególny sposób tj. po przez zastosowanie kontroli operacyjnej. Zarówno przez zdefiniowanie samego pojęcia „kontrola operacyjna” jak i wskazanie kręgu uprawnionych do jej prowadzenia podmiotów oraz ram prawnych tego typu czynności.

Niezbędnym, wartym zaprezentowania w niniejszym opracowaniu, jest także możliwy do wykorzystania, sposób oceny wiarygodności uzyskanej informacji w zależności od cech własnych źródła informacji, wcześniejszych doświadczeń w pracy z różnymi źródłami informacji oraz samych właściwości „organicznymi” uzyskanej informacji.

Rozdział I Informacja w organizacji.

I.1. Informacja. Pojęcie i podział.

Pojęcie „informacja” etymologicznie związane z językiem łacińskim, w którym oznaczało nadawanie postaci, formy w chwili obecnej posiada wiele ujęć znaczeniowych, w zależności od dziedziny nauki, z którą pozostaje w mniejszym lub większym związku. Podziałem najprostszym, wydaje się dychotomiczne ujęcie terminu informacja, odnoszące się do jej cech znaczeniowych tzn. jako danej, faktu, opisu rzeczywistości (ujęcie statyczne) bądź przez wskazanie jej miejsca w procesach towarzyszących jej wymianie (ujęcie dynamiczne).¹ Najszerzej znanymi koncepcjami związanymi z definiowaniem pojęcia *informacja* są dwa punkty widzenia informacji:

- *obiektywny* – który, odnosi się do nauk matematycznych i opiera się na pojęciu entropii. W tym przypadku jest ona odnoszona do właściwości fizycznych bądź strukturalno-przestrzennych obiektów.
- *subiektywny* – który, odnosi się do względnego charakteru informacji. W tym przypadku jest ona zdolnością analityczno – poznawczą umysłu.

Podejście obiektywne

Ten punkt widzenia polega na przyjęciu określonych modeli źródeł informacji oraz ustaleniu obliczeniowej miary jej ilości. Kojarzony jest najczęściej z matematyczną teorią komunikacji i postacią Claude Shannona, który jako definicję pojęcia *informacja* zaproponował określenie jej jako „ilościowa wymiana komunikatów” i mierzenie jej jako „prawdopodobieństwo zajścia jakiegoś zdarzenia”. Shannon założył, iż zdarzenia mniej prawdopodobne niosą ze sobą większy ładunek informacji. Niepewność odbiorcy przekazu, co do tego jaki symbol będzie kolejnym w konkretnym komunikacie, zwiększa zasób posiadanych przez niego informacji. Zatem w ujęciu obiektywnym informację można więc zdefiniować, jako *poziom niepewności* odbiorcy związanej z tym, co jest przekazywane.

„Wyobraźmy sobie zatem, że oglądamy pewien rysunek poprzez niewielkie okienko, które możemy przesuwac wzdłuż i w szerz obrazu. W danym momencie obserwujemy jedynie niewielki jego fragment, możemy jednak, w pewnym bardzo ograniczonym zakresie, przewidywać kolejne kolory jakie się będą pojawiać przy powolnym przesuwaniu okienka. Zatem na podstawie danego zbioru pikseli możemy szacować prawdopodobieństwo wystąpienia określonych sąsiadujących pikseli, których w danym momencie nie widzimy. Jeśli po przesunięciu okienka okaże się, że dobrze przewidzieliśmy, wówczas płynąca z tego

¹ Por. R. Zygala, *Podstawy zarządzania informacją w przedsiębiorstwie*, Wrocław 2007 r., s.27 i następne.

informacja będzie niewielka. Natomiast jeśli będziemy zaskoczeni kolejnymi kolorami, wówczas zysk informacyjny będzie znaczny.” Obiektywny punkt widzenia informacji pomija znaczenie, jakie niesie komunikat, a skupia się jedynie na jego składni. Oznacza to, że nie prowadzi się rozważań dotyczących prawdziwości czy znaczenia tego, co informacja ze sobą niesie.²

Podejście subiektywne

Ten punkt widzenia definiuje pojęcie *informacja* poprzez indywidualizację potrzeb każdego z odbiorców komunikatu. Dany zbiór informacji dla konkretnego odbiorcy może mieć fundamentalnie odmienne znaczenie i być nieużyteczny dla innego.

Informacja zatem, tak jak przedstawiono wyżej, stanowi w zależności od ujęcia, ważny element procesów decyzyjnych. Zarówno jako *obiektywny* ciąg symboli, których ilość jest wprost proporcjonalna do stanu, wprawdzie niepewnej ale jednak posiadanej wiedzy o rzeczywistości, jak i *subiektywny*, możliwy do wykorzystania wyłącznie przez konkretny podmiot potencjał ułatwiający podjęcie decyzji. Będąc elementem procesu podejmowania decyzji, stanowi ona szczególny rodzaj wartości ekonomicznej pozwalającej na realizację funkcji zarządczej wobec organizacji. Informacja o takim znaczeniu dla zarządzania określana jest mianem *informacji zarządczej* warunkującej prawidłowe planowanie, organizowania, przewodzenie i kontrolowanie. Informacja tego rodzaju może mieć, uwzględniając wyżej zaprezentowane podziały, różnego rodzaju znaczenie, i tak możemy wyróżnić:

- *informację pokrzepiającą* – odnoszącą się do bieżącej sytuacji organizacji, której celem jest upewnienie adresata, iż wszystko przebiega zgodnie z przyjętymi założeniami;
- *informację rozwojową* – oceniającą przebieg jakiegoś procesu lub stan rzeczy, której celem jest wskazanie potencjalnych zagrożeń dla podjętych działań;
- *informację ostrzegawczą* – sygnalizującą wystąpienie lub też możliwość wystąpienia zagrożeń związanych z działaniem organizacji;
- *informację planistyczną* – obrazującą stan przyszłych zjawisk lub procesów;
- *informację operacyjną* – wyznaczającą kierunek działania organizacji, pozwalająca na ocenę jej funkcjonowania w otoczeniu innych podmiotów;

² Za: P. Przybyłowicz, *Wstęp do teorii Informacji i kodowania*,
http://www.cmmsigma.eu/download/mat_info/wstep_do_teorii_informacji

- *informację opiniodawczą* – odnoszącą się do „otoczenia” organizacji, adresowaną do podmiotów zewnętrznych wobec organizacji, w znacznym stopniu *subiektywną (kontrolowaną)*, dotyczącą działania organizacji.³

Informacja mająca wpływ na proces zarządzania, niezależnie od jej znaczenia winna być oceniana na podstawie czterech kryteriów: *jakości informacji, jej aktualności, ilości i znaczenia dla potrzeb zarządzania, określanych też mianem istotności*.⁴ Istotnym jest, aby informacja była informacją odpowiedniej jakości, wnoszącą wartość dodaną do organizacji, często rekompensująca swoją przydatnością cenę jej pozyskania. Jej właściwe czasowe umiejscowienie, zarówno w odniesieniu do czasookresu, który informacja obejmuje jak i właściwy moment jej przekazania odpowiedniemu podmiotowi, ma szczególny wpływ na szybkość podejmowania decyzji w sytuacji kryzysowej. Ilość otrzymywanych informacji jak i ich znaczenie dla procesu zarządzania (istotność) wpływa na jakość funkcjonowania organizacji i pozwala na jasny podział zadań i kompetencji jej członków.

