

ŽVALGYBINIŲ METODŲ PANAUDOJIMAS SIEKIANČIŲ ĮGYTI PRANAŠUMŲ KONKURENCINĖJE KOVOJE

Vaidas Gaidelys

Kauno technologijos universitetas, Lietuva, Vaidas.Gaidelys@ktu.lt

Anotacija

Žvalgybos specialistų teigimu, žlugus Tarybų Sąjungai buvusiose postsovietinėse respublikose daugelis specialiosiose tarnybose dirbusių specialistų, (informacijos rinkimo bei analizės, operatyvinių darbuotojų, analitikų, IT specialistų, technikų ir kt.) buvo atleisti dėl etatų mažinimo, tarnybų išformavimo, suėjus pensiniam amžiui (dažnai užtenka 20-ies metų darbo stažo) ir dėl kitų priežasčių. Greitai stambios verslo korporacijos pamatė galimybę pasinaudoti minėtų specialistų sukaupta patirtimi bei žiniomis, todėl buvo pradėtos steigti vindikacijos, saugos ir kitos tarnybos ar atskiros konsultacinės kompanijos. Kai kurių mokslininkų teigimu stambiausios pasaulio korporacijos naudoja konkurencinės žvalgybos teikiama privalumais, tikslu įgyti konkurencinį pranašumą.

Bendrovei nusprendusiai investuoti į informacijos apie konkurentų veiksmus ir planus rinkimą bei analizę kyla klausimas apie naudą, kurią galėtų gauti bendrovė. Todėl daugelis mokslininkų teigia, kad galima verslo informacinio saugumo nauda yra: kompanijos lėšų taupymas, pelno augimas, reputabilumas, pagalba konkurencinėje kovoje, galimybės plėsti rinkas (Stephen, 2004).

Raktažodžiai: Žvalgybiniai metodai, informacijos šaltiniai, informacijos analizė.

Išvadas

Atsižvelgiant į pasaulinę verslo korporacijų praktiką pastebėta, kad daugelis stambių verslo korporacijų nepriklausomai nuo jų veiklos vietos geografinė prasme steigia korporacijose konkurencinės žvalgybos arba jų funkcijas visas ar iš dalies atliekančius padalinius (Prescott, 2000). Būtina atsižvelgti į tai, kad konkurencinės žvalgybos specialistas turi turėti ne tik ekonominių žinių, suvokti ekonominius procesus, bet turėti ir pakankamas teises žinias, tame tarpe išmanyti Lietuvos Respublikoje bei už jos ribų galiojančius teisės aktus (Operatyvinės veiklos įstatymą, LR Baudžiamąjį kodeksą, LR Baudžiamojo proceso kodeksą, LR Civilinį kodeksą, LR Administracinės teisės kodeksą ir kt.). Taip pat žinoti operatyvinės veiklos metodus, būdus ir galimybes. Tokia informacija bei patirtimi dažniausiai disponuoja buvę specialiųjų tarnybų pareigūnai, kuriuos pagal veiklos pobūdį galima būtų suskirstyti į sekančias grupes:

- Policijos įstaigų pareigūnai;
- Kovos su korupcija įstaigų pareigūnai;
- Mokesčių tarnybų pareigūnai;
- Valstybės saugumo pareigūnai;
- Kitų operatyvinių tarnybų pareigūnai.

Pagal veiklos pobūdį verslo struktūrose kuriose siekiama įdiegti ne tik saugos (vindikacijos) padalinį, bet ir turėti savo konkurencinės žvalgybos strategus, bei vykdytojus, lengviausia adaptuoti verslo sferoje turėtų valstybės saugumo (pvz. Valstybės saugumo departamento) ir mokesčių tarnybų (pvz. Finansinių nusikaltimų tarnyba) pareigūnai.

Tikslas – nustatyti konkurencinės žvalgybos panaudojimo galimybes konkurencinėje kovoje.

Uždaviniai:

- Nustatyti teisės aktus galinčius įtakoti konkurencinės žvalgybos padalinių veiklą;
- Nustatyti informacijos klasifikavimo metodiką;
- Nustatyti informacijos vertinimo bei pritaikomumo versle galimybes.

Objektas: Konkurencinė žvalgyba.

Metodika: mokslinės literatūros analizė, konkurencinės žvalgybos specialistų pateiktos informacijos analizė bei vertinimas.

Komercinis šnipinėjimas ar konkurencinė žvalgyba – reglamentavimas?

