РЕПУБЛИКА МАКЕДОНИЈА
УНИВЕРЗИТЕТ „Св. КИРИЛ И МЕТОДИЈ“ - СКОПЈЕ
ФИЛОЗОФСКИ ФАКУЛТЕТ
ИНСТИТУТ ЗА БЕЗБЕДНОСТ, ОДБРАНА И МИР

„ИНФОРМАЦИИТЕ И ИНФОРМИРАЊЕТО КАКО УСЛОВ ЗА ЕФИКАСНО ПЛАНИРАЊЕ ВО БЕЗБЕДНОСНИОТ СЕКТОР НА РЕПУБЛИКА МАКЕДОНИЈА“

Ментор:
Проф д-р Оливер Бакрески

Кандидат:
м-р Александар Нацев

Скопје, Март 2016 година

СОДРЖИНА

ВОВЕД **4**

2. ФОРМУЛАЦИЈА НА ПРЕДМЕТОТ НА ИСТРАЖУВАЊЕТО 6
2.1. ОПЕРАЦИОНАЛНО ОДРЕДУВАЊЕ НА ПРЕДМЕТОТ НА ТРУДОТ 11
2.2. ВРЕМЕНСКО, ПРОСТОРНО И ДИСЦИПЛИНАРНО ОПРЕДЕЛУВАЊЕ НА ПРЕДМЕТОТ НА ИСТРАЖУВАЊЕТО 14
2.3. РЕЗУЛТАТИ ОД ДОСЕГАШНОТО ИСТРАЖУВАЊЕ 14
3. ЦЕЛИ И ЗАДАЧИ НА ИСТРАЖУВАЊЕТО 15
4. ХИПОТЕТИЧКА РАМКА 16
4.1. ОПШТА ХИПОТЕЗА 16
4.2. ПОСЕБНИ ХИПОТЕЗИ 16
5. МЕТОДИ И ТЕХНИКИ НА ИСТРАЖУВАЊЕ 17
6. ОПШТЕСТВЕНА И НАУЧНА ОПРАВДАНОСТ НА ИСТРАЖУВАЊЕТО 19

ГЛАВА 1 ИНФОРМАЦИЈА И ИНФОРМИРАЊЕ **21**

1.1. Општо за поимот информација 22
1.2. Терминолошки дивергенции на поимите податок и информација 24
1.3. Општо за информирањето 26
1.3.1. Основните компоненти на информирањето 26

ГЛАВА 2 ОДНОСОТ ИНФОРМАЦИЈА-ИНФОРМИРАЊЕ **29**

2.1 Улогата на информирањето 30
2.2. Меѓузависноста на информациите и информирањето 31
2.3. Потреба од информации и информирање 33

ГЛАВА 3 ИНФОРМАЦИИТЕ И НИВНОТО ЗНАЧЕЊЕ ВО РАБОТАТА НА БЕЗБЕДНОСНИОТ СЕКТОР **37**

3.1. Информирањето како услов за ефикасно планирање во безбедносниот сектор 38
3.2. Информациите и безбедносниот сектор 38
3.3. Информациски циклус 42
3.3.1 Планирање и насочување 46
3.3.1.1 Одредување на потребите на крајните корисници 46
3.3.1.2. Дефинирање на предметот на интерес 47
3.3.2 Прибирање на податоците 49
3.4.3 Обработка и анализа на податоците 69
3.4.4 Изработка на информацијата и нејзино доставување до крајните корисници 77

ГЛАВА 4 СПОДЕЛУВАЊЕ ИНФОРМАЦИИ **83**

4.1. Општо за процесот за споделување информации 84
4.2. Придобивки од споделувањето 86
4.3. Препреки за споделувањето информации 87
4.3.1. Препреки кои произлегуваат од учесниците во процесот на споделување информации 88
4.3.2. Препреки кои произлегуваат од карактеристиките на информациите кои се споделуваат 92
4.3.3. Препреки од техничка природа 94
4.3.4. Препреки кои произлегуваат од недостатокот на утврдени законски регулативи и процедури за споделување 97
4.4. Решенија за унапредување на споделувањето 98
4.4.1. Генерални препораки за успешно споделување информации 99

4.4.2. Препораки за надминување на препреките кои произлегуваат од учесниците во процесот на споделување информации *100*
4.4.3. Препораки за надминување на препреките кои произлегуваат од карактеристиките на информациите кои се споделуваат *101*
4.4.4. Препораки за надминување на техничките препреки *102*
4.4.5. Препораки за надминување на препреките кои произлегуваат од недостатокот на утврдени законски регулативи и процедури за споделување *102*
4.5. Модел за споделување 103
4.6. Споделување информации помеѓу безбедносниот и приватниот сектор 108
4.7. Споделување информации со други држави 110
4.7.1. Карактеристики на билатералното споделување информации *112*
4.7.2. Препораки за надминување на препреките за споделување информации со други држави *115*

ГЛАВА 5 ЗАШТИТА НА ИНФОРМАЦИИТЕ ЗА БЕЗБЕДНОСНИОТ СЕКТОР 117

5.1. Класификација на информациите 118
5.2. Одредување на степенот на класификација 122
5.3. Потребата за заштита на класифицираните информации 130
5.4. Мерки и активности за административна безбедност на класифицирани информации 133
5.4.1. Прием и евиденција на класифицираната информација *134*
5.4.2. Ракување со класифицираната информација и нејзино чување *135*
5.4.3. Изготвување на копии, преводи и извадоци на класифицираната информација *135*
5.4.4. Остварување контрола врз распоредувањето и распространувањето на класифицираната информација *136*
5.4.5. Отстранување и уништување на класифицирани информации *136*
5.5. Мерки и активности за физичка безбедност на класифицирани информации 137
5.5.1. Процена за можно нарушување на безбедноста на класифицираната информација *139*
5.5.2. Определување на административни и безбедносни зони *142*
5.6. Мерки и активности за персонална безбедност на класифицирани информации 144
5.6.1. Безбедносна проверка *145*
5.6.2. Издавање на безбедносен сертификат *146*
5.7. Мерки и активности за информатичка безбедност на класифицирани информации 150
5.7.1. Компјутерска безбедност *151*
5.7.2. Комуникациска безбедност *155*
5.7.3. Криптографска безбедност *155*
5.7.4. Емисиска безбедност *156*
5.7.5. Процена за нарушување на безбедноста на комуникациско-информатичките системи. *158*
5.7.6. Акредитација на комуникациско-информатичките системи и процеси *160*
5.8. Мерки и активности кои се преземаат при настанато нарушување на безбедноста на информациите 160

ГЛАВА 6 ИНФОРМАЦИИТЕ И ИНФОРМИРАЊЕТО КАКО УСЛОВ ЗА ЕФИКАСНО ПЛАНИРАЊЕ ВО БЕЗБЕДНОСНИОТ СЕКТОР НА РЕПУБЛИКА МАКЕДОНИЈА 162

6.1. Информациите и информирањето во безбедносниот сектор на Република Македонија 163
6.2. Потребата за споделување информации во безбедносниот сектор на Република Македонија 166
6.3. Мерки и активности за заштита на информациите во безбедносниот сектор на Република Македонија 169
6.4. Информациите како услов за ефикасно планирање во безбедносниот сектор на Република Македонија 172

ГЛАВА 7 ИНТЕРПРЕТАЦИЈА НА РЕЗУЛТАТИТЕ ОД СПРОВЕДЕНОТО ИСТРАЖУВАЊЕ 175

7.1. Интерпретација и анализа на резултатите 176
7.1.1. Информации и информирање *179*
7.1.2. Информирањето како важен предуслов за ефикасното функционирање на безбедносните институции *180*
7.1.3. Планирањето како ефикасна алатка во менаџирањето на работата на безбедносниот сектор *181*
7.1.4. Превентивни активности на безбедносниот сектор *182*
7.1.5. Придонесот на информациите во работата на безбедносниот сектор *183*

7.1.6. Важноста на поседувањето навремени и точни информации *184*
7.1.7. Информационен циклус *185*
7.1.8. Фазите на информациониот циклус *186*
7.1.9. Методи на прибирање податоци *189*
7.1.10. Можноста за прибирање податоци преку дипломатско-конзуларните претставништва *190*
7.1.11. Техничките дисциплини за прибирање податоци наспроти класичните конспиративни методи за прибирање податоци *191*
7.1.12. Потребата од заштита на изворите на податоци и на методите на работа на безбедносните служби *192*
7.1.13. Евалуација на веродостојноста на прибраните податоци *193*
7.1.14. Аналитичката обработка на прибраните податоци *194*
7.1.15. Дисеминација на информациите *195*
7.1.16. Важноста на повратната врска (фидбекот) *195*
7.1.17. Споделување информации во безбедносниот сектор *197*
7.1.18. Придобивки и ризици од споделувањето информации *197*
7.1.19. Препреки за споделување информации *198*
7.1.20. Споделување информации помеѓу безбедносниот сектор и приватниот сектор *199*
7.1.21. Споделување информации со други држави *200*
7.1.22. Споделување информации во безбедносните институциите *201*
7.1.23. Ограничување одредени информации од слободна циркулација во јавност *202*
7.1.24. Евалуација на потребата за задржување на степенот на класификација *203*
7.1.25. Важноста на безбедносниот сертификат *204*
7.1.26. Влијанието на сајбер-заканите врз безбедноста на класифицираните информации *205*
7.1.27. Уништување класифицирани информации *206*
7.1.28. Нарушување на безбедноста на класифицирана информација *206*
7.1.29. Заштита на класифицираните информации во безбедносните институции *207*

ЗАКЛУЧОК **209**

ПРИЛОГ БР.1 - АНКЕТЕН ПРАШАЛНИК **214**

БИБЛИОГРАФИЈА **223**

НОРМАТИВНИ АКТИ И ДРУГИ МАТЕРИЈАЛИ **227**

ИНТЕРНЕТ СТРАНИЦИ **228**

Вовед

Со цел да се заштитат интересите и вредностите на една држава, како и нејзината внатрешна и надворешна безбедност од можните рапидни промени на светско, на регионално или на локално рамниште во иднина, раководните и безбедносните органи на државата мора постојано да добиваат навремени и соодветни информации кои се неопходни за успешно водење на сите витални државни функции. Она што е значајно и што произлегува од оваа констатација е потребата од успешно менаџирање со информациите кои се доставуваат до безбедносниот сектор, односно нивно навремено прибирање, нивна обработка и анализа и нивна навремена дисеминација до раководните државни или безбедносни органи. Бидејќи во фокусот на ова истражување се наоѓаат претежно информациите кои се употребуваат во безбедносниот сектор на една држава, најголем дел од образложението и е посветен на нив.

Безбедносниот систем со своите елементи (потсистеми) како извршен орган на политичката власт станува фундаментален конституенс во создавањето и во одржувањето посакувана безбедносна состојба и активен следбеник на реполитизацијата на животот[1]. За службите кои го составуваат безбедносниот сектор, којшто треба да го опфаќа военополитичкиот, геостратегискиот и безбедносниот амбиент, најголеми приоритети се:

- надгледување и борба против сите видови внатрешни политички закани за државата и јавниот мир и одржување на државната контрола;
- заштита на економската безбедност на државата (борба против сивата економија до обезбедување поддршка на домашните компании во стопанскиот натпревар со конкурентните стопански компании), следење на економскиот и индустрискиот развој на другите држави, силите на нивната индустрија, нивната надворешно-трговска размена и др.;
- собирање податоци од сите делови на светот за значајните проблеми и движења од областа на политиката, одбраната, науката, социјалните состојби, државната управа, движењата на масите, меѓудржавните и други односи;

---

[1] Оливер Бакрески, Милан Милошевиќ – „*Современи безбедносни системи*“ *Скопје, 2010,* стр.31

- анализа на енергетиката и на средствата, географски и демографски прашања, проблемите на животната средина и предизвиците на цивилната технологија, како од техничка, така и од политичка перспектива;
- пронаоѓање одговори за разузнавањето и контраразузнавањето, следење на трендовите на меѓународниот пазар за оружје, стратегијата на воената индустрија, пролиферацијата на оружјето за масовно уништување, борбата против сите современи видови тероризам, дури и против нуклеарниот криминал и недозволената трговија со наркотични средства[2];
- мониторирање и навремено предупредување за настаните што претставуваат директно или индиректно загрозување на националните интереси, без оглед дали се од политичка, од воена или од економска природа.

За да се осигура ефикасност, економичност и навремена адаптација на променливите потреби, неопходно е сите прибрани информации континуирано и навремено да се доставуваат до државните раководни органи со цел да се одговори на современите барања на државата за поддршка на нејзината политика и за целосна заштита на нејзините витални национални цели и интереси.

Брзиот општествен, научен, културен и технички развој доведува до нови побарувања кои ја наметнуваат потребата од што повеќе информации, кои ќе опфаќаат што поголем дијапазон на области. За таа цел, треба да се усовршат начините до доаѓање до нови информации, оценувањето на нивната вредност (сигурност на изворот од кој се добиени, точност на нивната содржина и нивната важност), колку што е можна побрза анализа на овие информации и нивно навремено доставување до крајните корисници. Освен сите овие постапки, треба да се води сметка и за одржувањето на безбедноста на тие информации, бидејќи со нарушувањето на нивната

---

[2] Разузнавањето преставува збир на плански, организирани и постојани мерки и активности, заради остварување увид во состојбата, можностите и намерите на одделни држави и појави кои се објект на разузнавачкото истражување, со цел врз основа на тие сознанија да се преземат соодветни активности на политички, економски и воен план. – Стајић, Љубомир - *„Основи безбедности", Београд, 2004,* стр.206

Според Милан Милошевиќ: Разузнавањето претставува специфична општествена активност насочена кон надворешните и внатрешните противници, т.е. актуелните и потенцијалните непријатели на одредена држава или општествена група, чиј предмет на интерес се најсуптилните и најдобро чуваните тајни на другите држави и останатите општествени субјекти, а кои се преземаат со цел реализација на виталните државни интереси. – Милошевиќ, Милан – *„Систем државне безбедности", Београд, 2001,* стр. 24

Контраразузнавањето се занимава со откривање и спречување на дејствувањето на противничките разузнавачки служби, заштита на сопствените тајни и заштита на одредени објекти и работни места што можат да бидат мета на противничките служби. – Баткоски, Томе – *„Разузнавачка и безбедносно-контраразузнавачка тактика", Скопје, 2008,* стр. 143

безбедност и нивното неовластено објавување би можело да се предизвика штета на интересите на државата.