Duże znaczenie dla określenia jakości otrzymanej informacji ma też aspekt związany ze źródłem informacji tj. obiektem, faktem, zdarzeniem bądź podmiotem dającym nam wiedzę o zachodzących bądź nie procesach. Organizacje, co do zasady pozyskują informacje w drodze sformalizowanych czynności i złożonych procedur, rzadziej na drodze nieformalnych działań, niezależnie jednak od formy pozyskania informacji, musi ona odpowiadać potrzebom informacyjnym organizacji. Proces ten wymaga opanowania umiejętności wykorzystania znanego źródła informacji lub identyfikacji nowych źródeł. Pozyskiwanie informacji odbywa się zatem na dwóch płaszczyznach tj. otoczenia samej organizacji jak i struktury jej samej. Pozyskania informacji pochodzącej z otoczenia jest procesem złożonym, wymagającym zaangażowania sił i środków, często sformalizowanym i obłożonym licznymi ograniczeniami zwłaszcza natury prawnej lub etycznej. Rodzi to często pokusę by sięgnąć do źródeł nieformalnych, nieetycznych lub nielegalnych co w efekcie prowadzi do uzyskania wiedzy ale często niemożliwej do wykorzystania.

Pozyskiwanie informacji z wewnętrznych struktur organizacji jest procesem z pozoru prostszym i szybszym, odpadają bowiem ograniczenia właściwe dla pozyskiwania informacji zewnętrznej, jednak uwzględnić należy w tym wypadku brak skłonności pracowników do efektywnego dzielenia się informacjami z własną organizacją. Działania pracowników,

³ R. Zygała, *Podstawy zarządzania informacją w przedsiębiorstwie*, Wrocław 2007 r., s.36-37.

⁴ J. A.F. Stoner, R.E. Freeman, D. Gilbert, *Kierowanie*, Warszawa 1997 r., s.589-590.

zarówno jako wytwórców jak i adresatów informacji wpływają na możliwość pozyskania informacji optymalnej i najbardziej wartościowej dla organizacji.⁵

I.2. Tajemnica przedsiębiorstwa, informacja niejawna i informacja wrażliwa.

Jak wspomniano wyżej, pozyskiwanie informacji przez organizację, odbywa się na poziomie jej własnej struktury bądź poziomie jej otoczenia i w trakcie takich działań organizacja napotyka na wiele ograniczeń/barier dostępności źródeł informacji m.in.:

- *technicznych* – przez brak odpowiednich instrumentów do zapewniających dostęp do źródła, ogląd informacji jej ocenę i transmisję;
- *prawnych* – przez obowiązujące w danym systemie prawnym regulacje powszechnie obowiązujące, zakazujące dostępu do źródeł informacji lub dostęp taki reglamentujący przez tworzenie szczególnych procedur dostępu;
- *organizacyjnych* – przez brak struktur organizacyjnych umożliwiających pozyskanie i przepływ informacji;
- *ekonomicznych* – rozumianych jak brak środków, głównie finansowych pozwalających na dostęp do źródła informacji;
- *psychologicznych* – gdzie ograniczeniem/barierą jest czynnik ludzki i samoświadomość człowieka związana z jego niedoskonałością, ułomnością i niekompetencją.⁶

Prezentując zagadnienie związane z możliwością zarządzania informacją uzyskaną w trakcie kontroli operacyjnej, w sposób właściwy dla organizacji/przedsiębiorstw, w sferze naszych zainteresowań winny pozostać kwestie związane z ograniczeniem dostępu do informacji głównie na poziomie prawnym oraz techniczno-organizacyjnym. W organizacji spotykamy bowiem informacje dotyczące funkcjonowania samej organizacji, dotyczące jej członków bądź dotyczące społeczności lub struktury i zadań państwa, w którym organizacja funkcjonuje.

Odnosząc powyższe do samej organizacji, mam w trakcie jej istnienia do czynienia z informacjami stanowiącymi m. in.:

- tajemnicę przedsiębiorstwa w rozumieniu przepisów ustawy z dnia 16.04.1993 r. o zwalczaniu nieuczciwej konkurencji (Dz. U. z 2003 r. Nr 153, poz. 1503, z późn. zm.) tj. „art. 11. ust. 4. nieujawnione do wiadomości publicznej informacje techniczne, technologiczne, organizacyjne przedsiębiorstwa lub inne informacje posiadające wartość gospodarczą, co do których przedsiębiorca podjął niezbędne działania w celu zachowania ich poufności.”;

⁵ Por. R. Zygala, *Podstawy zarządzania informacją w przedsiębiorstwie*, Wrocław 2007 r., s. 39.

⁶ Ibidem.

- dotyczącymi jej członków m. in. ich danych osobowych w rozumieniu przepisów ustawy z dnia 29.08.1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926, z późn. zm.) tj. „art. 6. ust. 1. ... wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.”, a także dane „art. 27. ust. 1. ...ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz danych dotyczących skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym.”, określane mianem „danych wrażliwych”;
- wymagającymi ochrony przed nieuprawnionym ujawnieniem, jako informacjami stanowiącymi tajemnicę państwową lub służbową zgodnie z przepisami ustawy z dnia 22.01.1999 r. o ochronie informacji niejawnych (Dz. U. z 2005 r. Nr 196, poz. 1631, z późn. zm).

Możliwym jest zatem, w sytuacji zastosowania wobec organizacji czynności operacyjno-rozpoznawczych w postaci *kontroli operacyjnej*, iż organ uprawniony do jej zastosowania informację o opisanym wyżej, szczególnym charakterze uzyska i będzie się nią w ramach obowiązujących przepisów posługiwał. Tym samym zostanie zmuszony do jej weryfikacji, analizy i przetworzenia, przekazania bądź przechowania, w sposób zapewniający jej bezpieczeństwo.

Rozdział II Kontrola operacyjna

II.1. Pojęcie kontroli operacyjnej.

Prezentując pojęcie *kontrola operacyjna*, tytułem wstępu, należy przybliżyć pojęcie szersze tj. pojęcie czynności operacyjno-rozpoznawczych. Mianem czynności operacyjno-rozpoznawczych określa się w literaturze przedmiotu czynności podejmowane w celu rozpoznawania, zapobiegania i wykrywania przestępstw oraz ścigania ich sprawców. W tym miejscu podkreślić należy, iż cechą zaprezentowanej definicji jest postrzeganie tego typu czynności w relacji do ich funkcji procesowej oraz w relacji do funkcji czysto informacyjnej. Stosując bowiem kryterium celu przy stosowanie czynności operacyjno-rozpoznawczych mówimy o procesowym wykorzystaniu ich rezultatów mimo, iż nie posiadają one przymiotu czynności podejmowanych w procesie karnym.⁷ Wśród katalogu czynności zmierzających do pozyskania informacji, wymienić można m.in.:

⁷ Por. S. Zalewski, *Czynności operacyjno-rozpoznawcze jako forma realizacji zadań służ specjalnych w systemie bezpieczeństwa państwa*, Przegląd Policyjny Nr 3-4/2002, s.125-126.