Neretai konkurencinė žvalgyba balansuoja ant komercinio šnipinėjimo ribos, kurią peržengus iškiltų pavojus pažeisti šalyje galiojančius teisės aktus ir už atliktus veiksmus atsakyti įstatymų bei poįstatyminių teisės aktų nustatyta tvarka. Skirtingai nuo pramoninio (komercinio) šnipinėjimo, tai yra legali informacijos rinkimo bei analizės forma. Todėl yra svarbu skirti konkurencinės žvalgybos ir pramoninio (komercinio)

šnipinėjimo sąvokas. Tas, kas neteisėtai įgijo komercine paslaptimi laikomą informaciją arba šią informaciją perdavė kitam asmeniui vadinama komerciniu šnipinėjimu (LR Baudžiamojo kodekso 210 str.). Komercinis šnipinėjimas (LR BK 210 str.) objektyvieji požymiai:

Objektas – komercinės paslapties turėtojo ekonominiai interesai;

Dalykas – informacija, sudaranti komercinę paslaptį;

Veika: neteisėtas informacijos, sudarančios komercinę paslaptį, *įgijimas* arba *perdavimas* kitam asmeniui;

Subjektas – fizinis asmuo, turintis 16 metų;

Baigtumas – nuo informacijos neteisėto įgijimo arba pranešimo kitam asmeniui momento (formalioji sudėtis).

Kalbant apie komercinį šnipinėjimą valstybė vaidina tikrai ne paskutinį vaidmenį. Galima būti išskirti šias valstybės įtakoje esančias kovas su komerciniu šnipinėjimu sritis:

Teisinės bazės sukūrimas;

Taisės aktų taikymas;

Valstybės interesas, siekiant apsaugoti komercines paslaptis.

Po komercinės paslapties suteikiamais privalumais gali pasinaudoti ir terorizmas remiančios organizacijos ar verslo grupės (Bučiūnas, 2008).

Komercine (gamybine) paslaptimi laikoma informacija, jeigu ji turi tikrą ar potencialią komercinę (gamybinę) vertę dėl to, kad jos nežino tretieji asmenys ir ji negali būti laisvai prieinama dėl šios informacijos savininko ar kito asmens, kuriam savininkas ją yra patikėjęs, protingų pastangų išsaugoti jos slaptumą (LR CK 1.116 str. 1 d). Taigi informacija, kurią bendrovė laiko ar ketina laikyti komercine paslaptimi, turi būti slapta, svarbi ir **identifikuojama** tinkamu būdu. Todėl labai svarbu atskirti veiksmus bei aplinkybes, kuriomis yra renkama informacija apie konkurentus, jų aplinką, numatyti galimus jų veiksmus ir pasirengti atitinkamai reaguoti į konkurentų veiksmus. Informacija gali būti apibrėžiama kaip duomenys apie reikšmingus faktus (asmenis, veiksmus, organizacijas, įvykius), kurie gali būti pagrindu priimant sprendimus apie administracinių ir organizacinių renginių pravedimą, taip pat apie pasiūlymų ir rekomendacijų parengimą.

Siekiant tinkamai įvertinti bei apibrėžti komercinio šnipinėjimo sąvokas, tikslinga išsiaiškinti kokie teisės aktai reglamentuoja konkurencinės žvalgybos veiklos ribas. Lietuvos Respublikos Konkurencijos įstatymo 16 straipsnis draudžia informacijos, kuri yra kito ūkio subjekto komercinė paslaptis, naudojimą, perdavimą, skelbimą be šio subjekto sutikimo, taip pat tokios informacijos gavimą iš asmenų, neturinčių teisės šios informacijos perduoti, turint tikslą konkuruoti, siekiant naudoti sau arba padarant žalą šiam ūkio subjektui. Proceso šalys ir kiti proceso dalyviai turi teisę bet kurioje tyrimo ar bylos nagrinėjimo stadijoje pateikti Konkurencijos tarybai prašymą dėl jų komercinių paslapčių apsaugos. Konkurencijos taryba ar jos įgaliotas pareigūnas turi priimti motyvuotą sprendimą dėl komercinių paslapčių apsaugos ir apie tai pranešti pareiškėjui (Lietuvos Respublikos konkurencijos įstatymas, 1999).