Секоја од овие фази се карактеризира со свои специфичности и побарувања. Со цел една значајна информација да ја постигне својата ефикасност, треба да се направи посебен осврт кон зачувувањето на нејзината безбедност, бидејќи ако дојде до нејзино предвремено објавување нејзината вредност значително се намалува. Во една ваква ситуација, залудни се напорите на сите оние што работеле на прибирањето на таа информација, залуден е ризикот што го има преземено некој соработник на разузнавачката или контраразузнавачката служба со цел тајно да го достави тој податок до својот ракувач, залудни се финансиските средства потрошени за добивање на таа информација (доколку е добиена со финансиски надомест), залудни се сите работни часови што ги имаат вложено сите оние лица што работеле на нејзина обработка, а не е за запоставување и фрустрацијата и губењето на моралот кај сите претходно споменати лица. Но, она што е најважно во оваа ситуација е што државата се лишува од еден адут што го држи в рака, и што би бил многу корисен при одлучувањето за одредени стратегиски или тактички ситуации. Одржувањето на безбедноста на информациите мора да се смета како компактен дел на целиот оној циклус на ракување со тие информации, со цел да се избегне токму неовластеното (или предвремено) изнесување и објавување на тие информации, што пак придонесува за поефикасно планирање на активностите што се преземаат во безбедносниот сектор.

2. ФОРМУЛАЦИЈА НА ПРЕДМЕТОТ НА ИСТРАЖУВАЊЕТО

Предметот на истражување на докторската дисертација е поделен во неколку области, кои се поблиску разработени и е посветено особено внимание на нивната меѓузависност. На почетокот на истражувањето се разработуваат основните поставки за поимот информација, односно се прави дефинирање на поимот, елаборација на потребата и значењето на информациите, како и целиот концепт на информирањето и информираноста. Наредниот дел се фокусира на улогата што ја имаат информациите во безбедносниот сектор на една држава, и како тој сектор има постојана потреба од што повеќе информации кои го засегнуваат неговото поле на интерес. Овие информации се потребни затоа што за да може да се изврши успешно планирање на активностите кои треба да се преземат, неопходно е да се поседуваат сите составни делови на една целина.

Она што следи после тоа е всушност делот на кој му е посветено најголемо внимание. Третиот дел се фокусира на влијанието на информациите во работата на безбедносниот сектор, односно се однесува на процесот на ефективно користење на една информација кој опфаќа неколку зависно поврзани постапки, кои редоследно би изгледале вака: запознавање со субјектите за прибирање информации, планирање и прибирање на информациите, обработка на информациите и нивно доставување до крајните корисници.

При прибирањето на информации, субјектите што го вршат тоа прибирање (односно државните органи кои влегуваат во безбедносниот сектор) имаат на располагање најразлични начини и методи за стигнување до нови (свежи) информации. За успешно да се исполни потребата од одреден тип информации кои се безбедносно интересни, исклучително важно е планирањето на начинот на кој може да се дојде до тие информации, односно како може тие информации да се приберат. Информациите се прибираат од најразлични извори, во прв ред од човечки извори, а потоа од најразлични документи и други пишани материјали, како и од разни предмети или технички средства.

Широкиот дијапазон на достапни методи кои можат да ги применат безбедносните органи вклучува примена на легални методи, под кои се подразбираат следните:

- прибирање информации преку соработка со други држави, односно преку соработка со нивните безбедносни органи;
- прибирање информации преку соработката со меѓународни организации (ЕВРОПОЛ, ИНТЕРПОЛ, Совет за безбедност на ОН и сл.);
- прибирање информации од отворени извори, односно преку следење на средствата за јавно информирање, преку следење на стручни и специјализирани списанија и сл.;
- прибирање информации со испитување на емигранти или затвореници;
- прибирање информации преку официјалните активности на дипломатско-конзуларните претставништва.

Користењето легални методи не е ограничено само на горенаведените. Бидејќи со користењето на легалните методи на прибирање информации не се прекршуваат некои законски или правни норми, тие може да се применуваат во која било ситуација, па дури и во најсекојдневните ситуации, како на пример преку разговор да се добијат некои информации од безбедносен карактер.

Можноста за користење на легалните методи на работа за разузнавачка дејност на сегашното ниво на меѓународни односи е прилично голема, бидејќи условите и средствата за нивна примена се многу поволни. Заради тоа може да се очекува дека користењето на легалните методи во прибирањето на информации ја претставува иднината во константната информираност, но сепак треба да се нагласи дека ваквите методи никогаш не можат да ги заменат класичните прикриени методи.

За разлика од легалните методи на прибирање информации, прикриените (или конспиративни) методи имаат свои специфичности и поставуваат поголеми побарувања пред припадниците на безбедносните органи. Најмногу користени конспиративни методи се:

- метод на инфилтрација во безбедносната или политичката структура на друга држава или во рамките на терористичка или криминална организација, со цел прибирање информации од „прва рака“, којшто е воедно и најризичниот конспиративен метод за прибирање информации;
- метод на тајно користење на технички средства, кој вклучува следење на комуникациите, прикриено набљудување и физичко следење и сл.;
- агентурниот метод на работа, односно врбување соработници и агенти од спротивставениот табор (противнички разузнавачи, припадници на криминални или терористички организации и сл.).

Од горенаведените методи, најголема ефикасност има методот на врбување соработници. Најважните податоци можат да бидат добиени преку човечки извор, односно преку оној човек што е во непосреден контакт со оригиналната информација, а овој метод обезбедува и оперативен (агентурен) продор во местата каде што се чуваат информации и документи со најголемо значење.

По успешното прибирање на информациите, потребно е да се почне со нивна верификација и анализа, а потоа и последната фаза од информациониот циклус, односно нивно доставување до крајните корисници. Со цел да се обезбеди што поголема ефикасност во оваа фаза, неопходно е да се исполнат следниве услови кои имаат директно влијание врз конечниот резултат:

- Силни аналитички капацитети. Овој прв услов ја акцентира потребата од компетентни аналитичари, кои всушност се главните актери во оваа фаза на обработка на информациите[3]. Аналитичарите треба да поседуваат висок степен на аналитичка

[3] Марина Малиш Саздовска - *„Прирачник за разузнавачки циклус“,Скопје, 2005,* стр.25

подготвеност, индивидуални квалитети, висок степен на образование и широки познавања од различни области. Сите предности што ги овозможува една важна информација може да се искористат само од аналитичар кој одлично ја познава својата работа.

- Постојан прилив на информации. За да може да биде успешна една анализа, на аналитичарите им е потребен постојан прилив на информации, по можност од различни извори. Доколку аналитичарот има постојан прилив на нови информации, тој многу полесно може да ја комплетира целосната слика за конкретниот предмет на обработка и многу поточно да ја направи својата анализа. Уште една предност од постојаниот прилив на информации е тоа што многу лесно ќе можат да се елиминираат погрешните информации и намерно пласираните дезинформации.

- Систематизација во работата. Работата на еден аналитичар ќе биде многу поуспешна доколку тој се фокусира само на одреден вид предмети на обработка. Одредувањето на работата врз основа на линиски или територијален пристап во голема мера ќе ја олесни работата на аналитичарот и ќе му овозможи да се фокусира единствено на своето поле на работа, со што ќе стекне поголеми знаења токму за тоа поле и ќе изготвува попрецизни анализи.

- Постојана обука и дообука на аналитичарите. Современиот начин на живот и постојаниот напредок на технологијата ја условува потребата од постојана обука на аналитичарите на различни полиња кои имаат допирни точки со нивната работа.

Со исполнувањето на горенаведените услови, во голема мера се зголемува шансата за успешно спроведување на фазата на анализа на информациите.

Фазата на обработка на информациите е составена од неколку постапки, кои се поврзани и меѓузависни. По успешното прибирање на информациите, потребно е да се изврши нивно оценување. При оценувањето на кредибилитетот на информациите, тие се разгледуваат од два различни агли. Првиот агол е веродостојноста на изворот преку кој е добиена информацијата, а вториот агол е точноста на податокот. Во однос на првиот случај, логично е дека со најголема внимателност ќе се пристапува кон информациите добиени од извори со кои немаме претходно позитивно искуство и на нив треба да им се пристапи најкритички. Доколку информацијата е добиена од претходно проверен извор, на неа треба да ѝ пристапиме со повеќе доверба, но сепак и таа треба да биде проверена и споредена со информација која се однесува на истиот предмет на работа, но која е добиена од друг извор. Од друга страна пак, при проценувањето на точноста на информацијата, се зема предвид веројатноста, која

означува дали една информација е одредена, неодредена или пак невозможна. Една информација се смета за вредна само кога е употреблива, а нејзината употребливост зависи од нејзината целовитост, прецизност и навременост. Објективното и совесно приоѓање при оценувањето на информацијата е неопходно, бидејќи секоја лоша процена во оваа фаза ќе има негативни импликации врз точната интерпретација на таа информација[4].

Анализата на информациите ја претставува наредната фаза од нивната обработка. По успешната верификација на информацијата, следува нејзино подредување и поврзување со претходно добиените информации кои се однесуваат на конкретен предмет. Ова не значи дека новодобиената информација ќе претставува хронолошко поврзување на еден предмет кој се обработува. Може да има случај кога ќе добиеме некоја информација која се однесува на ситуација која се случила многу порано, а која му недостасувала на аналитичарот во неговото следење на конкретниот предмет. Ваквата информација која објаснува нешто што се случило пред определено време, може да фрли ново светло врз некои настани кои аналитичарот не можел да ги објасни или да ги поврзе, и да му ја формира комплетната слика за предметот. По подредувањето на информацијата, следи стручна анализа на фактите кои се содржат во неа. Се разгледува поврзаноста на тие факти со претходните знаења за одреден предмет, се проценува нивната релевантност и значење и се склопува мозаикот за одреден предмет на истражување. Во оваа фаза се применуваат сите познати истражувачки методи, вклучувајќи ги аналитичко-синтетичкиот метод, дедуктивниот и индуктивниот метод, методот на анализа на содржината, методот на логичко поврзување на фактите, методот на апстрахирање, методот на докажување и негирање и др[5].

По завршувањето на анализата на информацијата се пристапува кон изготвување на завршните документи и нивна достава до крајните корисници (претпоставените, раководните органи на институцијата, раководните државни органи и сл.). Можеби најважното начело во оваа фаза е начелото на навременост. Изготвените анализи или документи мора да бидат навремено доставени до корисниците кои донесуваат важни одлуки според содржината на доставените документи. Во оваа смисла, особено се важни документите кои се однесуваат на воената и на безбедносната сфера, на пример, кога се работи за навремено

---

[4] Томе Баткоски – *„Разузнавачка и безбедносно-контраразузнавачка тактика",Скопје, 2008,* стр.129
[5] Ibid, стр.133

предупредување и спречување воен или терористички напад, бидејќи со нив му се одзема елементот на изненадување на агресорот. Исто така, многу важен елемент при изготвувањето на завршните документи и нивното презентирање пред крајните корисници, е да се заштити изворот на информациите доколку се работи за човечки извор (да се заштити неговиот идентитет). Ова е важно затоа што овие документи може случајно да дојдат до рацете на некои надворешни лица (или на некои кои немаат доволен степен на безбедносна култура) и да се открие идентитетот на изворот, што пак би имало штетни последици по него ако тоа откритие „протече“ во јавност. На крај, треба да се напомене дека треба да има одлична соработка помеѓу крајните корисници на документите и службите кои ги изготвуваат тие документи, со цел да се унапреди работата и на двете страни.

Во рамките на последниот дел од истражувањето, посветено е големо внимание на континуираната заштита на безбедноста на информациите. Во текот на целиот циклус при работата со информациите, неопходно е да се гарантира нивната заштита. Уште од првите фази на прибирање на информациите, па сè до последната фаза на доставување на крајните анализи до лицата кои донесуваат одлуки врз основа на таа анализа, неопходно е да се заштитува безбедноста на информацијата, со цел таа да не биде неовластено (и предвремено) изнесена пред јавноста, што ќе значи уништување на нејзината корисност. За таа цел, потребно е да се имплементираат мерки и активности за заштитата на безбедноста на информациите, во сите оние институции каде што се ракува со информации од таков вид. Сите мерки и активности за заштита на безбедноста на информациите треба синхронизирано и континуирано да се применуваат за да се избегне нејзино нарушување. Исто така, треба да се напомене дека е потребна постојана обука и реобука на сите оние лица што преку својата работа доаѓаат во контакт со чуствителни информации, со цел создавање и унапредување на нивната безбедносна култура.

2.1. ОПЕРАЦИОНАЛНО ОДРЕДУВАЊЕ НА ПРЕДМЕТОТ НА ТРУДОТ

Варијаблите кои се однесуваат на предметот на истражувањето се токму оние елементи што ја условуваат и ефективноста при ракувањето, употребата и заштитата на информациите.

1. Субјектите, односно непосредните учесници во процесот на прибирање на информациите, ракувањето со нив и нивната заштита се луѓето кои се извори на информациите (доколку добивањето на информациите вклучува човечки извори), припадниците на безбедносните органи кои ги обработуваат тие информации и лицата кои се корисници на тие информации. Значи, оваа варијабла ги вклучува сите оние што биле во контакт со конкретната информација.