- obserwację, w miejscach publicznych, ludzi, obiektów, zdarzeń i rejestrowania ich obrazu i dźwięku przy pomocy środków technicznych,
- uzyskiwanie pomocy od osób trzecich, nie będących funkcjonariuszami organów wykonujących tego typu czynności,
- uzyskiwania danych związanych z identyfikacją abonentów, zakończenia sieci lub urządzeń telekomunikacyjnych,
- uzyskiwanie danych dotyczących faktu, okoliczności i rodzaju połączeń pomiędzy określonymi urządzeniami,
- identyfikację podmiotów korzystających z usług pocztowych, dotyczących faktu, okoliczności świadczenia usług pocztowych lub korzystania z tych usług,
- niejawnie nadzorowanie wytwarzania, przemieszczania, przechowywania i obrotu przedmiotami przestępstwa.

Wyżej wymienione czynności stosowane są przez uprawnione podmioty, w celu realizacji ustawowo nałożonych zadań i prawo do ich wykonywania wynika wprost z przepisów regulujących funkcjonowanie danego podmiotu. Zastosowanie ich nie wymaga szczególnych zabiegów formalnych, szczególnie w postaci zasięgnięcia opinii bądź uzyskiwania zgody innego organu. W sytuacji wyjątkowej, gdy opisane środki okazały się bezskuteczne albo jest wysoce prawdopodobne, iż będą nieskuteczne lub nieprzydatne zarządza się - kontrolę operacyjną.

Kontrola operacyjna jest czynnością prowadzoną niejawnie i:

- zgodnie z treścią art. 19 ust. 6 ustawy z dnia 06.04.1990 r. o Policji (Dz. U. z 2007 r. Nr 43, poz. 277, z późn. zm.), polega na 1) kontrolowaniu treści korespondencji, 2) kontrolowaniu zawartości przesyłek, 3) stosowaniu środków technicznych umożliwiających uzyskiwanie w sposób niejawnie informacji i dowodów oraz ich utrwalanie, a w szczególności treści rozmów telefonicznych i innych informacji przekazywanych za pomocą sieci telekomunikacyjnych;
- zgodnie z treścią art. 27 ust. 6 ustawy z dnia 24.05.2002 r. o Agencji Bezpieczeństwa Wewnętrznego i Agencji Wywiadu (Dz. U. z 2010 r. Nr 29, poz. 154), polega na 1) kontrolowaniu treści korespondencji, 2) kontrolowaniu zawartości przesyłek, 3) stosowaniu środków technicznych umożliwiających uzyskiwanie w sposób niejawnie informacji i dowodów oraz ich utrwalanie, a w szczególności treści rozmów telefonicznych i innych informacji przekazywanych za pomocą sieci telekomunikacyjnych;

- zgodnie z treścią art. 17 ust. 5 ustawy z dnia 09.06.2006 r. o Centralnym Biurze Antykorupcyjnym (Dz. U. Nr 104, poz. 708, z późn. zm.), polega na 1) kontrolowaniu treści korespondencji, 2) kontrolowaniu zawartości przesyłek, 3) stosowaniu środków technicznych umożliwiających uzyskiwanie w sposób niejawnym informacji i dowodów oraz ich utrwalanie, a w szczególności treści rozmów telefonicznych i innych informacji przekazywanych za pomocą sieci telekomunikacyjnych;
- zgodnie z treścią art. 9e ust. 7 ustawy z dnia 12.10.1990 r. o Straży Granicznej (Dz. U. z 2005 r. Nr 234, poz. 1997, z późn. zm.), polega na 1) kontrolowaniu treści korespondencji, 2) kontrolowaniu zawartości przesyłek, 3) stosowaniu środków technicznych umożliwiających uzyskiwanie w sposób niejawnym informacji i dowodów oraz ich utrwalanie, a w szczególności obrazu, treści rozmów telefonicznych i innych informacji przekazywanych za pomocą sieci telekomunikacyjnych;
- zgodnie z treścią art. 36c ust. 4 ustawy z dnia 28.09.1991 r. o kontroli skarbowej (Dz. U. z 2004 r. Nr 4, poz. 65, z późn. zm.), polega na 1) kontrolowaniu treści korespondencji, 2) kontrolowaniu zawartości przesyłek, 3) stosowaniu środków technicznych umożliwiających uzyskiwanie w sposób niejawnym informacji i dowodów oraz ich utrwalanie, a w szczególności treści rozmów telefonicznych i innych informacji przekazywanych za pomocą sieci telekomunikacyjnych.

Z uwagi na charakter niniejszego opracowania przedstawione wyżej ustawowe definicje dotyczą wyłącznie wybranych podmiotów cywilnych, z którymi statystyczny obywatel może mieć styczność, z wyłączeniem sfery militarnej i służb typowo penitencjarnych.

II.2. Zakres zastosowania kontroli operacyjnej.

Zakres zastosowania kontroli operacyjnej odpowiada zakresowi zadań stawianych poszczególnym organom ochrony bezpieczeństwa wewnętrznego państwa i jego porządku konstytucyjnego. I tak w odniesieniu do:

Policji - kontrola operacyjna stosowana jest w celu zapobieżenia, wykrycia, ustalenia sprawców, a także uzyskania i utrwalenia dowodów ściganych z oskarżenia publicznego, umyślnych przestępstw:

- 1) przeciwko życiu, określonych w art. 148–150 Kodeksu karnego,
- 2) określonych w art. 134, art. 135 § 1, art. 136 § 1, art. 156 § 1 i 3, art. 163 § 1 i 3, art. 164 § 1, art. 165 § 1 i 3, art. 166, art. 167, art. 173 § 1 i 3, art. 189, art. 200, art. 200a, art. 204 § 4, art. 223, art. 228 § 1 i 3–5, art. 229 § 1 i 3–5, art. 230 § 1, art. 230a § 1, art. 231 § 2, art. 232, art. 245, art. 246, art. 252 § 1–3, art. 253, art. 258, art. 269, art. 280–282, art. 285 § 1, art. 286

§ 1, art. 296 § 1–3, art. 296a § 1, 2 i 4, art. 296b § 1 i 2, art. 299 § 1–6 oraz w art. 310 § 1, 2 i 4 Kodeksu karnego,

3) przeciwko obrotowi gospodarczemu, określonych w art. 297–306 Kodeksu karnego, powodujących szkodę majątkową lub skierowanych przeciwko mieniu, jeżeli wysokość szkody lub wartość mienia przekracza pięćdziesięciokrotną wysokość najniższego wynagrodzenia za pracę określonego na podstawie odrębnych przepisów,

4) skarbowych, jeżeli wartość przedmiotu czynu lub uszczuplenie należności publicznoprawnej przekraczają pięćdziesięciokrotną wysokość najniższego wynagrodzenia za pracę określonego na podstawie odrębnych przepisów,

5) skarbowych, o których mowa w art. 107 § 1 Kodeksu karnego skarbowego,

6) nielegalnego wytwarzania, posiadania lub obrotu bronią, amunicją, materiałami wybuchowymi, środkami odurzającymi lub substancjami psychotropowymi albo ich prekursorami oraz materiałami jądrowymi i promieniotwórczymi,

7) określonych w art. 8 ustawy z dnia 6 czerwca 1997 r. – Przepisy wprowadzające Kodeks karny (Dz. U. Nr 88, poz. 554 i Nr 160, poz. 1083 oraz z 1998 r. Nr 113, poz. 715),

8) określonych w art. 43–46 ustawy z dnia 1 lipca 2005 r. o pobieraniu, przechowywaniu i przeszczepianiu komórek, tkanek i narządów (Dz. U. Nr 169, poz. 1411),

9) ściganych na mocy umów i porozumień międzynarodowych;

ABW – kontrola operacyjna stosowana jest w celu rozpoznawania, zapobiegania i wykrywania przestępstw:

1) szpiegostwa, terroryzmu, naruszenia tajemnicy państwowej i innych przestępstw godzących w bezpieczeństwo państwa,

2) godzących w podstawy ekonomiczne państwa,

3) korupcji osób pełniących funkcje publiczne, o których mowa w art. 1 i 2 ustawy z dnia 21 sierpnia 1997 r. o ograniczeniu prowadzenia działalności gospodarczej przez osoby pełniące funkcje publiczne (Dz. U. z 2006 r. Nr 216, poz. 1584), jeśli może to godzić w bezpieczeństwo państwa,

4) w zakresie produkcji i obrotu towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa,

5) nielegalnego wytwarzania, posiadania i obrotu bronią, amunicją i materiałami wybuchowymi, bronią masowej zagłady oraz środkami odurzającymi i substancjami psychotropowymi, w obrocie międzynarodowym oraz ściganie ich sprawców;

CBA – kontrola operacyjna stosowana jest w celu rozpoznawania, zapobiegania i wykrywania przestępstw, a także uzyskania i utrwalenia dowodów przestępstw:

1) określonych w art. 228-231, 250a, 258, 286, 296-297, 299, 310 § 1, 2 i 4 ustawy z dnia 6 czerwca 1997 r. - Kodeks karny,

2) skarbowych, o których mowa w art. 2 ust. 1 pkt 1 lit. d, jeżeli wartość przedmiotu czynu lub uszczuplenie należności publicznoprawnej przekraczają pięćdziesięciokrotną wysokość minimalnego wynagrodzenia za pracę określonego na podstawie przepisów ustawy z dnia 10 października 2002 r. o minimalnym wynagrodzeniu za pracę (Dz. U. Nr 200, poz. 1679, z 2004 r. Nr 240, poz. 2407 oraz z 2005 r. Nr 157, poz. 1314);

Straży Granicznej – kontrola operacyjna stosowana jest w celu zapobieżenia, wykrycia, ustalenia sprawców oraz uzyskania i utrwalenia dowodów, ściganych z oskarżenia publicznego, umyślnych przestępstw:

1) określonych w art. 163 § 1, art. 164 § 1, art. 165 § 1, art. 166 § 1 i 2, art. 167, art. 168, art. 171, art. 172, art. 173 § 1, art. 258, art. 264 § 2 i 3 i art. 299 § 1 Kodeksu karnego,

2) określonych w art. 270–275 Kodeksu karnego w zakresie dokumentów uprawniających do przekraczania granicy państwowej,

3) skarbowych, o których mowa w art. 134 § 1 pkt 1 Kodeksu karnego skarbowego, jeżeli wartość przedmiotu czynu lub uszczuplenie należności publicznej przekraczają pięćdziesięciokrotną wysokość najniższego wynagrodzenia za pracę określonego na podstawie odrębnych przepisów,

4) pozostających w związku z przekraczaniem granicy państwowej lub przemieszczaniem przez granicę państwową towarów oraz wyrobów akcyzowych podlegających obowiązkowi oznaczania znakami akcyzy, jak również przedmiotów określonych w przepisach o broni, amunicji oraz o materiałach wybuchowych, a także o przeciwdziałaniu narkomanii,

5) określonego w art. 147 ustawy z dnia 13 czerwca 2003 r. o cudzoziemcach,

6) określonych w art. 228, 229 i 231 Kodeksu karnego, popełnionych przez funkcjonariuszy lub pracowników Straży Granicznej w związku z wykonywaniem obowiązków służbowych,

7) określonych w art. 229 Kodeksu karnego, popełnionych przez osoby nie-będące funkcjonariuszami lub pracownikami Straży Granicznej w związku z wykonywaniem czynności służbowych przez funkcjonariuszy lub pracowników Straży Granicznej;

8) ściganych na mocy umów międzynarodowych;

Wywiad skarbowy – kontrola operacyjna jest stosowana w celu wykrycia, ustalenia sprawców oraz uzyskania i utrwalenia dowodów przestępstw:

1) skarbowych, jeżeli wartość przedmiotu czynu lub uszczuplenie należności publicznoprawnej przekracza w dacie popełnienia czynu zabronionego pięćdziesięciokrotną

wysokość minimalnego wynagrodzenia za pracę określonego na podstawie odrębnych przepisów,

2) skarbowych, o których mowa w art. 107 § 1 Kodeksu karnego skarbowego,

3) przeciwko obrotowi gospodarczemu, powodujących szkodę majątkową, jeżeli wysokość szkody przekracza w dacie popełnienia czynu zabronionego pięćdziesięciokrotną wysokość minimalnego wynagrodzenia za pracę określonego na podstawie odrębnych przepisów,

4) przeciwko mieniu, jeżeli wartość mienia przekracza w dacie popełnienia czynu zabronionego pięćdziesięciokrotną wysokość minimalnego wynagrodzenia za pracę określonego na podstawie odrębnych przepisów,

5) przyjmowania lub wręczania korzyści majątkowej w związku z pełnioną funkcją publiczną lub funkcją związaną ze szczególną odpowiedzialnością,

6) ściąganych na mocy umów i porozumień międzynarodowych.

II.3. Uwarunkowania prawne kontroli operacyjnej.

Wszczęcie kontroli operacyjnej wymaga od organów uprawnionych do jej prowadzenia spełnienia, ściśle określonych wymogów formalnych, w celu przeprowadzenia tak szczególnych czynności, mających na celu uzyskanie stosownej informacji jeśli inne czynności operacyjno-rozpoznawcze nie przyniosły pożądanego rezultatu. Wymogi te, mają na celu, zapobieżenie stosowania tak dalece ingerujących w prawa obywateli działań, w sposób dowolny i pozbawiony nadzoru. Wyznaczają zarówno ramy przedmiotowe kontroli operacyjnej, jej ramy czasowe jak i określają obowiązki podmiotu gromadzącego w ten sposób informację w odniesieniu do nich samych.

Kontrola operacyjna, zgodnie z obowiązującymi w naszym kraju regulacjami zarządzana jest wyłącznie przez sąd powszechny w drodze stosownego wniosku konkretnego organu władzy publicznej. Proces ten prześledźmy na bazie regulacji ustawowych dotyczących Policji.

Wszczęcie kontroli operacyjnej

- kontrolę operacyjną zarządza, w drodze postanowienia właściwy miejscowo ze względu na siedzibę składającego wniosek organu Policji **sąd okręgowy**, na pisemny wniosek Komendanta Głównego Policji, złożony **po uzyskaniu pisemnej zgody** Prokuratora Generalnego albo na pisemny wniosek komendanta wojewódzkiego Policji, złożony po uzyskaniu pisemnej zgody właściwego miejscowo prokuratora okręgowego.
- w przypadkach gdy zwłoka w wydaniu postanowienia o zarządzeniu kontroli operacyjnej przez sąd okręgowy, mogłaby spowodować utratę informacji lub zatarcie albo zniszczenie dowodów przestępstwa, **Komendant Główny Policji** lub

komendant wojewódzki Policji może zarządzić, po uzyskaniu pisemnej zgody właściwego prokuratora, kontrolę operacyjną, zwracając się jednocześnie do właściwego miejscowo sądu okręgowego z wnioskiem o wydanie postanowienia w tej sprawie. W razie nieudzielenia przez sąd zgody w terminie 5 dni od dnia zarządzenia kontroli operacyjnej, organ zarządzający wstrzymuje kontrolę operacyjną oraz dokonuje protokolarnego, komisyjnego zniszczenia materiałów zgromadzonych podczas jej stosowania.