Baudžiamajame kodekse, 119 straipsnyje yra įtvirtintos nuobaudos už valstybinės paslapties atskleidimą. Tas, kas turėdamas tikslą perduoti užsienio valstybei, jos organizacijai pagrobė, pirkė ar kitaip rinko informaciją, kuri yra Lietuvos Respublikos valstybės paslaptis, arba šią informaciją perdavė užsienio valstybei, jos organizacijai ar jų atstovui, baudžiamas laisvės atėmimu nuo dvejų iki dešimties metų. Taip pat jeigu asmuo, vykdydamas kitos valstybės ar jos organizacijos užduotį pagrobė, pirkė ar kitaip rinko arba perdavė informaciją, kuri yra Lietuvos Respublikos valstybės paslaptis, arba kitą užsienio valstybės žvalgybą dominančią informaciją, baudžiamas laisvės atėmimu nuo trejų iki penkiolikos metų. 14 Valstybinė paslaptis gali būti atskleista ir tiesiog tarnybos, darbo metu, atliekant viešąsias funkcijas, nors ir nebuvo šnipinėji atvejų. Tai reglamentuota Baudžiamojo kodekso, 125 straipsnyje (Lietuvos Respublikos baudžiamasis kodeksas, 2002).

Visuomenės informavimo priemonės, organizacijos ar asmuo, paskelbęs informaciją neatitinkančią tikrovės, išplatinęs tokią informaciją, kuri buvo laikoma paslaptimi, atlygina moralinę žalą, kurios dydį kiekvienu atveju nustato teismas, atsižvelgdamas į konkrečias aplinkybes. Tai reglamentuota visuomenės informavimo įstatyme. Viešosios informacijos rengėjas ir (ar) platintojas, paskelbęs be fizinio asmens sutikimo informaciją apie jo privatų gyvenimą, taip pat paskelbęs tikrovės neatitinkančią, informaciją, atlygina asmeniui padarytą moralinę žalą įstatymų nustatyta tvarka. Moralinės žalos atlyginimo dydis negali viršyti 10 tūkstančių litų, išskyrus atvejus, kai teismas nustato, kad informacija buvo paskelbta tyčia. Tokiais atvejais teismo sprendimu ši suma gali būti padidinta, bet ne daugiau kaip 5 kartus (Lietuvos Respublikos visuomenės informavimo įstatymas, 1996).

Teismas, nustatydamas moralinės žalos, išreikštos pinigais, dydį, atsižvelgia į žalą padariusio asmens turtinę padėtį, teisės pažeidimo sunkumą, teisės pažeidimo pasekmes ir kitas turinčias reikšmės aplinkybes.¹⁵ Lietuvos Respublikos Konkurencijos įstatymo 22 straipsnis reglamentuoja, jog Konkurencijos taryba ir jos administracijos darbuotojai privalo saugoti šio įstatymo laikymosi kontrolės metu sužinotas ūkio subjektų komercines paslaptis ir be ūkio subjekto sutikimo naudoti jas tik tiems tikslams, dėl kurių jos buvo pateiktos. Už ūkio subjektų komercinių paslapčių atskleidimą Konkurencijos taryba ir jos administracijos darbuotojai atsako įstatymų nustatyta tvarka (Lietuvos Respublikos konkurencijos įstatymas, 1999).

Taip pat Civilinio kodekso 1.116 straipsnyje yra numatytas ir atleidimas nuo atsakomybės. Komercinę (gamybinę) paslaptį atskleidęs asmuo gali būti atleistas nuo atsakomybės, jeigu įrodo, kad paslapties atskleidimas pateisinamas visuomenės saugumo interesais. ¹⁶ Tai reiškia, kad asmuo turėtų įrodyti, kokią grėsmę būtų sukėlusì visuomenei informacija, jeigu ji būtų neatskleista. Gana svarbus būtų Lietuvos Respublikos Konstitucinio Teismo 2002 m. spalio 23 dienos nutarimas “Dėl Lietuvos Respublikos visuomenės informavimo įstatymo 8 straipsnio ir 14 straipsnio 3 dalies atitikties Lietuvos Respublikos Konstitucijai”. Konstitucinis Teismas konstatavo, kad įstatymų leidėjas, nustatydamas žurnalisto teisę išsaugoti informacijos šaltinio paslaptį, neatskleisti informacijos šaltinio, turi pareigą įstatymu nustatyti ir tai, kad kiekvienu atveju spręsti, ar žurnalistas turi atskleisti informacijos šaltinį, gali tik kompetentinga teisėsaugos institucija – t.y. teismas. Todėl šiuo nutarimu Konstitucinis Teismas konstatavo, kad visuomenės informavimo 8 bei 14 straipsnio 3 dalis prieštarauja Lietuvos Respublikos Konstitucijai (Lietuvos Respublikos civilinis kodeksas, 2000 ir Lietuvos Respublikos civilinio kodekso komentaras, 2001).