2. Условите во кои се планира прибирањето на информациите, во кои се ракува со нив и се внимава на нивната заштита, исто така, имаат големо влијание врз успешноста на нивната примена. Тие можат да се поделат во неколку категории:

- Психичките услови ги опфаќаат процесите на психичкиот живот на човекот.

  Тука спаѓаат психичката подготвеност на лицата кои доаѓаат во контакт со информацијата. Изворот на информацијата треба да се справи со психичкиот притисок кој го носи агентурниот однос (успешно справување со притисокот и стресот при работата). Припадниците на безбедносните органи мора внимателно да ја проучат и да ја оценат информацијата, и врз основа на тоа да изготват точна анализа. На крај, и оние што одлучуваат кои мерки да се преземат врз основа на добиената информација, треба да бидат соодветно психички подготвени да ја донесат вистинската одлука во вистинскиот момент.

- Општествените услови се карактеризираат со повеќе особености, што пак придонесува за нивна класификација во следниве групи:

  - Општоопштествени услови се оние што се однесуваат на постоењето на различни држави, стапката на криминалитет, развиеноста на национална безбедност и сл. Овие услови ја определуваат стратегијата на државата во борбата против внатрешните и надворешните закани.

  - Општествено-економски услови се оние што ја нагласуваат посебноста на секое различно општество во рамките на неговата економска моќ. Овде се мисли на економските односи во една земја, квалитетот на живот, силите на нејзината индустрија и сл. Од безбедносен аспект, овој услов е важен за тоа колку средства им се доделуваат на безбедносните органи и дали тие средства се доволни за сеопфатната борба против внатрешните и надворешните закани.

  - Политичките услови се исто многу важен фактор кој треба да се земе предвид при успешното користење класифицирани информации. Овде во прв ред се мисли на зачувување на безбедноста на информациите и на изворите од

кои се добиени, со цел да се избегнат политички пресметки и јавни осуди на одредени личности или институции.

- Општествената свест како услов ги вклучува: љубовта на граѓаните кон својата земја и силината на нивното чуство за национална припадност (дали сметаат дека е морално исправно одредени информации да ги достават до безбедносните органи), изградување безбедносна култура, формирање цврст став против шпионажа и др.

3. Мотивите на лицата кои работат со информациите се тесно поврзани. Нивна заедничка цел е што поточна интерпретација на тие информации и преземање на вистинските чекори како резултат на добиените информации (планирање на активностите кои се преземаат во безбедносниот сектор).

4. Активностите кои се преземаат со цел успешно искористување на одредени информации претставуваат плански осмислени дејности. Тие вклучуваат одлука дали има потреба од конкретна информација, потоа планирање на кој начин да се дојде до таа информација, конкретното прибирање на информацијата, нејзината обработка и анализа, и на крај преземањето (или непреземањето) одредени постапки врз основа на таа информација. Овде се вбројува и константната грижа за зачувување на безбедноста на таа информација.

5. Методи и средства

Методите и средствата за работа со информациите зависат од видот и од важноста на конкретната информација, од што зависи и начинот на кој ќе се заштити безбедноста на таа информација.

6. Резултатите од успешното искористување на одредена информација можат да се набљудуваат според неколку различни критериуми. Најважниот од нив секако е класификација според степенот на оствареност на целите:

- Позитивниот резултат означува успешно искористување на информацијата. Ова може да биде, на пример, донесување важна стратегиска одлука за државата, спречување терористички акт, откривање шпионажа, спречување криминално дело и сл.;

- Негативниот резултат подразбира неуспешно искористување на една информација. Причини за неуспехот може да бидат неовластено објавување на информацијата во јавност („протекување“ на информацијата), лоша процена за веродостојноста на информацијата, лоша анализа на добиената информацијата и сл.

2.2. ВРЕМЕНСКО, ПРОСТОРНО И ДИСЦИПЛИНАРНО ОПРЕДЕЛУВАЊЕ НА ПРЕДМЕТОТ НА ИСТРАЖУВАЊЕТО

Дисертацијата нуди повеќе пристапи за анализа на ситуацијата со ефективното искористување на информациите во безбедносниот сектор на Република Македонија, но изостанува една концизна временска рамка на предметот на истражувањето, бидејќи прибирањето информации од безбедносна природа и нивната заштита е едно широко поле кое се карактеризира со постојано усовршување и унапредување на активностите кои ги вклучува. Новите побарувања кои се поставуваат пред заштитата на информациите (особено информатичките побарувања), само ја потврдуваат неговата временска неограниченост.

Ова истражување се базира врз еден мултидисциплинарен пристап, кој ги вклучува сите оние науки и дисциплини кои имаат допирни точки со работата на безбедносните органи. Со вклучувањето на одредени безбедносни, криминолошки, психолошки и социолошки аспект сеопфатно се разгледува концептот на успешно прибирање, обработување, користење и заштита на информациите од безбедносен карактер.

2.3. РЕЗУЛТАТИ ОД ДОСЕГАШНОТО ИСТРАЖУВАЊЕ

Досегашните истражувања кои се поврзани со прибирањето, ракувањето и заштитата на информациите од безбедносен карактер во најголема мера се фокусираат на начините на прибирање на информациите, на циклусот на обработка и подготовка на информациите (во разузнавачките кругови познат како разузнавачки циклус). Но, сепак, може да се каже дека недостасува еден сеопфатен пристап што ќе ги обедини сите овие различни фази и постапки (кои секако имаат една заедничка цел, а тоа е ефективното искористување на информациите во безбедноснио сектор) и ќе направи

една целина која ќе го следи патот на информацијата од нејзиното создавање па сè до нејзиното оптимално искористување. Токму тоа е фокусот на ова истражување, да се долови значењето на онаа целина што е предуслов за успешното искористување на добиените информации.

3. ЦЕЛИ И ЗАДАЧИ НА ИСТРАЖУВАЊЕТО

Целите на истражувањето се така насочени да можат да понудат повеќе теоретски и практични решенија за ситуациите кои се појавуваат при работата со информации кои се користат во безбедносниот сектор. Поединечни цели кои ги постигнува ова истражување се следниве:

- формирање теоретска основа која ќе овозможи понатамошно усовршување и дополнување на научните знаења во оваа област;
- ќе понуди насоки за ефективно и оптимално искористување на информациите кои се користат во безбедносниот сектор;
- унапредување на практиката на работа на институциите во безбедносниот сектор на Република Македонија;
- подигнување на безбедносната култура кај сите оние што доаѓаат во контакт со безбедносно чуствителни информации;
- насочување на корисниците на информациите како да ја заштитат безбедноста на тие информации и да го одберат правилниот начин за постапување со нив.

Задачите кои се поставуваат пред ова истражување треба да помогнат во утврдувањето на актуелната состојба при ракувањето со информациите во безбедносниот сектор на Република Македонија, и ги опфаќаат следниве постапки:

- спроведување на емпириското истражување во кое ќе се видат ставовите на лицата кои работат со информации кои се користат во безбедносниот сектор;
- запознавање со теоријата и практиката на безбедносните институции во Република Македонија кои ракуваат со чувствителни информации, и мерките и активностите кои ги преземаат за заштита на тие информации;
- детектирање на ситуациите (доколку постојат такви ситуации) во кои е нарушена безбедноста на информациите и проучување на факторите заради кои настанало тоа нарушување;

- доаѓање до сознанија за тоа до кој степен е развиена соработката помеѓу институциите кои го формираат безбедносниот сектор, и каква е размената на информации помеѓу нив;
- запознавање со веќе завршените трудови (во домашната и меѓународната научна јавност) кои се однесуваат на конкретното поле на истражување.

4. ХИПОТЕТИЧКА РАМКА

4.1. ОПШТА ХИПОТЕЗА

Заштитата на информациите кои се користат во безбедносниот сектор и нивната ефективна обработка и анализа имаат директно влијание врз планирањето на активностите кои се преземаат со цел одржување на внатрешната и надворешната безбедност на Република Македонија.

4.2. ПОСЕБНИ ХИПОТЕЗИ

Успешната заштита на безбедносните информации е во директна корелација со нивното ефективно искористување.

Значењето на информации кои се користат во безбедносниот сектор се зголемува со нивното навремено доставување до крајните корисници.

Поседувањето на потребните информации ќе има директно влијание врз адекватните постапки кои ги преземаат припадниците на безбедносниот сектор и раководните органи кои донесуваат одлуки врз основа на тие информации.

Безбедносниот сектор на Република Македонија има постојана потреба од прилив на нови информации кои се однесуваат на неговиот делокруг на работа.

Со постојаното усовршување на методите за прибирање нови информации се зголемува и приливот на информации кои можат да бидат корисни за безбедносниот сектор на Република Македонија.

Со зголемувањето на безбедносната култура на лицата кои ракуваат со информациите од безбедносен карактер, се зголемува и шансата за оптимално искористување на тие информации.

5. МЕТОДИ И ТЕХНИКИ НА ИСТРАЖУВАЊЕ

Одредувањето на методите и техниките кои се користат во ова истражување во голема мера се условени од изворите на податоците кои се однесуваат на предметот на истражувањето. Овде, во прв ред, треба да се потенцираат следните извори на податоци[6]:

- теоријата на безбедносните науки и нормативно-правната регулатива на безбедносните дејности, кои се однесуваат на теоретскиот фонд кој ги поддржува ваквите дејности, како и законските и подзаконските рамки кои го оградуваат ова поле на дејствување;
- промените во факторите и условите на безбедносните и на разузнавачките дејности, кои ги вклучуваат новонастанатите ситуации и променливите приоритети;
- претходните истражувања во безбедносната област;
- искуствата на странските органи на безбедноста и литературата.

Во проучувањето на предметот на истражувањето се применува теориско-емпириско истражување, односно комбинирана теоретско-емпириска постапка и преку примената на соодветна методолошка постапка се проучени основните карактеристики на постапувањето со информациите од страна на вработените во безбедносниот сектор.

Во ова истражување се применети повеќе методи:

- **Дијалектичкиот метод**, како универзален метод на теоретско мислење е користен при проучувањето на општите законитости кои се застапени во безбедносните активности.;
- **Историскиот метод** се применува во согледувањето на начинот на кој се постапувало со чувствителните информации во минатото (донесување на првите регулативи за заштита на информациите, развивање на методите за доаѓање до информации и сл.).;

---

[6] Цане Т. Мојаноски – *„Методологија на истражување на безбедносните појави", Скопје, 2007, стр.109*

- **Методот на анализа на содржината** се употребува при анализата на документи, прирачници, упатства и директиви. Оние материјали кои се предмет на анализа се однесуваат строго на прибирањето на информации кои се употребуваат во безбедносниот сектор, условите кои треба да се исполнат за нивно успешно искористување и активностите кои се преземаат за задоволување на овие услови.;
- **Компаративниот метод** се користи при воочувањето на разликите во безбедносната практика на различните држави или на разликите помеѓу институциите кои влегуваат во безбедносниот сектор. Со негова помош се добиени резултати кои можат да бидат значајни за усовршувањето на искористливоста и заштитата на информациите.

Кога станува збор за употребата на истражувачките техники, во ова истражување првенствено е користено анкетирањето, а како помошна техника се користи и интервјуто. Целната група на испитаници кои се бидат опфатени со истражувачките техники се припадниците на безбедносните органи на Република Македонија, односно луѓе кои секојдневно се во контакт со безбедносно интересни информации и кои се вклучени во целиот циклус на ракување со тие информации. Овде во прв ред се мисли на вработени во Министерството за одбрана, Министерството за внатрешни работи, Министерството за надворешни работи, Агенцијата за разузнавање, Дирекцијата за безбедност на класифицирани информации, Управата за финансиско разузнавање, како и останатите институции кои го сочинуваат безбедносниот сектор. Исто така, во истражувањето се опфатени и еминентни професори кои работат на полето на безбедносната тематика.

Како истражувачки инструмент во ова истражување се користи анкетен прашалник, како и интервју, и овие техники ги опфаќаат главните аспекти при работата со информациите. Врз основа на добиените резултати и спроведената анализа се добиени важни заклучоци и се предложени нови решенија и механизми за подобрување на работата со информациите кои се користат во планирањето на активностите на безбедносниот сектор.

Вака спроведеното емпириско истражување претставува добра основа и начин за доаѓање до размислувањата и ставовите на луѓе кои се доволно практично и теоретски потковани за да дадат одговор на клучните прашања од оваа тематика.

6. ОПШТЕСТВЕНА И НАУЧНА ОПРАВДАНОСТ НА ИСТРАЖУВАЊЕТО

Концептот за научното значење на истражувањето кое се однесува на аспектот на информациите и информираноста се согледува во продлабочувањето на теоријата која се однесува на ракувањето со нив. Бидејќи ракувањето и заштитата на информациите е една дејност која може да се надополнува и практично (како поддршка на ова тврдење стои фактот дека голем дел од унапредувањето на мерките и активностите за заштита на информациите се темелат врз основа на претходни негативни практични искуства), сепак сметам дека теоретската поткованост на сите оние што работат со информации важни за безбедноста треба да биде основата на нивната понатамошна работа. Оттаму, научното значење на ова истражување е насочено токму кон стекнувањето нови и проширени знаења за ракувањето со информации кои се користат во безбедносниот сектор. Исто така, ова истражување ќе помогне и во пополнувањето на теоретската празнина која се однесува на подетаљното проучување на мерките и активностите кои треба да се преземаат со цел да се обезбеди заштитата на информациите, преку катагоризирање и сублимирање на постојните теоретски знаења и практичните искуства кои ја допираат таа тема.