Wymagania formalne co do wniosku o zarządzenie kontroli operacyjnej

Wniosek właściwego organu Policji, o zarządzenie przez sąd okręgowy kontroli operacyjnej powinien zawierać w szczególności:

- numer sprawy i jej kryptonim, jeżeli został jej nadany,
- opis przestępstwa z podaniem, w miarę możliwości, jego kwalifikacji prawnej,
- okoliczności uzasadniające potrzebę zastosowania kontroli operacyjnej, w tym stwierdzonej albo prawdopodobnej bezskuteczności lub nieprzydatności innych środków,
- dane osoby lub inne dane, pozwalające na jednoznaczne określenie podmiotu lub przedmiotu, wobec którego stosowana będzie kontrola operacyjna, ze wskazaniem miejsca lub sposobu jej stosowania,
- cel, czas i rodzaj prowadzonej kontroli operacyjnej.

Czas trwania kontroli operacyjnej

- kontrolę operacyjną zarządza się na okres nie dłuższy niż 3 miesiące,
- sąd okręgowy może, na pisemny wniosek Komendanta Głównego Policji lub komendanta wojewódzkiego Policji, złożony po uzyskaniu pisemnej zgody właściwego prokuratora, na okres nie dłuższy niż kolejne 3 miesiące, wydać postanowienie o **jednorazowym** przedłużeniu kontroli operacyjnej, jeżeli nie ustały przyczyny zarządzenia tej kontroli,
- w uzasadnionych przypadkach, gdy podczas stosowania kontroli operacyjnej pojawiają się nowe okoliczności istotne dla zapobieżenia lub wykrycia przestępstwa albo ustalenia sprawców i uzyskania dowodów przestępstwa, sąd okręgowy, na pisemny wniosek Komendanta Głównego Policji, złożony po uzyskaniu pisemnej zgody Prokuratora Generalnego, może wydać postanowienie o kontroli operacyjnej przez czas oznaczony również po upływie okresów, o których mowa wyżej.

Zakończenie kontroli operacyjnej

Kontrola operacyjna powinna być zakończona **niezwłocznie**, po ustaniu przyczyn jej zarządzenia, najpóźniej jednak z upływem okresu, na który została wprowadzona. Organ policji, wnioskujący o zarządzenie kontroli operacyjnej, informuje właściwego prokuratora o wynikach kontroli operacyjnej po jej zakończeniu, a na jego żądanie również o przebiegu tej kontroli.

Rezultaty kontroli operacyjnej

- w przypadku uzyskania dowodów pozwalających na wszczęcie postępowania karnego lub mających znaczenie dla toczącego się postępowania karnego, Komendant Główny Policji lub komendant wojewódzki Policji przekazuje właściwemu prokuratorowi wszystkie materiały zgromadzone podczas stosowania kontroli operacyjnej, w razie potrzeby z wnioskiem o wszczęcie postępowania karnego,
- zgromadzone podczas stosowania kontroli operacyjnej materiały niezawierające dowodów pozwalających na wszczęcie postępowania karnego przechowuje się po zakończeniu kontroli przez okres 2 miesiące, a następnie dokonuje się ich protokolarnego, komisyjnego zniszczenia. Zniszczenie materiałów zarządza organ Policji, który wnioskował o zarządzenie kontroli operacyjnej.

Rozdział III Zarządzanie informacją w organizacji.

III.1. Podstawowe definicje.

Tak jak wspomnieliśmy na wstępie, iż zarządzanie organizacją nierozzerwalnie związane jest z pozyskiwaniem, gromadzeniem, analizą i wykorzystaniem informacji w procesie kierowania nią samą, tak należy również podkreślić, iż sam fakt pozyskania i przetworzenia informacji nie może być celem samym w sobie. Istotnym jest wykorzystanie wartości jakie każda informacja ze sobą niesie w celu rozwoju organizacji. Poszukując jednej definicji terminu „zarządzanie informacją” można przyjąć, iż jest to „świadome postępowanie ludzi, zmierzające w kierunku optymalizacji roli informacji w osiągnięciu celów przez organizację”.⁸ R. Zygała prezentuje również propozycje definiowania tego pojęcia przez innych autorów, gdzie termin ten oznacza:

- planowanie polityki informacyjnej całej organizacji, rozwój i utrzymanie systemów zintegrowanych i usług, optymalizacje przepływów informacji i wykorzystanie

⁸ R. Zygała, *Podstawy zarządzania informacją w przedsiębiorstwie*, Wrocław 2007 r., s. 46.

przełomowych technologii do wymagań funkcjonalnych użytkowników końcowych, bez względu na ich status i rolę w organizacji,

- cykl procesów, które wspierają uczenie się organizacji,
- planowanie, budżetowanie, przetwarzanie i kontrolowanie informacji w całym jej cyklu życia,
- ustrukturalizowany zestaw procesów pracy, które określają sposób w jaki przedsiębiorstwa pozyskują, dystrybuują i używają informacji,
- reprezentowanie przedsiębiorstwa przez informację.⁹

III.2. Koncepcje zarządzania informacją.

Proces zarządzania informacją rozpoczyna swoje działanie w chwili powstania samej informacji. Pierwszym elementem procesu jest pojawienie się stanu barku stabilizacji. Nowo otrzymana informacja wywołuje określone reakcje organizacji i jej systemów informacyjnych, zmieniając je, w efekcie tworząc kolejną informację. Organizacja w reakcji na zaistniałą niestabilność systemu poszukuje rozwiązań optymalnych dla podejmowania jak najwłaściwszych decyzji. Sekwencja działań podejmowanych przez organizację i jej członków, tworzenie relacji w ramach samej organizacji i poza nią tworzy pewien powtarzalny model/wzorzec zachowań związanych z zarządzaniem informacją.

R. Zygała podjęła, za T. Davenportem, iż taki model zachowań organizacji powinien obejmować:

- identyfikację potrzeb informacyjnych,
- akwizycję informacji,
- organizowanie i magazynowanie informacji,
- produkty i usługi informacyjne,
- dystrybucję informacji,
- użycie informacji.

Przytacza także, następujące propozycje modeli rozwiązań:

ekologię informacji – zorientowaną na otoczenie organizacji, jej klientów. Wypracowanie przez organizację strategii informacyjnej rozumianej jako element strategii organizacji z jednej strony, z drugiej zaś jako wytyczna jej środowiska informacyjnego. Nadanie kluczowej roli kulturze informacyjnej w organizacji rozumianej jako skłonność do dzielenia się informacją;

⁹ Ibidem.

informacyjny federalizm – gdzie informacja ogólna dedykowana jest władzy centralnej. Jej lokalne komponenty dysponują wysokim poziomem autonomii i tam przebiegają główne procesy informacyjne oparte o dialog i wymianę informacji;

informacyjny feudalizm – gdzie dominującą rolę odgrywają kierownicy poszczególnych komórek organizacyjnych. Ich potrzeby są najważniejsze i do nich dostosowują przebieg procesów informacyjnych;

informacyjna monarchia – gdzie proces informacyjny kierowany jest w całej organizacji wyłącznie przez jeden podmiot, który określa jaka informacja jest ważna, co odgrywa w niej rolę kluczową i jak ma być ona interpretowana;

informacyjna anarchia – rozumiana jako stan, w którym każdy radzi sobie sam, partykularnie gromadząc informacje, tworząc własne bazy danych i własne struktury informacyjne.