Informacija apibrėžiama kaip duomenys apie reikšmingus faktus (asmenis, veiksmus, organizacijas, įvykius), kurie gali būti pagrindu priimant sprendimus apie administracinių ir organizacinių renginių pravedimą, taip pat apie pasiūlymų ir rekomendacijų parengimą.

Žvalgybinės informacijos klasifikavimas

Žvalgybinė informacija gali būti klasifikuojama pagal (Krizan, 1999):

- Kokybės charakteristikas;
- Saugumo lygmenis;
- Informacijos analizės etapus;
- Informacijos apsaugos nuo galimų grėsmių etapus.

Pagal kokybės charakteristikas informacija gali būti skirstoma į penkias grupes, tai:

- tikrumas;
- priskiriamumas;
- naujumas;
- išsamumas;
- svarbumas.

Be to, informacija taip pat gali būti skirstoma į keturis slaptumo lygius, tai (Valstybės paslapčių apsaugos įstatymo pakeitimo įstatymas, 1997):

- riboto naudojimo;
- konfidencialiai;
- slapčiai;
- visiškai slapčiai.

Pastarieji du lygiai dažniausiai naudojami valstybės atsakomybėje esančiose srityse. Tai yra srityse kur informacijos praradimas galėtų pakirsti valstybės ekonominius pagrindus. Riboto naudojimo informacijos slaptumo lygmuo gali būti naudojamas bet kurioje verslo struktūroje vadovo ar jo įgaliotų asmenų sprendimu. Slaptumo lygmuo „Konfidencialiai“ dažniausiai naudojamas bankinėje sistemoje, siekiant apsaugoti informaciją apie klientus bei bankines operacijas (Prescott, 2000). Yra keliami specialūs reikalavimai ir patalpoms kur yra saugoma atitinkamo lygmens informacija, kuo slaptumo lygmuo aukštesnis, tuo jos saugojimui keliami aukštesni reikalavimai.

2001-2006 m. Komisijos komunikatuose Tarybai, Europos Parlamentui, Europos ekonomikos ir socialinių reikalų komitetui ir regionų komitetui tinklų ir informacijos saugumas apibrėžiamas kaip „tinklo ar informacinės sistemos atsparumas tam tikru lygmeniu atsitiktiniams įvykiams ar nusikalstamiems veiksams, kurie kelia pavojų šiuose tinkluose ir sistemose sukauptų ir jais perduodamų duomenų bei susijusių paslaugų prieinamumui, tikrumui, vientisumui ir konfidencialumui“ (Briuselis, 2006). Todėl vienas

svarbiausių uždavinių yra informacijos rinkimo bei analizės etapų numatymas bei finansavimo šiai veiklai užtikrinimas. Tuo tikslu reikalinga numatyti sekančius informacijos rinkimo bei analizės etapus (žr. 1 pav.):

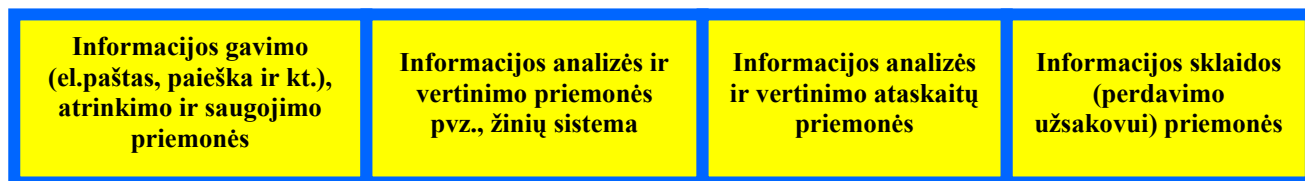
- poreikio nustatymas (konsultacijos nustatant informacijos apsaugos reikalingumą ir apimtį);
- poreikio įvertinimas;
- poreikio patenkinimo planas;
- poreikio finansavimas;
- ilgalaikių planų sudarymas.

Tačiau galima būti ir priešingas – informacijos apsaugos poreikis. Esant atvirkštiniam poreikiui, t.y. apsisaugojimui nuo informacijos praradimo galima išskirti sekančius etapus:

- galimų grėsmių identifikavimas;
- galimų grėsmių įvertinimas;
- grėsmės lygio nustatymas;
- prioritetų parinkimas;
- finansavimo skyrimas;
- grėsmių pašalinimas.