Општественото значење на истражувањето за значењето на информациите кои се користат во рамките на безбедносниот сектор, односно на нивната специфична улога во одржливоста и унапредувањето на конструкцијата на општествениот систем, најдобро може да се согледа само доколку го визуелизираме ракувањето и заштитата на тие информации како средство за сопствена општествена одбрана и за зајакнување на позицијата на своето општество и држава на меѓународен план. Преку умешното користење на прибраните информации, раководните органи во Република Македонија можат да донесуваат одредени државнички одлуки или изготвувањето на државни стратегиски и тактички планови, што на државата би ѝ донело предност во различни полиња. Исто така, со ефективното користење на информациите може да се спречат различни општествени појави кои би имале негативни импликации врз граѓаните на Република Македонија. Имено, преку навремено информирање, нашите безбедносни органи би можеле да спречат разни терористички закани, агресии од друга држава, да се откријат посериозни кривични дела (убиства, тешки кражби, трговија со дрога и сл.) и да се заштити населението на многу други начини.

Глава 1

Информација и информирање

1.1. Општо за поимот информација

Во последните неколку декади, голем број научни области (особено психологијата, теоријата на комуникации и информатичките науки) се фокусираат на истражувањето на начините на кои луѓето прибираат, чуваат и пренесуваат информации. Во минатото, луѓето го обезбедувале својот опстанок преку своето чувство за собирање, разбирање и пренесување одредени информации за околината во која живееле. Денес, во времето на информатичко-технолошката и комуникациска средина во која живееме, значително е зголемена и способноста на човекот да се справува со информациите кои го опкружуваат и засегаат. Голем број дисциплини, секоја со своја сопствена дефиниција за поимот информација, се обидуваат уште повеќе да го унапредат процесот на ефективно искористување на информациите преку дополнителни истражувања на ова поле.

Скоро секоја научна дисциплина денес го користи концептот информација во свој контекст и во однос на свој специфичен феномен. Во истражувањето на овој поим, многу е лесно да се изгуби ориентација како резултат на бројните истражувања кои се посветени на концептите на информација и информирање. Ваквите истражувања претставуваат еден интердисциплинарен микс, почнувајќи од кибернетиката (науката за комуникациските и контролните процеси), оперативните истражувања (анализа на процесите за донесување одлуки), менаџментот со разни операции, системската анализа, психологијата, социологијата, политичките науки и многу други науки[7]. Информацијата и информирањето имаат трансдисциплинарна природа, што пак е причината за нивно различно дефинирање и толкување во еден широк дијапазон од науки.

Токму затоа, потребно е да се направи една анализа на поимот информација и да се понуди еден краток преглед на различните толкувања и сфаќања за овој поим. Денес постојат голем број пристапи кон концептот информација кои се вградени во различни теоретски структури. Ваквиот пристап доведува до низа сериозни проблеми, бидејќи поимот информација во денешно време има добиено огромно проширување на своето значење. На прашањето „Што значи поимот информација?“ во денешно време има голем број одговори. Така, на пример, за информација се смета она што го објавуваат

[7] Gackowski J. Zbigniew - *„Subjectivity Dispelled: Physical Views of Information and Informing”*, Informing Science: the International Journal of an Emerging Transdiscipline Vol.13, California, 2010, p.35

весниците, радијата и телевизиите. По информации одиме на шалтерот на кој пишува „Информации“ во поштите, банките, факултетите и сл. Информациите се знаењето што го пронаоѓаме во книгите и во различните видови извештаи и документи, а истото тоа знаење ја претставува основата на научните истражувања, економијата и политиката. Информацијата го претставува основното обележје на информатичката доба, информатичката наука, науката и технологијата и општеството во кое живееме, а информациите се употребуваат во најразлични ситуации, од употребата во секојдневниот живот, па до употребата во специјализираните научни подрачја. Од многуте значења на овој поим, во ова истражување информацијата ќе се разгледува од концептот на пренесување на одредена порака.

Поимот информација има латинско потекло (*Informatio* - поим, претстава, сознание) и употребата на информацијата во антиката ни покажува дека таа е користена во смисла на можностите за креирање (формирање) на нови знаења[8]. Дефиницијата за информација треба да го претстави феноменот информација преку една прецизна дескрипција на нејзината природа, преку воочување на разликата помеѓу информацијата и останатите поврзани концепти, како податокот, значењето, знаењето, а во исто време треба да ја воочи и суштинската разлика помеѓу овие концепти[9]. Информацијата може да се претстави како збир на вредности, како порака, како концепт, идеја, дизајн и слично, и токму затоа е многу тешко да се направи една комплетна дефиниција без да се изостави барем некој од овие елементи[10]. Оттука, во литературата се изведени голем број дефиниции за поимот информација, кои имаат за цел што попрецизно определување на овој поим[11]. Информацијата во својата

---

[8] Horić, Andrea - *„Informacija – Povijest jednog pojma - O Capurrovom razumijevanju pojma informacije”*, Zagreb, 2007, str.1

[9] Losee, M. Robert - *„A Discipline Independent Definition of Information”* – Journal of the American Society for Information Science 48, Chappel Hill, 1998, p.6

[10] Gackowski, J. Zbigniew - *„Subjectivity Dispelled: Physical Views of Information and Informing”*, Informing Science: the International Journal of an Emerging Transdiscipline Vol.13, California, 2010, p.36

[11] Под информација се подразбира само она сознание кое го менува знаењето на примачот, односно сознанието што дава ново знаење, различно од претходното. - Davis, G. B. and Olson, M. H. - *„Management Information Systems:Conceptual Foundations, Structure, and Development*”, New York, 1985McGraw-Hill, p.200
Една друга дефиниција, која ја дава Р.Р.Бошковиќ гласи „Информација е извор на стекнување сознанија за појави, предмети и настани во одреден простор и време".
Во трудовите на I.G.Wilson и M.M.Wilson, прифатено е следново објаснување „Кога податоците т.е. зборовите, броевите и специјалните знаци ќе се поврзат во една изјава, односно реченица, се добива информација".

суштинска форма претставува трансмисија на симболи, кои имаат одредено значење за лицата меѓу кои се пренесува таа информација. Под информација се подразбира само она сознание што го менува знаењето на примачот, односно сознанието што дава ново знаење, различно од претходното. До информации се доаѓа преку податоци. Со обработка и анализирање на овие податоци се добиваат информации кои овозможуваат да се конципираат поквалитетни плански одлуки[12].

1.2. Терминолошки дивергенции на поимите податок и информација

Бидејќи податокот и информацијата неретко се користат како синоними, многу е важно да се направи дистинкција помеѓу овие два поими. Во обидот да се направи тоа, многу нивни карактеристики треба да бидат разграничени и дефинирани на начин што ќе го отсликува експлицитно фокусот и перспективата од кои тие се составени (нивните составни делови и спецификации).

Податокот е основниот градбен блок на информацијата. Тоа е телефонскиот број кој случајно сме го забележале на идентификаторот за броеви на телефонот, натписот во дневен весник, регистарските таблички на возилата со кои се разминуваме додека возиме или деловите од разговорот кои сме ги наслушнале додека се возиме во автобус. Податоците се буквално секаде околу нас. Токму заради ваквата неорганизирана природа на податоците е неопходно тие да подлегнат на обработка со цел да бидат искористени. Во денешно време, кога има изобилство на податоци кои можеме да ги добиеме, споделуваме и мемориграме преку интернетот и другите форми на мрежни системи, проблемот не е дали има доволно податоци, туку дали може да се направи дистинкција на потребните од непотребните податоци[13]. Податокот е поим кој

„Информацијата е збир на податоците за сите можни објекти, појави и процеси. Таа се претставува во облик на цртеж, текст, звучни и светлосни сигнали, енергетски и нервни импулси и сл. Според критериумот на настанувањето, информациите се делат на елементарни (ги претставуваат процесите и појавите на мртвата природа), биолошки (ги претставуваат процесите во растителниот и животинскиот свет) и социјални (ги претставуваат процесите во општеството). Информациите кои ги создава и ги користи човекот се делат на масовни (друштвено-политички, научно-популарни и сл), специјални (научни, технички, економски и сл.) и лични“.- Enciklopedija Matematika-Fizika

[12] Бакрески, Оливер - *„Координација на безбедносната заедница во Република Македонија”*, Скопје, 2005, стр.43

[13] Metscher, Robert and Gilbride Brion - *„Intelligence as an Investigative Function”*, International Foundation for Protection Officers, 2005, p.3

ја опишува и ја квантифицира состојбата на некој процес. Податокот го посочува фактот кој претставува карактеристика за нешто (број, збор, слика или звук) и претставува симболички и формализиран приказ на фактите, поимите и инструкциите, и е погоден за комуникација, интерпретација и преработка од страна на луѓе или машини. Тој претставува порака која може да се искористи, и доколку таа порака е еднозначна и точна, тогаш таа претставува неоспорлив факт, односно информација.

Информацијата е податок кој има одредено значење или употребливост во даден контекст.[14] Или со други зборови, информацијата е она коешто останува кога сè она што е ирелевантно е исфрлено. За информација се смета обработениот податок кој ќе ни помогне да ги изградиме нашите ставови, процени и предвидувања.[15] Дефиницијата за информацијата означува дека таа е составена од податоци кои се ставени во некој контекст кој има одредено значење, додека самите податоци се надвор од контекст, тоа се само сурови спознанија. Со други зборови, податокот е бескорисен се додека не пренесува одредена информација. Информацијата е збир од знакови кои на примачот му значат нешто, односно откриваат нешто ново, и таа е примена и сфатена порака[16]. Таа е резултат на моделирањето, форматирањето, трансформацијата и организирањето на податоците на начин кој го зголемува знаењето на примачот на таа информација, односно информацијата е значењето кое човекот им го доделува на податоците преку нивна трансформација. Информацијата го претставува знаењето со коешто сме се стекнале преку логичката интеграција и интерпретација на прибраните податоци и е доволно сеопфатна за да може да се донесуваат одлуки базирани на нејзините постулати и тврдења.

---

[14] Информацијата има многу поголемо значење од податокот. Таа претставува знаење кое е специјално подготвено со цел да ги исполни уникатните побарувања на корисниците на таа информација. – Krizan, Lisa - *„Intelligence essentials for everyone"*, Joint Military Intelligence College, Washington DC, 1999, p.7

[15] Metscher, Robert and Gilbride, Brion - *„Intelligence as an Investigative Function"*, International Foundation for Protection Officers, 2005, p.4

[16] Gackowski, J. Zbigniew - *„Subjectivity Dispelled: Physical Views of Information and Informing"*, Informing Science: the International Journal of an Emerging Transdiscipline Vol.13, California, 2010, p.39

1.3. Општо за информирањето

За да постои информирање, потребно е да постои разлика во знаењата кај двете страни во однос на предметот што го опфаќа информацијата. Информирањето претставува процесирање на информации помеѓу две страни, при што едната страна пренесува одредено знаење, а другата страна се здобива со проширување на своите знаења за одреден предмет или состојба. Притоа, страната која е информирана, со помош на новостекнатите спознанија може да ја унапреди својата состојба во средината или во општеството во кое живее, може да ги насочи своите активности во онаа насока која ќе му донесе најголеми придобивки, да ги промени своите ставови во однос на одредени состојби и др. (всушност, можностите се неограничени и зависат од природата и карактеристиките на страната која е информирана). Со други зборови, мора да постои почетна разлика во знаења помеѓу информирачот и информираниот за предметот за кој се однесува информацијата. Исто така, за да постои информирање, информацијата која се пренесува мора да биде искористлива и доволно квалитетна за да може да предизвика одредени случувања (разјаснување на нејаснотии, донесување одлука дали да се дејствува или не). Информирањето е неефикасно доколку преку него се пренесени дезинформации или информации кои лицето кое се информира веќе ги знае.[17]

Треба да се сфати дека информирањето е неопходно за да се оствари успех во работата во оние професии или области кои се поврзани со користење на информации.

1.3.1. Основните компоненти на информирањето

Ефикасноста и ефективноста во работата со информациите полека станува еден од најзначајните фактори за успех во голем број сфери на човечки активности, а во исто време истражувањето на информациите станува сè покомплексно и бара сè поголеми специјализирани знаења и техники. Овде ќе се разгледа динамичниот процес на информирање преку кредибилитетот на неговите составни делови и каналите кои се користат за да се оствари тоа информирање.

---

[17] Gackowski J. Zbigniew - *„Subjectivity Dispelled: Physical Views of Information and Informing"*, Informing Science: the International Journal of an Emerging Transdiscipline Vol.13, California, 2010, p.39

Моделот за информирање е составен од три делови: извор на информирањето (информатор), комуникационен (информирачки) канал/и и примач на информациите (информиран).

- **Изворите на информирање** можат да бидат активни или пасивни.
  - Активни извори за информирање – извори кои според својата природа служат за трансмисија, дисеминација или емитирање на информации. Ова се субјекти кои се активни и кои преку својата активност се трудат да го пренесат своето знаење (своите информации) на поширок круг на луѓе. Пример за вакви извори се научници, професори, политичари, новинари, борци за човекови права, проповедници и сл.
  - Пасивните извори се извори кај кои информациите се добиваат преку опсервација, испитување, експериментирање, мерење, анализа и сл. Ова се историски и археолошки артефакти, временски прогнози, начини на однесување, лабораториски истражувања и сл.[18]
- **Каналите за информирање** ги поврзуваат изворите на информации и примачите на информациите. Каналите за информирање (или комуникација) ги претставуваат начините на кои информацијата се пренесува од информирачот до информираниот. Трансферот на сигнали (информации) преку каналите за информирање го претставуваат процесот на информирање. Во однос на каналите за информирање, информирањето може да биде директно или индиректно. Во директното информирање, информацијата се пренесува директно од информирачот (изворот) до информираниот, односно преку персонален, непосреден контакт (лице в лице). Во индиректното информирање, информацијата се пренесува преку средства за посредна комуникација. Ваквата посредна комуникација може да се оствари на неколку различни начини (писмо, телефон, телефакс, компјутер и сл.).[19]
- **Примачи на информации** (јавноста, студентите, гласачите, донесувачите на одлуки) се оние кај кои информациите кои се пренесуваат и информирањето како процес треба да предизвика проширување на знаењето или одредени

[18] Gackowski J. Zbigniew - *„Quality of Informing – Bias and Disinformation Philosophical Background and Roots"*, Issues in Informing Science and Information Technology, Vol.3, California, 2006, p.732

[19] Gackowski J. Zbigniew - *„Informing for operations – The first Principia"*, Issues in Informing Science and Information Technology, Vol.5, California, 2008, p.688

промени во нивните ставови, однесувања и постапки. Примачите на информациите можат да бидат едноставни или комплексни ентитети, да бидат индивидуални лица или организации, па дури и роботички уреди кои се контролираат нумерички или преку вештачка интелигенција.[20]

Ова истражување ќе се обиде да ги отстрани нејаснотиите и недореченостите кои ги опкружуваат поимите информации и информирање, ќе ја нагласи нивната важност и ќе постави основа за нивна ригорозна дескрипција, анализа и синтеза, како процес и како зголемување на знаење.