Zaprezentowane modele wykorzystują do zarządzania informacją jednak jest ona traktowana bardziej jako narzędzie niż cel sam w sobie.¹⁰

III.3. Systemy zarządzania informacją.

Systemy zarządzania informacją (SI) pozwalają organizacji sprawnie funkcjonować i reagować na zmieniającą się rzeczywistość. Najczęściej spotykanymi elementami, charakterystycznymi dla SI, jest model oparty o składowe: **wejście-proces-wyjście**, posiadający wiele poziomów pozwalającą użytkownikowi na przetwarzanie, za ich pomocą informacji. Od pojęcia SI należy odróżnić pojęcie systemu informatycznego, jako wydzielonej, wspartej komponentem technologicznym, częścią systemu informacyjnego.

Za J. Kisielnickim i H. Sroką¹¹, stosując kryterium poziomu zaawansowania technicznego można wyróżnić cztery generacje systemów informatycznych:

system transakcyjny - oparty na pełnych, porównywalnych i wiarygodnych danych, które przetwarzają za pomocą prostych modeli;

system informacji kierowniczej - wykorzystujący nie zawsze pełne i porównywalne dane, które przetwarza wykorzystując modele oparte na równaniach i przepływach międzygałęziowych;

system wspomagania decyzji – opierający się na danych niepełnych i obarczonych błędem o znanym prawdopodobieństwie, które przetwarzają w modelach optymalizacyjnych lub symulacyjnych;

system ekspertowy - przetwarzający niepełne i często sprzeczne informacje pochodzące z różnych źródeł, które przetwarzane są metodami heurystycznymi i logicznymi.

¹⁰ Ibidem. s. 48-55

¹¹ J. Kisielnicki, H. Sroka, Systemy informacyjne biznesu. Informatyka dla zarządzania, Warszawa 2005, s. 27.

Składowe systemu informacyjnego

Wskazane wyżej, składowe SI mimo, iż ograniczone o trzech obszarów wykazują daleko idącą złożoność i specyfikę.

Układ wejścia – może przybierać formę danych i informacji wejściowych, kanałów informacyjnych i nośników informacji;

Układ przetwarzania (proces) – to gromadzenie danych na nośnikach, klasyfikacja i porządkowanie informacji, ich przetwarzanie i przechowywanie;

Układ wyjścia – najbardziej zorganizowany składnik SI, warunkujący zaspokojenie potrzeb informacyjnych członków organizacji.¹²

Cech systemu informacyjnego zarządzania (SIZ)¹³

SI winien odpowiadać na potrzeby organizacji, w której funkcjonuje i gwarantować po zakończeniu procesu **wejście-przetworzenie-wyjście**, odpowiedniej jakości wiedzę.

Za najważniejsze cechy SIZ można przyjąć:

Celowość – SIZ służy osiągnięciu definiowalnych i mierzalnych celów organizacji,

Wiarygodność – informacje pozyskane z SIZ pochodzą z rzetelnego i prawdziwego źródła, a metoda pozyskania, oceny i przekazywania oraz przechowywania jest sprawdzalna,

Dostępność – rozumiana jako techniczna możliwość otrzymania informacji jak i uprawnienie do jej otrzymania, zgodnie z zasadą **niezbędnej wiedzy**,

Aktualność – informacja czasu rzeczywistego, odzwierciedlająca faktycznie zachodzące procesy, bez cechy historyczności informacji,

Efektywność – koszt utrzymania SIZ równoważony jest przez korzyści płynące z jego funkcjonowania,

Wydaźność – SIZ zapewnia stałą ilość informacji, przy zachowaniu wymaganego poziomu pozostałych kryteriów,

Niezawodność – gwarantującą stabilność pracy SIZ, przy zachowaniu wymaganego poziomu pozostałych kryteriów,

Kompleksowość – SIZ zaspokaja potrzeby różnych użytkowników i dostosowuje się zmiennych do warunków jego użytkowania,

Bezpieczeństwo – SIZ gwarantuje nienaruszalność zasobów i procedur, przy zapewnieniu, że dane nie zostaną utracone a nieupoważnione podmioty nie będą miały do nich dostępu,

Przyjazność – SIZ przejrzystości i w uproszczony sposób ułatwia opanowania procedur przez użytkownika.

¹² R. Zygała, *Podstawy zarządzania informacją w przedsiębiorstwie*, Wrocław 2007 r., s. 71-73.

¹³ *Ibidem*. s. 74-76.

SIZ podzieliliśmy wyżej na, ze względu na zaawansowanie technologiczne komponentu informatycznego można dokonać także podziału ze względu na kryterium funkcjonalne, wynikające ze zróżnicowania adresatów SIZ jako przeznaczenie ich do działania w zróżnicowanych obszarach gospodarki.

Systemy te mogą wspierać pracę typowo biurową (OAS – office automation system), gdzie istotnym jest edycja tekstu, zarządzanie czasem i korespondencja bądź wspierać wysokokwalifikowanych specjalistów (KWS – knowledge work system). Mogą też funkcjonować jako wsparcie operacyjne w bieżącym działaniu organizacji (TPS – transaction processing system) lub wspierać proces decyzyjny kierownictwa (MIS – management information system, ESS – executive support system).

Rozdział IV Zarządzanie informacją uzyskaną w trakcie kontroli operacyjnej.

IV.1. System zarządzania.

Pozyskanie informacji w drodze kontroli operacyjnej, mimo iż jest to, jak wspomniano wyżej, czynność poza procesowa, to jest jednak gromadzona, przetwarzaniu i przekazywaniu w celu wykrywania i ścigania sprawców przestępstw oraz zapobiegania i zwalczania przestępczości. Ustawodawca uznał za stosowne, aby informacje te gromadzone, przetwarzane i przekazywane były w sposób skoordynowany, reglamentowany z zachowaniem zasad bezpieczeństwa w specjalnie stworzonym systemie.

Krajowe Centrum Informacji Kryminalnych

Centrum, powołane do życia ustawą z dnia 06.07.2001 r. o gromadzeniu, przetwarzaniu i przekazywaniu informacji kryminalnych (Dz. U. z 2010 r. Nr 29, poz. 1530) funkcjonuje jako komórka organizacyjna w Komendzie Głównej Policji, przy pomocy której Komendant Główny Policji wykonując zadania określone ww. ustawą.

Zgodnie z brzmieniem jej przepisów:

- informacje kryminalne – **to określone dane dotyczące spraw będących przedmiotem czynności operacyjno-rozpoznawczych**, wszczętego lub zakończonego postępowania karnego, w tym postępowania w sprawach o przestępstwa skarbowe, oraz dotyczące innych postępowań lub czynności prowadzonych na podstawie ustaw, istotnych z punktu widzenia czynności operacyjno-rozpoznawczych lub postępowania karnego,
- gromadzenie informacji kryminalnych – to wprowadzanie do bazy danych informacji kryminalnych otrzymanych od podmiotów zobowiązanych, przekazanych w odpowiedzi na zapytanie lub z własnej inicjatywy,

- przetwarzanie informacji kryminalnych – to czynności związane z utrwalaniem, przechowywaniem, wyszukiwaniem, analizowaniem i usuwaniem informacji kryminalnych. Przetwarzania informacji kryminalnych dokonuje się przy wykorzystaniu urządzeń i systemów informatycznych i teleinformatycznych, kartotek, skorowidzów, ksiąg, wykazów i zbiorów ewidencyjnych.,

ponadto ustawa reguluje czynności związane z:

- usuwaniem informacji kryminalnych – tj. trwałym zniszczeniem informacji kryminalnych w bazach danych,
- analizą informacji kryminalnych – tj. zestawianiem cech, części lub składników informacji kryminalnych, a także wniosków z nich wynikających.