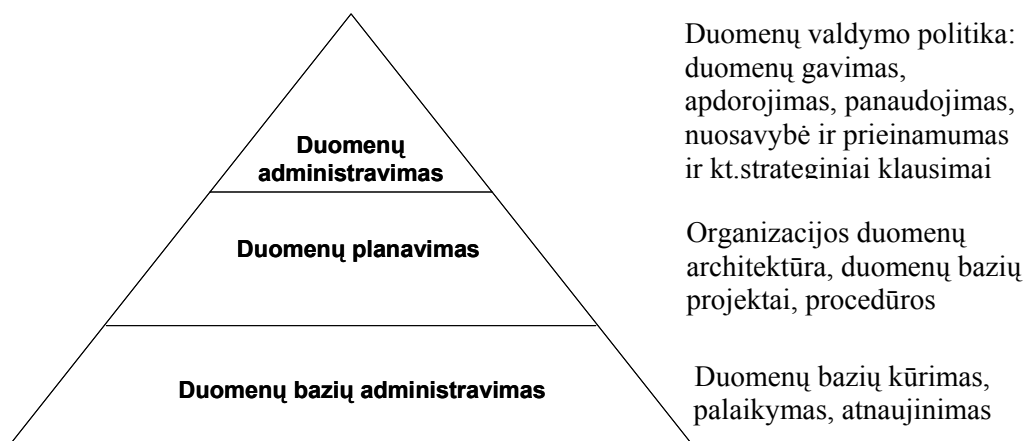
Išanalizavus daugelio mokslininkų pateiktą informaciją galima išskirti šias verslo informacinio saugumo–apsisaugojimo kryptis:

- informacijos analizė;
- teisinės bazės analizė;
- teisinės bazės suderinimas;
- IT tinklų auditas;
- IT tinklų tvarkymas;
- bendros tvarkos nustatymas;
- kompleksinių priemonių suderinimas.



1 pav. Sistemos nuo informacijos gavimo iki jos pateikimo schema (ENISA, 2006):

Vienas pagrindinių informacijos surinkimo šaltinių yra įvairios duomenų bazės. Remiantis duomenų bazėmis galėtume išskirti sekančią duomenų valdymo veiklą (žr. 2 pav.):



2 pav. Duomenų planavimo ir perdavimo schema

Remiantis informacijos šaltiniais, specialistų komentarais, bei asmenine patirtimi galima išskirti sekančius informacijos nutekėjimo šaltinius:

- Žmogiškasis veiksnys;
- Komunikacijos kanalai;
- IT tinklai;
- Konkurentų veikla;
- Partnerių veikla;
- Atsitiktinai prarasta informacija.

Išanalizavus surinktą informaciją bei remiantis asmenine patirtimi galima išskirti tokias verslo saugumo kryptis, kurias įgyvendinus galima būtų pasiekti pakankamą verslo saugumo lygį:

- Informacijos analizė;
- Teisinės bazės analizė;
- Teisinės bazės suderinimas;
- IT tinklų auditas;
- IT tinklų tvarkymas;
- Bendros tvarkos nustatymas;
- Kompleksinių priemonių suderinimas.

Remiantis specialistų teigimu, galima būtų išskirti tokius dažniausiai konkurencinės žvalgybos analitikams pateikiamus vienkartinis užklausimus (CIA, 1997):

- Demografija ir statistika;
- Finansinių rodiklių palyginimas;
- Informacijos paieška spaudoje;
- Naujų besivystančių rinkų apžvalga;
- Analitinė investicijų apžvalga;
- Aukščiausio lygio vadovų biografiniai duomenys;
- Tyrimai ir ataskaitos apie jau atliktus tyrimus;
- Konkurencinė informacija;
- Užsienio verslo tyrinėjimai;
- Kiti viešai prieinami informacijos šaltiniai;
- Ekonominiai rodikliai.

Kaip konkurencinės žvalgybos įdiegimo stambiose pasaulio korporacijose pavyzdį galime pateikti korporacijos „Procter & Gamble“ konkurencinės žvalgybos vaidmens ir strategijos pakeitimus bei jų įtaka bendrovės valdymui. Vykdydama konkurencinę žvalgybą minėta korporacija remiasi penkiomis pagrindinėmis dedamosiomis, tai (Competitive Intelligence Review, 1999), (žr. 1 lentelę):

- Būtinumo pagrindimas;
- Struktūra;
- Prieėjimas prie informacijos/technologijų vaidmuo;
- Informacijos panaudojimas;
- Kultūra.