[20] Gackowski J. Zbigniew - *„Quality of Informing – Bias and Disinformation Philosophical Background and Roots"*, Issues in Informing Science and Information Technology, Vol.3, California, 2006, p.732

Глава 2

Односот информација-информирање

2.1 Улогата на информирањето

Земајќи ги предвид сите дефиниции кои беа дадени за поимот информација во претходната глава (и прифаќајќи ги сите ризици и можности за дополнителни толкувања или одредени несогласувања за овој поим кои со себе ги носат ваквите дефиниции), потребно е сега да се фокусираме на односот помеѓу информацијата и информирањето. Информациите и информирањето се неопходни и конзистентни во многу различни околини и претставуваат една од основните карактеристики на човечкиот род, а тоа е можноста субјективно да се процесираат спознанија и факти и да се генерира одредено знаење (разбирање, спознавање, перцепирање)[21]. Кога веќе стана очигледно дека информациите и информирањето имаат витално значење за општеството како целина и за граѓаните како индивидуи, голем број научници се зафатија со нивно проучување. Во последните 50 години, нагло е зголемен бројот на истражувања кои се однесуваат на дефинирањето на поимите, начините на прибирање информации, пренесувањето на информациите, нивното толкување и анализа и нивното искористување.

Ако информаците се составени од зборови и фрази, тогаш информирањето е значењето и знаењето кое произлегува од тие зборови и фрази. Генерално, да се информира некој значи да му се пренесе одредено знаење. Информирањето може да се сфати како процес преку кој одреден човек или групација на луѓе се здобиваат со нови знаења преку информациите кои им се доставени или презентирани, односно се здобиле со ново знаење за одреден предмет на интерес[22].

Информирањето има свој придонес во сите области на човечки активности. Тоа претставува наука и уметност за преземање практични постапки кои ќе придонесат за зголемување на ефективноста, етичноста и/или ефикасноста во проширувањето на знаењето и контролата врз реалноста. За да биде сметано за наука, информирањето мора да биде ефективно и постојано. Тоа претставува една систематска студија на содржината и формата на реалноста (податоци и информации, и нивната меѓусебна релација), резонирањето и исходите, гледано од перспективата за целта и

[21] Faibisoff G. Sylvia and Ely P. Donald - *„Information and Information Needs"*, Commissioned Papers Project, Teachers College, Columbia University, US, p.2

[22] Ibid, p.4

карактеристиките на информирањето.[23]

Информирањето е трансдисциплинарно бидејќи се појавува во сите дисциплини. Во исто време, информирањето е и интердисциплинарно, бидејќи процесот на информирање најчесто има пресек со една или повеќе дисциплини кои се карактеристични за изворот на информациите и примачот на информациите. Потеклото на информирањето може да се бара во: реториката; теоријата на комуникации; филозофијата и науката; политичката филозофија и политичките науки воопшто; образованието; новинарството; лингвистиката; маркетингот; психологијата; социологијата; компјутерските науки; менаџментот; правото; воените науки; и многу други, т.е. претставува еден вистински интердисциплинарен микс. Информирањето има развиено свои сопствени теории и методи кои подоцна се применуваат во планирањето, дизајнот и имплементацијата на практични решенија и апликации.

Денес информирањето претставува посебно поле на истражување и практични постапки со цел да се прошири знаењето и да се зголеми ефективноста, етичноста и ефикасноста во контролирањето на реалноста. Огромен број науки од различна природа се занимаваат со истражување на информациите и информирањето во контекст на своето специфично поле на интерес.

2.2. Меѓузависноста на информациите и информирањето

Информациите и информирањето се хетерогена колекција на различни дефинирања и објаснувања, направени од различни перспективи (психолошка, социолошка, политичка и сл.) и се многу блиску поврзани во еден интерактивен однос.[24]

Информациите се употребуваат на дневно ниво во различни контексти и со различна намена. Едноставното споделување на одредена информација во различен формат преку широк дијапазон на медиуми не ја гарантира рецепцијата и разбирањето на таа информација. За да има успешно информирање, мора да постои размена на

[23] Gackowski J. Zbigniew - *„Informing as a discipline – An initial proposal"*, Issues in Informing Science and Information Technology, Vol.13, California, 2010, p.171

[24] Gackowski J. Zbigniew - *„Subjectivity Dispelled: Physical Views of Information and Informing"*, Informing Science: the International Journal of an Emerging Transdiscipline Vol.13, California, 2010, p.36

одредено значење (знаење) - мора да се разберат информациите кои се пренесуваат. Само ваквото разбирање може да биде гаранција дека постои информирање. Информирањето е истовремено многу едноставно и многу комплексно – едноставно во смисла на тоа што може да се разложи на специфични, одредени, квантитативни елементи кои овозможуваат прекин на процесот на информирање во кој било момент; а комплексно во смисла на тоа што сите овие елементи мора да бидат во целина и во одреден контекст, бидејќи информирањето е процес.[25] Бидејќи може да се каже дека информациите и информирањето се меѓусебно поврзани и зависни, потребно е да се разгледаат динамичките карактеристики на нивната меѓузависност.

За да постои ефективно информирање, мора да бидат исполнети следниве побарувања:

- Да има ефикасна дисеминација на информациите. Голем број истражувања истакнуваат дека најголемиот проблем за информирањето го претставува временскиот јаз помеѓу продукцијата и дисеминацијата на информацијата.;
- Да има филтрирање во поглед на квалитетот на информациите. Сите информации мора да бидат проверени за прецизност, релевантност и квалитет пред да бидат пренесени.;
- Потребата од вистинските информации во вистинско време.;
- Потребата за добивање информации во посакуваната форма, најчесто усна или писмена, и на разбирлив јазик.;
- Потребата за активно, селективно добивање информации. Идеалната ситуација овде би била добивањето на вистинската информација без да се побара.;
- Потреба да се добие одредена информација лесно и економично.;
- Потребата да се биде во тек со настаните и со активностите кои се во тек.;
- Доколку има потреба од тоа, да се поседуваат неопходните познавања од работа со средствата за информирање (на пример, компјутер, криптосистем).;
- Да се поседува способност за поврзување на добиените информации со претходно добиени информации за истиот предмет на интерес.[26]

---

[25] Faibisoff G. Sylvia and Ely P. Donald - *„Information and Information Needs"*, Commissioned Papers Project, Teachers College, Columbia University, US, p.4

[26] Ibid, p.6

Кога се работи за информирање, нереално е да се очекува дека тоа ќе биде секогаш објективно, бидејќи многу често е зависно од намерите, емоциите и знаењето/незнаењето на учесниците.

2.3. Потреба од информации и информирање

Потребите за информации се одредуваат преку неколку постапки, меѓутоа како најглавни од овие може да се истакнат неопходната потреба од одредена информација во временски чувствителен интервал, ширината на потребата за информации и можноста за остварување пристап до потребната информација. Јасно е дека се неопходни дополнителни истражувања на полето на потребите за информации и дека индивидуите и институциите кои имаат потреба од информации мора да бидат запознаени со генералните постулати кои веќе се прифатени и се составен дел на одредувањето на потребата за информации.

При одредувањето на потребата за информации мора да се земат предвид одредени прашања. Меѓу нив најважни се следниве: „Дали потребите за информации на крајните корисници се добро разбрани?“, „Дали е направен комплетен план за тоа како ќе се дојде до посакуваните информации?“, „Колкава е веројатноста да се дојде до посакуваните информации?“ и „Колкав временски период се има на располагање за да се дојде до тие информации?“.

Може да се направи една генерализација и да се каже дека потребите за информации се поврзани со професионалното поле на интерес на индивидуите или институциите и дека информациите се прибираат со цел да се унапреди нивната работа. Притоа, зачетокот на овие потреби може да има две форми. Првата форма е кога потребата се обликува според одредена активност, како, на пример, решавање проблеми или донесување одлуки, па се бараат дополнителни информации со цел да се има на располагање колку што е можно поголемо знаење за одредена ситуација која треба да се разреши, и да се намали колку што е можно повеќе веројатноста за донесување погрешна одлука или решение. Втората форма е полатентна од првата и се манифестира преку пасивната рецепција на информации кои се складирани како знаење. Имено, во овој случај, проширувањето на знаењето само по себе ја наметнува потребата за дополнителни информации. Меѓутоа, овие две форми на поттикнување на

потребите за информации не треба да се гледаат како статични или разделени, туку напротив, тие се многу блиски и меѓусебно испреплетени и се варијабилни со текот на времето.[27]

Оваа генерализација, за која со сигурност може да се каже дека не претставува своевидна методологија за објаснување на потребите на информации, сепак претставува многу конструктивен пристап кон разбирањето на потребите за информации. Преку неа се издиференцирани неколку елементи кои се формативни фактори во одредувањето на потребите за информации. Тие фактори се: субјектот кој има потреба од информации, природата на информацијата и квалитетот на информацијата.

а) Субјекти кои имаат потреба од информации

- Луѓето имаат тенденција да ги бараат информациите кои се најлесно достапни.;
- Луѓето следат одредени постапки кога бараат информации. Средствата за јавно информирање се секогаш првиот извор на информации во кои луѓето пробуваат да го најдат она што ги интересира, а во последниве децении интернетот ја презема улогата на најголем информатор на јавноста.;
- Корисниците на информациите најчесто не се свесни за изворите на информациите и како да ги користат тие извори. Оваа генерализација сепак зависи од софистицираноста и познавањата на корисникот. Во денешно време, може да се каже дека не постои недостаток на информации за било кој објект на интерес, меѓутоа предизвикот е да се најдат вистинските и точни информации од најрелевантните извори.;
- Посредната комуникација помеѓу луѓето сè уште и примарниот извор на информации. Бројни истражувања покажуваат дека луѓето кога имаат потреба од одредени информации, прв избор им се роднините, пријателите и соседите.;
- Различни луѓе имаат различни потреби за информации. Потребите за информации зависат од возраста, полот, професионалните ангажмани, финансиската состојба, хиерархискиот статус во општеството и сл.[28]

---

[27] Faibisoff G. Sylvia and Ely P. Donald - *„Information and Information Needs"*, Commissioned Papers Project, Teachers College, Columbia University, US, p.8

[28] Faibisoff G. Sylvia and Ely P. Donald - *„Information and Information Needs"*, Commissioned Papers Project, Teachers College, Columbia University, US, p.9

б) Природата на информацијата

Природата и содржината на потребните информации се различни и комплексни, и варираат од дисциплина до дисциплина и од група до група. Исто така, постојат и разлики во ширината на информациите кои се бараат и кои се потребни. Понекогаш се потребни општи информации за одреден предмет на интерес, а понекогаш може да се укаже потреба од специфични информации кои се однесуваат на некој многу тесен предмет на интерес.

в) Квалитетот на информацијата

- Квалитетот на информациите не треба да се одредува според квантитетот на податоците кои биле потребни за да се изготви таа информација. Многу присутен е ставот дека со прибирањето на колку што може повеќе податоци ќе се направи поквалитетна информација, затоа што ова може да доведе до ситуација во која самата бројност на информациите оневозможува нивна навремена и прецизна анализа. Квантитетот на информациите може да го спречи нивното ефективно искористување. Особено во денешно време, кога има огромен број информации, може да дојде до ситуација да се поседуваат премногу информации за одреден предмет на интерес, а да се нема доволен капацитет за да се обработат сите (без разлика дали станува збор на индивидуа или институција).;
- Квалитетот на една информација во голема мера зависи од оној што ја изготвува. Доколку лицето кое ја изготвува информацијата има широки познавања од областа на која се однесува информацијата, експоненцијално се зголемува и квалитетот на самата информација.;
- Бидејќи квалитетот на информацијата го оценуваат крајните корисници за кои е наменета таа информација (без разлика дали се работи за јавноста или за донесувачи на одлуки), нејзината валоризација и конечниот суд за квалитет зависат од тие корисници. Колку поголеми познавања имаат крајните корисници за областа на која се однесува информацијата, толку поверодостојно ќе можат да го проценат нејзиниот квалитет.;

- Квалитетот на информацијата може да биде одреден според некои нејзини карактеристики, а тоа се точноста, релевантноста и веродостојноста.;
- Навременоста на информацијата е тесно поврзана со квалитетот на информацијата. Квалитетната информација може да биде залудна доколку не е доставена во оној интервал кој е клучен за нејзино искористување.[29]

Бидејќи во последниве децении значително се зголеми потребата за информираност, потребно е да се направи идентификување на крајните корисници и запознавање со нивните карактеристики и објекти на интерес, како и идентификување на специфичните информации кои им се потребни на крајните корисници. Откако ќе се направи ова, неопходно е информацијата да биде претставена во најсоодветната форма и приспособена на побарувањата на крајните корисници, а како крајно побарување е и постоењето на интеракција и повратна врска (фидбек) помеѓу создавачот на информацијата и крајниот корисник.