Zakres gromadzonych danych

Zakres gromadzonych informacji kryminalnych obejmuje następujące dane:

- datę i miejsce popełnienia przestępstwa,
- rodzaj popełnionego przestępstwa i kwalifikację prawną czynu,
- sygnaturę akt, pod którą zostały zarejestrowane czynności lub postępowanie,
- nazwę organu lub jednostki organizacyjnej prowadzącej czynności lub postępowanie oraz informację o sposobie nawiązania kontaktu z tym organem lub jednostką organizacyjną,
- informacje o:
 - osobach, przeciwko którym prowadzone jest postępowanie karne, w tym postępowanie w sprawach o przestępstwa skarbowe, lub w stosunku do których prowadzone są czynności operacyjno-rozpoznawcze,
 - przedmiotach wykorzystanych do popełnienia przestępstwa lub utraconych w związku z przestępstwem,
 - przedsiębiorcach, spółkach cywilnych, fundacjach, stowarzyszeniach, co do których zachodzi uzasadnione podejrzenie, że zostały wykorzystane w celu popełnienia przestępstwa, zgromadzone w rejestrach prowadzonych na podstawie odrębnych przepisów,
 - numerach rachunków bankowych lub rachunków papierów wartościowych, co do których zachodzi uzasadnione podejrzenie, że zostały wykorzystane w celu popełnienia przestępstwa lub że gromadzone są na nich środki pochodzące z przestępstwa,
 - innych postępowaniach lub czynnościach prowadzonych na podstawie ustaw, istotnych z punktu widzenia czynności operacyjno-rozpoznawczych lub

postępowania karnego, w tym postępowania w sprawach o przestępstwa skarbowe.

Informacje o osobach, przeciwko którym prowadzone jest postępowanie karne, w tym postępowanie w sprawach o przestępstwa skarbowe, lub w stosunku do których prowadzone są czynności operacyjno-rozpoznawcze, obejmują:

- dane personalne:

- nazwisko,
 - imiona,
 - imiona i nazwiska poprzednie,
 - imiona rodziców i nazwisko rodowe matki,
 - datę i miejsce urodzenia,
 - płeć,
 - pseudonim,
 - adres miejsca zameldowania,
 - adres miejsca pobytu,
 - cechy dokumentów tożsamości: rodzaj dokumentu, datę wystawienia dokumentu, organ wystawiający dokument, numer, serię dokumentu,
 - numer ewidencyjny Powszechnego Elektronicznego Systemu Ewidencji Ludności (PESEL) lub obywatelstwo, w przypadku cudzoziemca nieposiadającego numeru PESEL,
 - numer identyfikacji podatkowej NIP,
 - numer identyfikacyjny REGON;
- inne dane pozwalające na określenie tożsamości osoby, a w szczególności rysopis i przynależność do grupy przestępczej.

Podmioty uprawnione i zobowiązane

Podmiotami uprawnionymi, w zakresie swoich zadań ustawowych, do otrzymywania informacji kryminalnych z Centrum, zwanymi „podmiotami uprawnionymi”, są:

- 1) organy prokuratury,
- 2) organy Policji,
- 2) Centralne Biuro Antykorupcyjne,
- 3) Agencja Bezpieczeństwa Wewnętrznego,
- 4) organy Straży Granicznej,
- 5) organy celne,
- 6) organy podatkowe,

- 7) organy kontroli skarbowej,
- 8) wywiad skarbowy,
- 9) Biuro Ochrony Rządu,
- 10) Żandarmeria Wojskowa,
- 11) organy informacji finansowej,
- 12) organy administracji publicznej właściwe w sprawach obywatelstwa, cudzoziemców i repatriacji,
- 13) Szef Służby Kontrwywiadu Wojskowego oraz Szef Służby Wywiadu Wojskowego,
- 14) Przewodniczący Komisji Nadzoru Finansowego lub upoważniony przez niego przedstawiciel,
- 15) Dyrektor Generalny Lasów Państwowych, dyrektorzy regionalnych dyrekcji Lasów Państwowych, nadleśniczowie oraz Główny Inspektor Straży Leśnej,
- 16) dyrektorzy parków narodowych.

Podmiotami zobowiązanymi do przekazywania informacji kryminalnych do Centrum są ww. podmioty uprawnione oraz:

- 1) organy administracji rządowej lub organy samorządu terytorialnego właściwe w sprawach ewidencji ludności, Powszechnego Elektronicznego Systemu Ewidencji Ludności, ewidencji paszportowych, ewidencji wydanych i unieważnionych dowodów osobistych, ewidencji wojskowej, centralnej ewidencji pojazdów, centralnej ewidencji kierowców, rejestracji pojazdów, rejestru cywilnych statków powietrznych, rejestru administracyjnego polskich statków żeglugi śródlądowej, polskiego rejestru jachtów, polskiego rejestru okrętowego, nadzoru geodezyjnego i kartograficznego, administracji geodezyjnej i kartograficznej, ewidencji gruntów i budynków, rejestracji stanu cywilnego, publicznej służby zatrudnienia lub pomocy społecznej,
- 2) sądy prowadzące Krajowy Rejestr Sądowy, księgi wieczyste i rejestr zastawów,
- 3) organy Inspekcji Ochrony Środowiska,
- 4) organy Państwowej Straży Pożarnej,
- 5) organy Zakładu Ubezpieczeń Społecznych,
- 6) Prezes Kasy Rolniczego Ubezpieczenia Społecznego,
- 7) Komisja Nadzoru Finansowego,
- 8) Państwowa Straż Rybacka,
- 9) Prezes Urzędu Ochrony Konkurencji i Konsumentów,
- 10) Prezes Głównego Urzędu Statystycznego i dyrektorzy urzędów statystycznych w zakresie prowadzonych przez nich krajowych rejestrów urzędowych,

- 11) dyrektor Biura Informacyjnego Krajowego Rejestru Karnego,
 - 12) dyrektorzy jednostek organizacyjnych Służby Więziennej,
 - 13) Państwowa Straż Łowiecka
- zwanych „podmiotami zobowiązanymi”.

IV.2. Metody weryfikacji informacji.

Zgodnie z ustawą 06.07.2001 r. o gromadzeniu, przetwarzaniu i przekazywaniu informacji kryminalnych Komendant Główny Policji, jako organ administracji rządowej właściwy w sprawach gromadzenia, przetwarzania i przekazywania informacji kryminalnych do zadań którego, jako Szefem Krajowego Centrum Informacji Kryminalnych, należy w szczególności opracowywanie analiz informacji kryminalnych. Poniżej przedstawione zostaną dwie metody dokonywania analizy informacji otrzymywanych w drodze czynności operacyjno-rozpoznawczych, w tym także kontroli operacyjnej.