1 lentelė. Esminiai pasikeitimai korporacijoje „Procter & Gamble“ įdiegus naują konkurencinės žvalgybos sistemą

Buvusi sistema	Nauja sistema
Statistinė konkurencijos analizė	Dinaminis konkurentų reakcijos modelis
Pasyvios rutininės ataskaitos	Konkrencinė žvalgyba dalyvauja strategijos parengime ir galimų variantų analizėje
Atsakingi tikrai konkurencinės žvalgybos analitikai	Atsakingi visi korporacijos darbuotojai
Maksimaliai centralizuotas arba maksimaliai decentralizuotas	„Radialinė-ašinė“ schema
Individualus darbas ir funkcionali specializacija	Komandinis darbas
Poreikis sužinoti	Poreikis pasidalinti žiniomis
Aukščiausio lygio vadovų palaikymas – ribotas ir epizodinis	Aukščiausio lygio vadovai nuolat dalyvauja konkurencinės žvalgybos darbe

Konkurencinės žvalgybos pritaikomumas bei vertinimas

Autoriai išskyrė sritis labiausiai besirūpinančias savo informacijos saugumu įmones (Society of Competitive Intelligence Professionals, 1996) (žr. 2 lentelę):

2 lentelė. labiausiai informacijos saugumu besirūpinančios įmonės

<u>Aukščiausias įvertinimas</u>	<u>Vidutinis įvertinimas</u>	<u>Žemas įvertinimas</u>
Oro erdvė ir gynyba; Biomedicina; chemijos pramonė; Elektronika; Finansinės paslaugos; Sveikatos apsauga; Informacinės paslaugos; Farmacija; Mažmeninė prekyba.	automobilių pramonė; statybos ir nekilnojamas turtas; naftos ir dujų pramonė; transporto įmonės; didmeninė prekyba;	žemės ūkis; maisto pramonė; pramonės įranga; žaliavų išgavimas;

Tinkamai įgyvendinus pranešime apžvelgtas priemones verslo organizacijos turėtų gauti sekančią naudą (Miller, 2004):

- Kompanijos lėšų taupymas;
- Pelno augimas;
- Respektabilumas;
- Pagalba konkurencinėje kovoje;
- Galimybės plėsti rinkas.

Žvalgybos tarnybos siekiančios kokybiškai ir savalaiki gauti informaciją bei padaryti atitinkamas išvadas neretai yra naudoja divergencinę analizę. Divergencinė analizė yra pastovus hipotezių, požiūrių ar idėjų iškėlimo metodas, reikalaujantis, kad analitikas būtų mastantis susitvardantis ir labai kūrybingas.