Сметам дека овде е корисно да се напомене дека во согласност со остатокот од моето истражување, ќе направам едно насочување преку кое потребите за информации ќе бидат проучувани во контекст на безбедносниот сектор и неговите специфични потреби.

[29] Faibisoff G. Sylvia and Ely P. Donald - *„Information and Information Needs"*, Commissioned Papers Project, Teachers College, Columbia University, US, p.14

Глава 3

Информациите и нивното значење во работата на безбедносниот сектор

3.1. Информирањето како услов за ефикасно планирање во безбедносниот сектор

Планирањето е исклучително тежок процес во кој е потребно големо искуство, знаење, размислување, расудување и барање решенија за разни мали и големи проблеми. Планирањето успешно се остварува само ако се заснова на соодветни информации. Ако не се располага со бројни и сигурни информации, не е можно да се спроведе анализа на работењето во претходниот период, да се предвиди иднината, да се оствари процесот на планирање. Според ова, може да се сумаризира дека планирањето како процес тешко се остварува и за тоа постојат повеќе причини, меѓу кои:

- недоволно информирање, односно недостиг на соодветни информации;
- невозможно е точно да се предвидат идните настани;
- мора да се земе предвид и временската димензија, бидејќи за колку подолгорочен период се прави планирањето, се зголемува можноста за евентуални грешки и неточности.

Како што може да се види погоре, недостигот на соодветни информации е еден од основните предуслови за погрешно планирање. Информациите и информирањето овозможуваат да се конципираат што поквалитетни плански одлуки

3.2. Информациите и безбедносниот сектор

Една од одликите на луѓето е желбата за поголемо знаење со цел да ја намалат несигурноста при донесувањето најразлични видови одлуки. Низ историјата, многу пати се покажало дека доаѓањето до точна информација и нејзината правилна употреба им било од круцијално значење на донесувачите на одлуки пред да донесат став за тоа како да се разреши одредена ситуација. Знаењето и информациите, доколку се инкорпорираат во процесот на донесување одлуки, може да се покажат како факторот кој ќе одлучи дали одредена ситуација ќе се разреши успешно или ќе доживее фијаско. Информацијата го претставува најсилното оружје на секој што умее и што може да ја дофати во вистинско време и да ја искористи на вистински начин за да може да ја

координира определената задача што треба да ја материјализира со успех.[30] Таа е потребна со цел да се донесат одлуки – колку е подобар квалитетот и сеопфатноста на информацијата, толку подобра ќе биде одлуката. Кога не се поседуваат доволно информации за некој предмет, донесувањето одлука е многу потешко, и таа одлука треба освен врз информациите да се базира и врз претпоставка, искуство, логика и возможност.[31] Со цел да се заштитат интересите и вредностите на една држава, како и нејзината внатрешна и надворешна безбедност од можните рапидни промени на светско, на регионално или на локално рамниште во иднина, раководните и безбедносните органи на државата мора постојано да добиваат навремени и соодветни информации кои се неопходни за успешно водење на сите витални државни функции.[32] Потребно е да се одржи максимална будност, флексибилност и оперативна агресивност со цел успешно спротивставување на константната еволуција и зголемувањето на безбедносните закани и предизвици, што пак значи дека за успешно остварување на своите цели и задачи, конституентите на безбедносниот сектор мора да прибираат, да оценуваат и да анализираат податоци кои се поврзани со националната безбедност[33].

Меѓутоа, неизбежно е поставувањето на неколку прашања кои се однесуваат на тие податоци: Каков вид податоци им се потребни на институциите кои го сочинуваат безбедносниот сектор? Како се определуваат тие потреби? На кој начин да се дојде до тие податоци? Кога и во каква форма ќе се добијат тие податоци? Дали е потребен безбедносен сертификат за пристап до конечната информација, односно дали таа информација треба да се класифицира?[34] На каков начин да се заштити таа

---

[30] Бакрески, Оливер - *„Координација на безбедносната заедница во Република Македонија"*, Скопје, 2005, стр.42

[31] Carter, L. David - *„Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies"*, Michigan, 2006, p.147

[32] Внатрешната безбедност се однесува на непречено функционирање на конкретниот уставен поредок, односно на функционирањето на општествено-економскиот и политичкиот систем на државата, како и заштитеноста на другите вредности и добра и објекти на заштита.
Надворешната безбедност во суштина се однесува на заштитата на независноста, суверенитетот на земјата и територијалната целокупност. – Котовчевски, Митко – *„Национална безбедност на Република Македонија"*, прв дел, Скопје, 2000, стр.18

[33] Безбедноста е состојба која се однесува на: светот, континентот, регионот, националната држава и во неа на вредносниот систем (основниот национален капитал); природата; човекот; човековите творби; културното наследство; културата; парите; институциите и слично. – Спасески, Јордан – *„Човекот и безбедноста"*, Годишник на Факултетот за безбедност, Скопје, 2010, стр. 26-27

[34] "Безбедносен сертификат" е документ со кој се потврдува дека правното или физичкото лице има право на пристап и користење на класифицирани информации. - *„Закон за класифицирани информации"*, Службен весник на Република Македонија бр.9/04 од 27.02.2004 година.

информација? Дали и со кого треба да се сподели таа информација? Колку време да се чува таа информација? За да се зголеми ефикасноста при работата на безбедносниот сектор, одговорите на овие прашања треба да бидат јасно дефинирани и да им бидат добро познати на сите конституенти на тој сектор.[35]

Информациите кои се од интерес за безбедносниот сектор можат да бидат од различен вид. Имено, тоа може да биде секоја информација или материјал изготвен од државните органи, органите на единиците на локалните самоуправи, јавните установи и служби, разни правни и физички лица кои се однесуваат на безбедноста и одбраната на државата, нејзиниот територијален интегритет и суверенитет, уставниот поредок, јавниот интерес, слободите и правата на граѓаните. Исто така, тоа може да бидат најразлични записи на информации, вклучувајќи пишани или печатени текстови, карти, шеми, фотографии, слики, цртежи, гравури, скици, работни материјали, како и звучни, гласовни, магнетски или електронски, оптички или видео снимки во која било форма, како и преносliва опрема за автоматска обработка на податоци со вградени или преносливи мемории за складирање податоци во дигитална форма.[36] Институциите на безбедносниот сектор мора да ги земаат предвид сите најнови случувања кои се релевантни за нив, да го проценат нивното значење и импликациите кои тие можат да ги нанесат и да им помогнат на донесувачите на одлуки да ги пополнат празнините во нивното познавање на одредена ситуација или одреден предмет, како и да направат процена за можни случувања и нивните исходи и последици. Успехот на безбедносниот сектор зависи од комбинација на различни фактори, па за таа цел институциите кои го сочинуваат тој сектор мора да ги разгледуваат безбедносните ризици и закани од колку што е можно повеќе гледни точки, а за да го направат тоа, потребно им е да поседуваат доволно информации кои се однесуваат на нив. Токму затоа, активностите на безбедносниот сектор мора да вклучуваат широк дијапазон на методи и начини на работа со цел да произведат навремени, точни и релевантни информации.

Тоа што е значајно и што произлегува од оваа констатација е потребата од успешно менаџирање со податоците и информациите кои се користат во безбедносниот сектор, односно нивно навремено прибирање, нивна обработка и анализа и нивна

---

[35] Carter, L. David - *„Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies"*, Michigan, 2006, p.4

[36] *„Закон за класифицирани информации"*, Службен весник на Република Македонија бр.9/04 од 27.02.2004 година

навремена дисеминација до раководните државни или безбедносни органи. За да се обезбедат потребната ефикасност, економичност и навремена адаптација на променливите потреби, неопходно е сите прибрани податоци, континуирано и навремено да се обработуваат со цел да се подготви информација која ќе се достави до државните раководни органи, кои врз основа на таа информација ќе најдат начин да се одговори на современите барања на државата за поддршка на нејзината политика и за целосна заштита на нејзините витални национални цели и интереси. Секој елемент на безбедносниот сектор, без разлика од неговата големина, мора да поседува капацитет за да ги разбере детално импликациите кои се однесуваат на прибирањето податоци, нивната анализа и споделувањето на конечната информација. Секоја безбедносна институција мора да има организиран механизам за прием и обработка на податоци, како и механизам за известување и споделување со останатите институции кои го сочинуваат безбедносниот сектор.[37] Секоја од овие институции мора да поседува можност за ефективно искористување на информациите кои се споделени помеѓу различните компоненти на безбедносниот сектор и да даде соодветно толкување на тие информации во рамките на својот домен.

На секоја информација мора да ѝ биде проценета релевантноста и веродостојноста со цел да се одреди колку може да придонесе кон разбирањето и наоѓањето начини за превенирање или сузбивање одредена безбедносна закана. Кога ќе се одреди колку е значајна таа информација, врз основа на нејзината релевантност и материјалност, треба да се направи процена за нејзиниот придонес кон процесот на менаџирање со безбедносната закана. Ова е постојан процес кој бара континуирана активност со цел секоја нова информација која ги исполнува ригорозните стандарди на проверка да се вклопи во целосната слика и треба константно да се применува. Очекувано, ова е еден многу интензивен и побарувачки процес кој има високи очекувања и бара огромно знаење и силни аналитички капацитети пред човечките ресурси кои се вклучени во него.

Брзиот општествен, научен, културен и технички развој доведува до нови побарувања кои ја наметнуваат потребата од што повеќе податоци, кои ќе опфаќаат што поголем дијапазон на области. Фокусот треба да се насочи кон прибирањето податоци кои можат да ни ги откријат плановите, намерите и можностите на потенцијалните нарушувачи на националната безбедноста и кои ќе ја претставуваат

---

[37] Carter, L. David - *„Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies"*, Michigan, 2006, p.1

основата за одлучување и преземање одредени акции[38]. За таа цел, треба да се усовршат начините до доаѓање до нови податоци, оценувањето на нивната вредност (сигурност на изворот од кој се добиени, точност на нивната содржина и нивната важност), колку што е можна побрза анализа на овие податоци, изработка на информацијата и нејзино навремено доставување до крајните корисници.

3.3. Информациски циклус

Термините податок и информација најчесто се поистоветуваат во поглед на своите значења и бидејќи многу ќе се користат во понатамошниот дел од текстот, од круцијално значење е да се направи една исклучително исцрпна дистинкција помеѓу нив во контекст на нивната употреба во безбедносната теорија и практика, и чија цел ќе биде елиминацијата на секаков вид забуна кога се во прашање овие два поими.[39] Овие поими формираат еден вид на континуум, во кој податоците се наоѓаат на почетокот, а информацијата на крајот, и како се поаѓа од почетокот, се додава сè поголема вредност и контекст, коишто го претвораат податокот во информација, која е финалниот продукт кој ќе им се презентира на корисниците. Деловите на една информација прибрани од најразлични извори, како, на пример, следење комуникации,

---

[38] Во нејзиното најшироко значење ја дефинираме како дејност за подготвување и осигурување од изворите на идното загрозување во природата, општеството и помеѓу општествата. Во потесна смисла, безбедносната политика може да ја дефинираме како збир на севкупните мерки, дејности и постапки наменети за дејствување како современ систем на националната безбедност.

Безбедноста која се однесува на општеството/државата во целина претставува национална безбедност во која се инкорпорирани внатрешната и надворешната безбедност. – Котовчевски, Митко – *„Национална безбедност на Република Македонија"*, прв дел, Скопје, 2000, стр.85

[39] Со поимот податок треба да се одбележат оние сознанија или известувања кои се непосредно применети од изворите (човечки или технички), истите не се обработени, туку само регистрирани.
Со поимот информација треба да се одбележат оние сознанија или иззвестувања кои се резултат на соодветна обработка на определни податоци. – Стаменковски, Алекса - *„Основи на разузнавањето"*, Скопје, 1999, стр. 89-90

Поимот податок се однесува на суровите податоци кои се прибрани, но сè уште не се анализирани. Во најголемиот број на оперативни ситуации, од витално значење е да се формира колку што е можно поголема и различна база на податоци заради две причини: прво, голем дел од податоците се со временско ограничување, и нивното значење може да се изгуби доколку не се приберат навреме и во првата прилика која ќе се укаже; и второ, наизглед неповрзаните податоци може да се покаже да имаат критичко значење при изработката на анализата.