4X4

System ten wprowadzony w Polsce w 2003 r., a wzorowany na rozwiązaniach obowiązujących w Unii Europejskiej bazuje na tzw. Meldunku Informacyjnym tj. informacji każdorazowo sporządzanej w przypadku uzyskania przez policjanta informacji mogących przyczynić się do zapobieżenia, rozpoznania i wykrycia przestępstw, ustalenia sprawców lub metod popełniania przestępstw albo do rozpoznania organizacji grup przestępczych. Polega on na ocenie **wiarygodności źródła informacji**, a wyniki tej oceny zaznaczane są w odpowiednich polach formularza meldunku, w formie następujących kodów:

- kod "A" - oznacza brak wątpliwości co do wiarygodności źródła informacji,
- kod "B" - oznacza, że informacja pochodzi ze źródła, które w większości przypadków dotychczas było wiarygodne,
- kod "C" - oznacza, że informacja pochodzi ze źródła, które w większości przypadków dotychczas nie było wiarygodne,
- kod "X" - oznacza, że informacja pochodzi z nowego źródła, którego wiarygodność nie jest znana, bo źródło nie było sprawdzane lub sprawdzenie nie jest możliwe. (EUROPOL w tym przypadku używa kodu „D”)¹⁴

Następnie sporządzający meldunek informacyjny dokonuje **oceny prawdziwości i sposobu uzyskania informacji** przekazywanej tym meldunkiem, a wyniki tej oceny wpisuje w odpowiednim polu formularza meldunku w formie następujących kodów:

¹⁴ Por. T. Noszczyński, *System oceny informacji - 4X4*, Gazeta Policyjna Nr 12/2003, s.6.

- kod "1" - oznacza, że informacja jest oceniana jako prawdziwa przez wprowadzającego,
- kod "2" - oznacza, że fakty wskazane w informacji są znane bezpośrednio źródłu przekazującemu informację,
- kod "3" - oznacza, że fakty wskazane w informacji nie są znane bezpośrednio źródłu przekazującemu informację, ale zostały potwierdzone przez inne źródła informacji,
- kod "4" - oznacza, że fakty wskazane w informacji nie są znane bezpośrednio źródłu przekazującemu informację i nie mogą być sprawdzone przez inne aktualnie dostępne źródła informacji.

Ostatnim elementem analizy meldunku informacyjnego jest wprowadzenie w odpowiednim polu formularza dokumentu (MI) dopuszczalnego sposobu wykorzystania informacji, w formie następujących kodów:

- kod "H1" - oznacza, że informacja nie może być wykorzystana w postępowaniu karnym bezpośrednio, bez uprzedniego dowodowego przetworzenia w sposób określony przepisami postępowania karnego,
- kod "H2" - oznacza, że informacje można udostępnić tylko po uprzednim uzyskaniu zgody policjanta, który sporządził dokument źródłowy lub jego bezpośredniego przełożonego,
- kod "H3" - oznacza, że wykorzystanie informacji podlega ograniczeniom innym niż wymienione wyżej możliwości.

Kod "H1" wpisuje się do każdego dokumentu źródłowego wprowadzanego do systemu, a kody "H2" i "H3" dodatkowo w przypadku uznania, że zachodzą określone powody do dalej idącego ograniczenia sposobu wykorzystania informacji.

Kodem "H2" określa się sposób wykorzystania informacji w przypadku konieczności szczególnej ochrony przebiegu prowadzonych czynności operacyjno-rozpoznawczych przed dekonspiracją, zapewnienia właściwego toku postępowania karnego albo ochrony zdrowia i życia policjantów lub innych osób uczestniczących w czynnościach służbowych.

Ograniczenie sposobu wykorzystania informacji kodem "H2" lub "H3" obowiązuje przez okres trzech miesięcy od daty sporządzenia dokumentu źródłowego. Okres ten może być przedłużany o kolejne trzymiesięczne okresy po przedłożeniu pisemnego wniosku.¹⁵

*Aguillar- Spinelli two-prong test*¹⁶

¹⁵ Por. Decyzja Nr 773 KGP z dnia 19 grudnia 2008 r. w sprawie prowadzenia w Policji zestawu zbiorów informacji „System Informacji Operacyjnych”, Dz. Urz. KGP z 2009 r. Nr 1, poz. 3.

Ocena wiarygodności informacji prowadzona jest w tym przypadku, w oparciu o badanie dwóch kwestii:

Po pierwsze – wiarygodności źródła informacji. Przy czym za „wiarygodną” uznaje się informację pochodząca od funkcjonariusz policji, pokrzywdzonego bądź „uczciwego, zaniepokojonego obywatela” którego dane są znane policji. Tym samym informacja, której źródłem jest przestępca uznawana jest za niewiarygodna i wymaga dodatkowej weryfikacji w drodze tzw. *corroboration*. Instytucja ta polega na sprawdzeniu czy informacje przestępcy są wiarygodne przez obserwację osoby podejrzanej. Jeśli zachowuje się on w sposób podany przez informatora, informację tę, można przyjąć za wiarygodną.

Po drugie – ustalenie podstawy wiedzy informatora o zdarzeniu tj. czy wie on o czym mówi np. był naocznym świadkiem bądź zna zdarzenie ze słyszenia.

Zakończenie.

Zastosowanie metod i technik zarządzania właściwych dla gospodarczej sfery aktywności człowieka, w odniesieniu do szczególnych form działania organów władzy publicznej, pozwala z jednej strony na usprawnienie funkcjonowania „aparatu władzy” a z drugiej wymusza na podmiotach publicznych, sięgających po te metody pewnego „wysiłku intelektualnego, dzięki któremu taka adaptacja będzie możliwa i efektywna. I ta cecha systemu zarządzania informacja uzyskana w trakcie kontroli operacyjnej wydaje się najważniejszą. Wraz z komponentem bezpieczeństwa/dostępności zapewnia ona jego właściwe funkcjonowanie. Odnosząc tę opinię do opisanego wyżej Krajowego Systemu Informacji Kryminalnej, można posłużyć się oceną systemu wystawioną przez prof. B. Hołysta, zdaniem którego przejrzystość komponentów i możliwość współpracy z systemami opartymi na dowolnych standardach to przyszłość rozwiązań w tym zakresie.¹⁷

¹⁶ A. Taracha, *Czynności operacyjno-rozpoznawcze. Aspekty kryminalistyczne i prawnodowodowe.*, Lublin 2006, s. 242-243.

¹⁷ B. Hołyst, *Kryminalistyka*, Warszawa 2007 r., s. 1026 i nast.

Bibliografia

1. B. Hołyst, Kryminalistyka, Warszawa 2007 r.,
2. J. Kisielnicki , H. Sroka, Systemy informacyjne biznesu. Informatyka dla zarządzania, Warszawa 2005,
3. T. Noszczyński, System oceny informacji - 4X4, Gazeta Policyjna Nr 12/2003,
4. J.A.F. Stoner, R.E. Freeman, D. Gilbert, Kierowanie, Warszawa 1997 r.,
5. P. Przybyłowicz, Wstęp do teorii Informacji i kodowania, http://www.cmmsigma.eu/download/mat_info/wstep_do_teorii_informacji,
6. A. Taracha, Czynności operacyjno-rozpoznawcze. Aspekty kryminalistyczne i prawnodowodowe., Lublin 2006,
7. S. Zalewski, Czynności operacyjno-rozpoznawcze jako forma realizacji zadań służb specjalnych w systemie bezpieczeństwa państwa, Przegląd Policyjny Nr 3-4/2002,
8. R. Zygała, Podstawy zarządzania informacją w przedsiębiorstwie, Wrocław 2007 r.