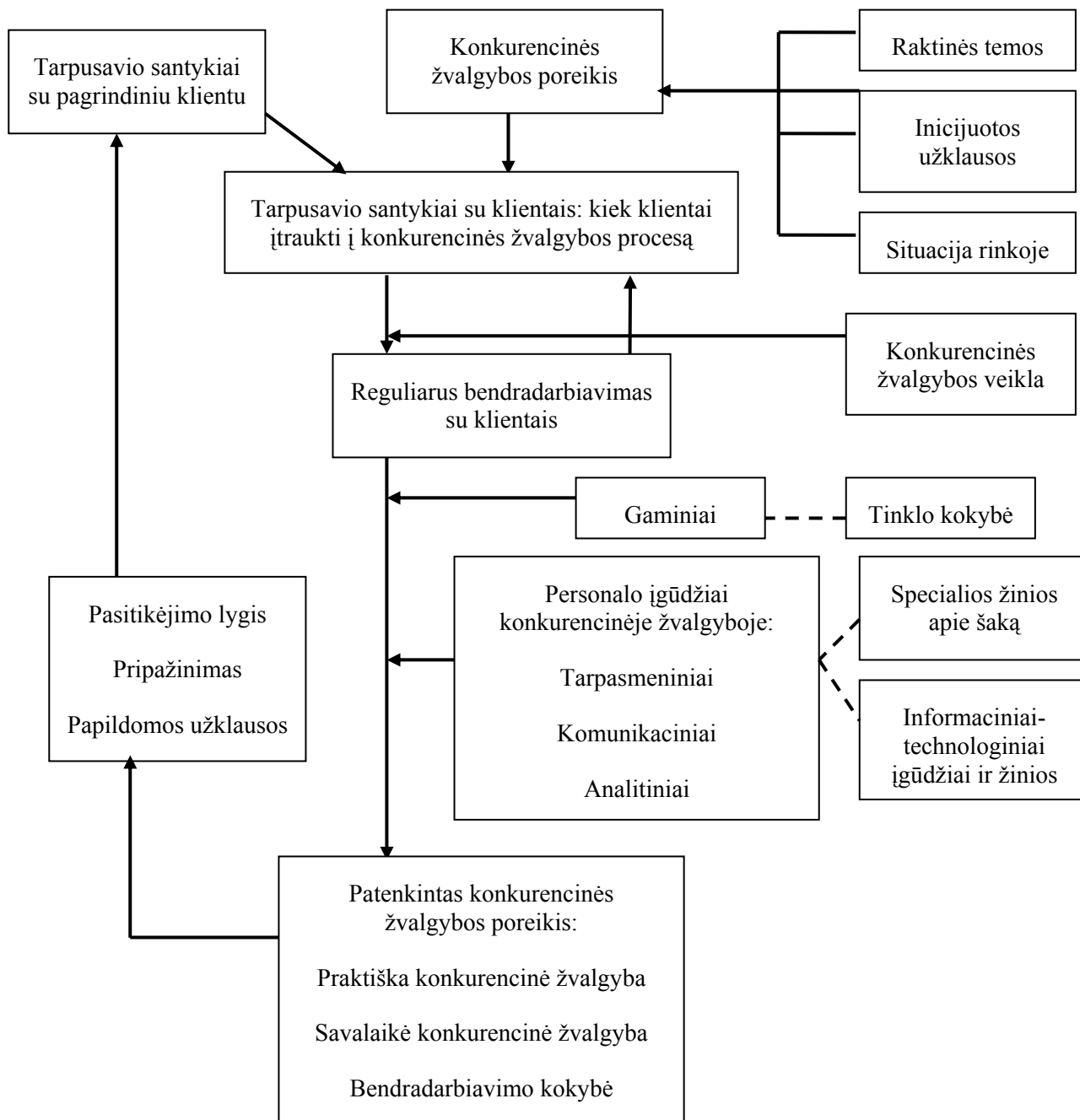
Procesas prasideda nuo užrašyto teiginio, problemos ar klausimo apibrėžimo. Analitikas sudaro prielaidų sąrašą ir nusprendžia kaip tos prielaidos galėtų pakeisti jo požiūrį į problemą. Tuo metu, analitikas sudaro jo turimų duomenų surinkimo klausimų sąrašą, jeigu yra duomenys, kuriuos jis nori turėti prieš pradėdamas kurti idėjas ar hipotezes. Galiausiai performuluoja problemą.

Valymas: prieš kurdamas ir įvertindamas hipotezes, žvalgybininkas turi atsikratyti šališkumo, kad nesustabdytų kūrybinio proceso. Tai daroma užrašant sveikas idėjas. Surašant jas pačioje pradžioje, išvengiama proto blokavimo vėliau. Tačiau šios idėjos vis dar turi vertę ir bus panaudotos.

Divergencija: po to žvalgybininkas išbando tris hipotezių kūrimo technikas – Teorijos, Situacinės logikos ir Palyginimo panaudojimo. Jis surašo klausimus prasidedančius „Kaip...“, „Kodėl ne...“, „Kas jeigu...“ ir „Aš noriu...“, stengdamasis sukurti kuo daugiau hipotezių ir idėjų. Ir jis abstrahuojasi nuo idėjų vertinimų dėl jų tinkamumo ir netinkamumo ar gerumo ir nepraktiškumo. Ir kuo daugiau pasineriama į savo pasąmonę, tuo daugiau geresnių idėjų yra tikimybė iškelti. Turėtų būti iškelta ne mažiau 5 ar 10 tokių idėjų, ir jokių būdu ne mažiau kaip 3. Mažiau nei 3 hipotezės retai kada gali apimti visą norimų atsakymų ar pasirinkimų diapazoną.

Naudingų hipotezių atrinkimo procesas yra neužbaigtas tol, kol nebus gautas kiekvienos hipotezės rezultatas su išvadomis ir požymiais. Kiekviena hipotezė ar prielaida yra išdėstoma motyvuojant, kodėl ji turi būti priimta arba atmesta. Po to, kiekvienos hipotezės rezultatas yra pasirenkamas pagal išvadų arba galimų rezultatų, kurie galėtų būti gauti, jeigu ši alternatyva būtų pasirinkta, sąrašą. Galiausiai išvaidinami kai kurie požymiai, kurie bus matomi, jei išties bus pasirinktas tas rezultatas.