Информацијата ќе биде дефинирана како синтеза од податоците и аналитичката обработка. Таа е продукт на внимателната евалуација и анализа на прибраните податоци. Овој продукт потоа се дисеминира преку извештаи или други видови документи со цел да им помогне на крајните корисници за подобро разбирање на оперативната средина и подобра алокација на соодветните ресурси. - Barrett, Michael – *„The Need for Intelligence-Led Policing"*, DomPrep Journal Online Edition, 2006, p.2

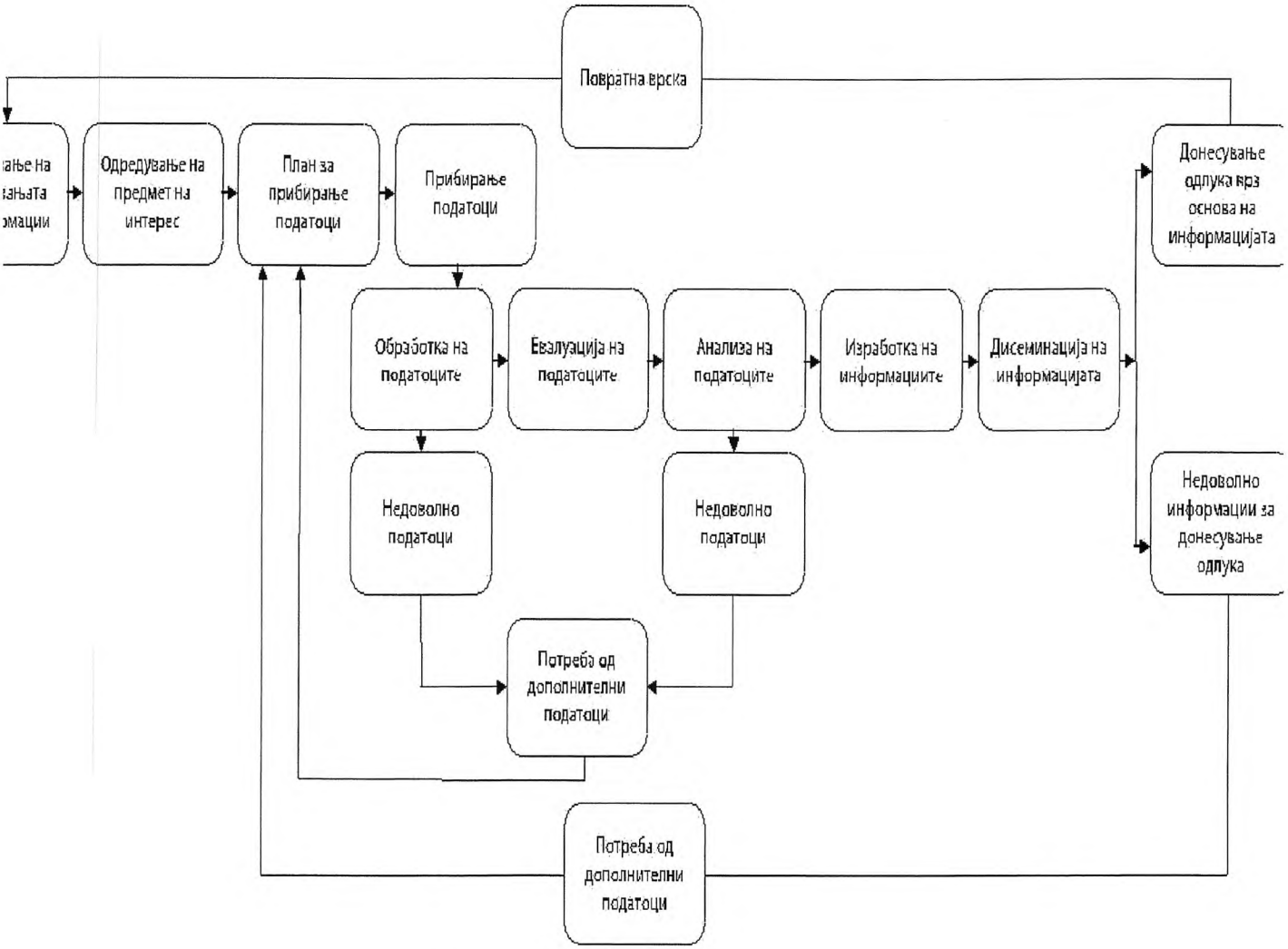
користење соработници, банкарски податоци или прикриено опсервирање, се само сурови податоци кои најчесто имаат ограничено и бесмислено значење. Готовата информација претставува собир на еден широк спектар од податоци кои се внимателно проценети во поглед на нивната веродостојност, детално обработени со цел да се види дали се од важност за конкретниот предмет на интерес и на кои им е дадено значење преку примената на индуктивните и дедуктивните логички процеси.[40]

Информациите се продукт на аналитичките процеси кои им даваат интегрирано значење на најразличните податоци кои имаат најразличен степен на поврзаност и релевантност со безбедносните закани. Во нејзината најчиста форма, информацијата е продукт на аналитичките процеси кои ги проценуваат податоците прибрани од најразлични извори, ги интегрираат податоците во еден кохезивен пакет и даваат заклучок или процена за безбедносната закана преку употребата на научни пристапи за решавање проблеми. Оттука, за информацијата можеме да кажеме дека е синергистички продукт кој е наменет за обезбедување реални и веродостојни насоки за донесувачите на одлуки во случаите на сложени криминогени и безбедносни закани. Начелно, со цел да ја исполни својата функција, одликите на информацијата треба да бидат следниве:

- Превенција. Ги вклучува прибирањето и обработката на податоците кои се однесуваат на безбедносните закани и употребување на таа информација за спречување на сите активности кои можат да ја загрозат националната безбедност.
- Планирање и искористување ресурси. Обработените податоци ги запознаваат донесувачите на одлуки со променливата природа на безбедносните закани, нивните карактеристики и начини на дејствување, и предвидувања за еволуцијата и усовршувањето на овие закани, со цел да се развијат соодветните стратегии за неутрализирање на заканите од овој вид и ефективното искористување на ресурсите со кои располага безбедносниот сектор.[41]

---

[40] Carter, L. David - *„Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies"*, Michigan, 2006, p.7
[41] Ibid, p.8



Дијаграм бр.1 - Информациски циклус

Динамиката на донесување одлуки, во индустријата, економијата, бизнис секторот и секако во државните органи, значително се потпира на навремени и прецизни информации. Со револуцијата на комуникациско-информатичките технологии се чини дека нема недостиг на податоци за која било област. Како резултат на ова, донесувачите на одлуки многу често се наоѓаат пред дилема која информација е важна и може да придонесе во процесот на одлучување. Потребата за внимателно анализирани и веродостојни информации е од неопходно значење бидејќи и политичките и безбедносните одлуки се донесуваат со помош на користењето на овие информации. Токму затоа, мора да се изведе еден беспрекорен процес со цел да се осигура дека важните одлуки се донесуваат прецизно, внимателно и непогрешливо и врз основа на точни, навремени и релевантни информации.

Процесот на прибирање, обработка и дистрибуција на точни, навремени и релевантни податоци кои можат да бидат претворени во информација не се случува сам по себе, туку е точно утврден циклус, кој е развиен на начин да претставува своевиден водич за креирањето релевантни и точни информации од брдото на податоци со кое се соочуваме. За да биде ефикасен, овој циклус мора да биде проактивен, да развива уникатни методи и принципи, и да ги доставува финалните информации навремено и конзистентно до соодветните корисници. Целта на овој процес е да им обезбеди на донесувачите на одлуки готови информации кои ќе им помогнат при донесувањето важни политички, безбедносни, економски и други одлуки. Овие информации може да се разгледуваат и врз основа на нивниот предмет, но и врз основа на нивната намена.

Според предметот може да бидат: биографски, економски, географски, воени, политички, социолошки, научни и технички и да се однесуваат на транспорт и комуникации. Според нивната намена, може да бидат: истражување, извештај, процена, предупредување, анализа.[42]

Всушност, овој процес е мултидимензионален, мултидирекционален, и најважно интерактивен и меѓусебно зависен.[43] Концептуално, овој циклус никогаш не завршува. Низ сиот процес, кој претставува една динамична средина, постојано ќе има побарувања за нови податоци или дадени случувања ќе им дадат нови значења на веќе изготвените информации, што ќе доведе до продолжување на овој циклус. Намената на овој циклус не е да воспостави процедура која мора да се следи, туку само да опише еден процес кој природно се појавува кога ќе се укаже потребата за дополнителна информираност за одреден предмет на интерес за безбедносниот сектор.

Влијанието и ефикасноста на информациите и информирањето во безбедносниот сектор се однесува на процесот на ефективно користење на една информација кој опфаќа неколку зависно поврзани постапки, кои последователно би изгледале вака: планирање и насочување, прибирање на податоците, обработка и

---

[42] Garst, D. Ronald - *"Components of Intelligence"*, A Handbook of Intelligence Analysis, Defense Intelligence College, Washington DC,1989, p 5.

[43] Dearth, H. Douglas - *"National Intelligence: Profession and Process"*, Joint Military Intelligence Training Center, Washington DC, 1995, p.17

анализа на податоците, изработка на информацијата и нејзино доставување (дисеминирање) до крајните корисници.

3.3.1 Планирање и насочување

Првата фаза од овој процес е фазата на планирање и насочување. Оваа фаза ги опфаќа одредувањето на целта или предметот на интерес, одредувањето на податоците кои треба да се прибираат, иницијална идентификација на очекуваните извори на податоци и обликување на операциите и активностите со цел задоволување на тие побарувања. Кои податоци ќе се прибираат може да биде одлука на службата која работи по линија на одреден предмет на интерес или тоа да биде побарано од крајните корисници на информациите со цел да им помогне во донесувањето одлуки.

3.3.1.1 Одредување на потребите на крајните корисници

Побарувањата, или потребите на корисниците, посебно ако се сложени и временски ограничени, бараат интерпретација или анализа од страна на безбедносниот сектор пред да бидат поставени како цели кон кои треба да се стреми процесот на прибирање податоци. Потребно е да се направи дијалог помеѓу службите кои ги изготвуваат информациите и крајните корисници, кој треба да вклучува одреден број прашања и да претставува взаемно дефинирање на предметот на интерес. Петте прашања кои треба да се постават КОЈ, ШТО, КОГА, КАДЕ и ЗОШТО – претставуваат добар почеток за транзиција на потребите на корисниците во побарувања кои се претставуваат за прибирање одредени податоци. Уште едно прашање кое е поврзано со претходните е прашањето КАКО, и ова прашање исто така треба да биде внимателно разгледано. Овие прашања ја формираат основната рамка која треба да ги дефинира побарувањата кои се поставуваат пред службите и стратегијата како да се стигне до посакуваните податоци, сè со цел да бидат задоволени потребите на крајните корисници.[44]

---

[44] Krizan, Lisa - *„Intelligence essentials for everyone"*, Joint Military Intelligence College, Washington DC, 1999, p.13

Прегледот на овие основни сценарија треба да поттикне понатамошен развој на концептот на одредување на потребите на корисниците во специфични ситуации. Одредувањето на предметот од интерес има огромно значење за наредните чекори кои треба да се разгледаат, во прв ред побарувањата за податоци, а секако и процесот на прибирање и анализа. Кога веќе ќе се одреди предметот од интерес и кога се знае кои податоци се потребни, тогаш може многу проактивно и континуирано да се пристапи кон прибирањето на тие податоци. [45]

3.3.1.2. Дефинирање на предметот на интерес

Многу често се случува службите кои ги прибираат податоците и крајните корисници да потрошат драгоцено време и ресурси, бидејќи претходно не успеале да остварат координација и дефинирање на предметот од интерес[46]. Употребата на структуриран приод може да придонесе за избегнување на ваквата неефикасност и да го претставува првиот чекор кон јасното дефинирање на предметот од интерес и можните приоди за успешно справување со него. Овој приод ја зголемува ефикасноста на процесот и обезбедува таргетирање токму на оние податоци кои се потребни да се исполнат поставените побарувања. Овој начин на работа е многу подобар од користењето на еден магнетски начин на работа, при што се прибираат сите можни податоци, а потоа аналитичарите се надеваат дека ќе успеат да подготват значајна информација од брдото добиени податоци. Слободно може да се каже дека начинот на работа при кој се следат претходно поставените побарувања за одреден тип податоци претставува еден научен пристап, со што се постигнува поголема објективност, ефикасност и навременост. Бидејќи ова е научен пристап, може да се направи опис на методолошката рамка која се користи при неговото планирање и спроведување. Тој има прецизно одредени фази, од кои секоја се истакнува со својата уникатност и детаљност, што придонесува за еден квалитативен пристап при планирањето и насочувањето на активностите:

---

[45] Ibid, p.18

[46] Координирањето во сферата на безбедноста и одбраната на секоја земја претставува мошне важна задача на државното раководство и тоа овозможува создавање услови за организирано дејствување во случај на појавување на некоја закана по државата. - Бакрески, Оливер - *„Координација на безбедносната заедница во Република Македонија"*, Скопје, 2005, стр.129

1. Точно утврдување на целите кои треба да се постигнат:
   - Проширување сознанија за одреден предмет на интерес – ова е ситуација кога се имаат одредени сознанија за некои случувања, но заради актуелноста на тој предмет на интерес од безбедносен аспект, потребно е да се ажурираат или да се добијат нови податоци и да се согледаат сите аспекти во однос на тој предмет на интерес.;
   - Превенирање одреден тип на безбедносна закана – во оваа ситуација се имаат индикативни податоци за типот на безбедносната закана, и мерките и активностите се насочуваат конкретно кон таа закана. Се одредуваат изворите на таа закана, се проучуваат поранешни искуства со слични закани, се одредуваат нејзините карактеристики, се разгледуваат начините и појавните облици преку кои би можела да се манифестира таа закана, можните последици од остварувањето на заканата, се прави кадровска поделба на улогите во безбедносните институции, а во оваа фаза е потребно да се направат планови и елаборати во случај да не се успее со превенирањето на заканата.;
   - Справување со безбедносна закана – спроведување во дело и реализација на плановите и активностите кои се однесуваат на конкретната безбедносна закана.
2. Дефинирање на објектот од интерес за безбедносниот сектор:
   - Потенцијални цели на безбедносната закана?
   - Запознавање со карактеристиките и историјата на безбедносната закана.;
   - Како да се обезбеди пристап кон предизвикувачот на безбедносната закана?
   - На кој начин може да се манифестира безбедносната закана, односни со какви методи може да се спроведе?;
   - Извори на финансирање и логистика.;
   - Комуникациски мрежи и технологии кои ги користи.
3. Планирање на процесот на прибирање податоци:
   - Кој тип на податоци ни се потребни?
   - Какви извори на податоци може да се користат?
   - Какви методи да се применат за да се стигне до потребните податоци? и
   - Во која временска рамка треба да се стигне до потребните податоци? [47]

[47] Carter, L. David - *„Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies"*, Michigan, 2006, p.150

Целта на примената на овој пристап е да обезбеди еден сеопфатен и конзистентен модел за планирање и насочување на активностите на безбедносниот сектор. Овој пристап воопшто не е лесен или едноставен, меѓутоа резултатите кои ги дава можат да се покажат како бесценети.