Norint tinkamai pritaikyti bei pilnai išnaudoti konkurencinės žvalgybos galimybes reikalinga tinkamai (struktūrine bei kokybine prasme) įdiegti konkurencinės žvalgybos padalinį kompanijoje (žr. 3 pav.). Čia galima pasinaudoti Rick Chabell modeliu.



3 pav. Rick Chabell modelis

Išvados

Atlikus literatūros analizę, pasinaudojus Lietuvos ir užsienio žvalgybos specialistų vertinimais bei remiantis asmenine patirtimi galima pateikti sekančias išvadas:

1. Konkurencijos sąlygomis rinkoje atsiranda papildomos priemonės ir metodai, kurių naudojimas gali turėti didelės reikšmės konkurencinėje kovoje.
2. Konkurencinės žvalgybos specialistas turi turėti ne tik ekonominių žinių, suvokti ekonominius procesus, bet turėti ir pakankamas teises žinias.
3. Dirbant kryptingai ir naudojant specialius žvalgybinius metodus, įmanoma pasiekti gerų rezultatų bei įgyti svarų pranašumą konkurencinėje kovoje.
4. Gerų rezultatų įmanoma pasiekti tik laikantis nustatyto plano ir dirbant kryptingai pasirinkta kryptimi.

Literatūra

1. Lietuvos Respublikos visuomenės informavimo įstatymas // Valstybės žinios, (1996), Nr. 71-1706.
2. Lietuvos Respublikos konkurencijos įstatymas // Valstybės žinios, (1999 03 23). Nr. VIII – 1099.
3. Lietuvos Respublikos, Baudžiamojo kodekso 210 straipsnis.
4. Lietuvos Respublikos baudžiamasis kodeksas // Valstybės žinios (2002), Nr. 37 – 1341.
5. Lietuvos Respublikos Civilinio Kodekso 1.116 straipsnio 1 dalis.
6. Lietuvos Respublikos civilinis kodeksas // Valstybės žinios, (2000) 07 19. Nr. VIII – 1864.
7. Lietuvos Respublikos civilinio kodekso komentaras. Pirmoji knyga. Bendrosios nuostatos. Vilnius, (2001).
8. Valstybės paslapčių apsaugos įstatymo pakeitimo įstatymas, (1997 m. birželio 10 d.) Nr. VIII-255, Vilnius.
9. Europos tinklų ir informacijos apsaugos agentūra, Gairės vartotojams: Kaip didinti informacijos saugumo suvokimą. (2006 m. birželis).
10. Krizan, Lisa (1999). Intelligence Essentials for Everyone. Washington, DC: Government printing office.
11. Tao, Qingju, Nad John E. Prescott (2000). China: Competitive Intelligence Practices in an Emerging Market Environment, Competitive Intelligence Review.
12. Directorate of Intelligence, Central Intelligence Agency. A Compendium of Analytic Tradecraft Notes, Volume 1. (1997). Washington, DC: Government Printing Office.
13. Competitive Intelligence Review, Vol. 10 (4) 4-9, 1999.
14. Society of Competitive Intelligence Professionals/Rutgers University CEO Roundtable. Symposium: „Understanding the Competition: A CEO's Perspective“, Competitive Intelligence Review. 7(3), 4-14.
15. Prescott E., Miller H. Stephen (2004). Proven Strategies Competitive Intelligence. Wiley.
16. Gaidelys, V. and G. Buciunas (2008). 'Money laundering and its economic impacts in the context of the fight against terrorism', Inžinerinė Ekonomika-Engineering Economics(3), pp. 26-33.

USE OF RECONNAISSANCE METHODS SEEKING ADVANTAGES IN COMPETITIVE CONTEST

Vaidas Gaidelys

Summary

According to the experts in reconnaissance opinion after the Soviet Union had been destroyed great many specialists working in special detachments (collecting and analyzing information, operational servants, analysts, IT specialists, technicians and others) were fired in post soviet republics because of reduction of staff, services dissolution, also were tired (20 years' working experience is enough) and on the other grounds. Large business corporations soon spotted the possibilities to use such specialists' experience and knowledge so the services of vindication, security and others as well as separate consulting companies were founded. Some scientists maintain that large world corporations successfully use virtues provided by competitive reconnaissance in order to achieve competitive advantages. The company, which decided to invest into collecting and analyzing information about rivals' activity and plans, is usually interested in the benefit it could get. Therefore in the most scientists' opinion the possible benefit of business information's safety includes the company's funds economy, profit gain, respectability, support in competitive contest, possibility to expand the market (Stephen, 2004).

Keywords: reconnaissance methods, sources of information, analysis of information.