Активностите на институциите на безбедносниот сектор мора да бидат насочени и тоа насочување мора да биде обликувано на начин што ќе ги задоволи потребите на крајните корисниците. Според ова, планирањето и насочувањето е директно поврзано со прибирањето, обработката, анализата и дисеминацијата, како и со развивањето на структурата која ќе ги изврши и ќе ги поддржи планираните или тековните операции. Оваа фаза е круцијална за успешното менаџирање на целиот процес, од идентификувањето на податоците до кои треба да се дојде, па сè до доставувањето на конечниот продукт до корисниците. Таа е почетокот и крајот на циклусот - почеток бидејќи го вклучува формирањето на конкретните побарувања за информации, а крај бидејќи конечната информација, која се користи при донесувањето одлуки, поставува нови потреби за дополнителни информации.

3.3.2 Прибирање на податоците

Прибирањето е втората фаза од информацискиот циклус. За време на оваа фаза, безбедносните служби прибираат податоци кои треба да бидат евидентирани и обработени. Во најголемиот дел од случаите, ова се сурови податоци прибрани од најразлични извори кои на некој начин се поврзани со предметот на интерес. Ефективното прибирање во голема мера зависи од разновидноста на изворите и можноста за меѓусебно потврдување на податоците. Најдоброто сценарио е да се приберат што е можно поголем број податоци и тие меѓусебно да се преклопуваат што ќе придонесе кон зголемување на нивната веродостојност и ќе придонесе за формирање посеопфатна информација. За разлика, многу непожелна ситуација е кога сите податоци се добиени од еден ист извор, и за чија точност не може да се тврди со сигурност.

Фазата на прибирање податоци мора да биде добро фокусирана со цел да се исполнат специфичните побарувања кои се однесуваат на прибраните податоци. Таа се базира на истражување – на поврзување на одредените предмети на интерес со достапните извори на податоци, со краен резултат обработка на тие податоци во

корисни информации. Еден од начините да се избере стратегија за прибирање е најпрво да се подготви листа за тоа какви податоци се очекува да се приберат. Успешната анализа на очекуваните податоци во корелација со потребите на корисниците може да помогне во одлуката какви извори и методи ќе бидат најефикасни за добивање на тие податоци. Преку детална и софистицирана анализа на потребите за податоци, може да се добијат заклучоци кои од податоците се есенцијални за извлекување завршни заклучоци за предметот на интерес, и на нив може да им се даде приоритет при процесот на прибирање. Исто така, може да се проучи и дали безбедносната институција е способна во поглед на вештини, ресурси, време и авторитет да се справи со поставената задача за прибирање на потребните податоци. Уште една работа која треба да се земе предвид е тоа во каков формат ќе бидат прибрани податоците и дали аналитичарите ќе успеат од тие сурови податоци да извлечат корисна информација која ќе може да биде преточена во искористлива форма.

По дефинирањето на изворите на потребните информации и стратегијата која ќе се искористи за тие да се добијат, службата треба да пристапи кон поделба на задачи на персоналот и започнување на активностите.

Извори на податоци

Прибирањето на податоци со цел да се направи конечна информација може да варира од многу едноставно до крајно сложено. Податокот, основниот градбен блок на информацијата, се добива од извори кои генерално се класифицирани во две групи, отворени извори и затворени извори.

Отворени извори се оние што се јавни и што се достапни за сите, а затворени извори се оние кои не се достапни за јавноста. Овој концепт е прилично едноставен. Голем број од изворите од кои може да се прибираат податоци, отворени или затворени, ги има во изобилство, но предизвикот е како да се пронајдат потребните податоци навремено и ефективно. Примери за отворени извори се домашните и странските средства за јавно информирање, печатените и електронските медиуми, интернет порталите, разни списанија, книги и научни истражувања, бази на податоци достапни за јавноста, владини извештаи и документи и сл. Начелно, за отворен извор се смета оној извор преку кој законски и етички може да се дојде до податоци кои се

однесуваат на лица, локации, настани, групи или трендови.[48] Користењето на отворените извори е интегрален дел од процесот на прибирање податоци.

Затворените извори вклучуваат чувствителни или класифицирани документи и предмети, криптирани комуникации, тајни државни програми, заштитени објекти кои имаат важно значење за државата и сл. Врз основа на ова, има широко распространето мислење во јавноста дека податоците добиени од затворени извори се оние вистинските, што во некои случаи е точно, меѓутоа мора да се напомене дека во најголемиот број од случаите податоците се добиваат од отворените извори. Од друга страна, податоците кои не можат да се добијат од отворени извори, како на пример, податоците кои се однесуваат на структурираноста и методите на работа на терористички или криминални групи или пак податоците кои се однесуваат на чувствителни активности поврзани со државни, политички или безбедносни активности се многу значајни за поврзување на комплетната слика за предметот од интерес за службите.

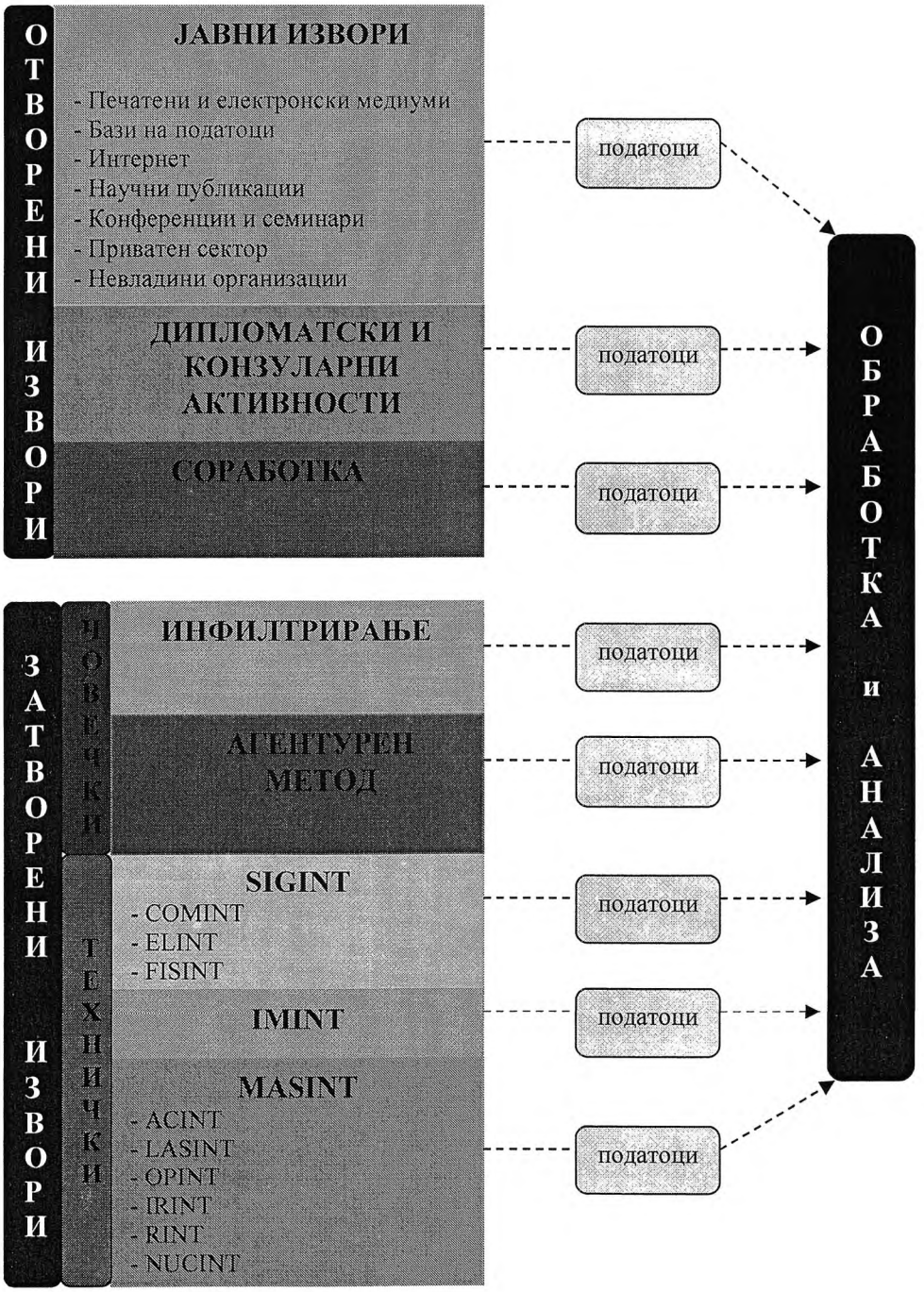
Податоците се сметаат за сурови се додека не се направи процена на изворите, не се направи нивно потврдување преку споредба со други податоци кои се однесуваат на истата проблематика и додека врз нив не се применат аналитичките и другите логички методи кои треба да ја потврдат нивната веродостојност. Недостатокот на ваквата критичка евалуација може само да резултира со некомплетна информација, и да не ги исполни потребите на крајните корисници.

Методи за прибирање податоци

При прибирањето податоци, субјектите кои го вршат тоа прибирање (конституенсите на безбедносниот сектор) имаат на располагање најразлични начини и методи за стигнување до нови податоци. За успешно да се исполни потребата од одреден тип податоци кои се безбедносно интересни, исклучително важно е планирањето на начинот на кој може да се дојде до тие податоци, односно како може тие податоци да се приберат. Податоците се прибираат од најразлични извори, почнувајќи од човечки извори, потоа од најразлични документи и други пишани материјали, како и од разни предмети или технички средства. Во зависност од тоа дали податоците се прибираат од отворени или од затворени извори, се избираат и методите

[48] Ibid, p.70

кои ќе се користат за прибирање на тие податоци. Нормално, методите кои се користат за прибирање податоци од затворени извори имаат поспецифична природа и соодветно на своите карактеристики поставуваат многу поголеми побарувања пред институциите од безбедносниот сектор кои ги користат ваквите методи.



Дијаграм бр.2 - Прибирање податоци

Бидејќи со користењето на методите на прибирање податоци од отворени извори не се прекршуваат некои законски или правни норми, тие може да се применуваат во која било ситуација, па дури и во најсекојдневните ситуации, како, на пример, преку разговор да се добијат некои податоци од безбедносен карактер. Можноста за користење отворени извори на сегашното ниво на меѓународни односи е прилично голема, бидејќи условите и средствата за нивна примена се многу поволни. Заради тоа може да се очекува дека нивното користење ја претставува иднината во константната информираност.

Методите за прибирање податоци од затворени извори, кои ги користат службите кои го сочинуваат безбедносниот сектор имаат свои специфичности и поставуваат поголеми побарувања пред припадниците на безбедносните органи. Тие се одликуваат со својата конспиративност и висок степен на ризичност и во зависност од начинот на кој се прибираат податоците се делат на методи на прибирање податоци со користење човечки извор и методи на прибирање податоци преку користење технички средства.

Прибирање податоци од отворени извори

Можноста за прибирање податоци од отворени извори на сегашното ниво на информираност и меѓународни односи е прилично голема, бидејќи условите и средствата за прибирање податоци се многу поволни. Со зголемувањето на квантитетот и достапноста на податоците од отворени извори, како последица на револуцијата во информатичко-комуникациската технологија, експоненцијално се зголемува и нивното користење од страна на безбедносните институции и веќе станува практика податоците добиени од отворени извори да имаат свое значење при изработката на информациите. Денешните комерцијални и технички напредоци се само последниот чекор во развојот на методот за прибирање податоци од отворени извори кој почна да се развива во доцните 30^ти^ години од минатиот век преку мониторингот на странските радиопрограми и пишаните медиуми пред и по Втората светска војна, до следењето на научните публикации, јавните настапи и сите медиуми за време на периодот на Студената војна, па сè до информатичката револуција во последниве две декади. Револуцијата на информатичката технологија, економијата и политиката во последните две декади ги направи отворените извори подостапни, позначајни и

присутни насекаде. Едноставно кажано, сега може да се соберат многу податоци евтино и брзо.

Прибирањето податоци од отворени извори вклучува:

1. Користење на сите извори на податоци од јавен карактер. Отворените извори од јавен карактер претставуваат едно широко поле, кое опфаќа:
   - печатени и електронски медиуми;
   - бази на податоци достапни за јавноста;
   - отворени дискусии на политички или економски форуми, научни предавања, презентации, конференции;
   - извештаи и документи изработени од државни органи;
   - научни истражувања и заклучоци;
   - податоци од приватниот сектор и невладините организации;
   - интернет страници и онлајн дискусии[49].
2. Прибирање податоци преку официјалните активности на дипломатско-конзуларните претставништва на државата, кои со оглед на поголемиот степен на безбедност, привилегии и имунитет, како и сигурната комуникација со централата во својата матична земја, несомнено даваат најповолни можности за прибирање корисни податоци за државата на прием.
3. Прибирање податоци преку соработка со други држави, односно преку соработка со нивните безбедносни органи, како и преку соработката со меѓународни организации (со потпишување билатерални или мултилатерални протоколи за соработка, каде се утврдуваат областите и прашањата што ќе бидат предмет на соработка и начинот на нејзиното реализирање).

Еволуцијата на отворените извори може да се смета како резултат на неколку фактори. Првиот од овие е проширувањето на безбедносната агенда во текот на последните 20 години. По бројните промени кои се случија на глобално, на регионално и на локално ниво, природата на безбедносните закани и предизвици е изменета во голем степен. Во денешно време, освен класичните безбедносни предизвици, како на пример конфликт меѓу две држави што може да резултира со објавување војна или поттикнување граѓански немири преку учество на странска разузнавачка служба, безбедносниот сектор е соочен со предизвици чиј број е значително зголемен и чија

[49] Carter, L. David - *„Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies"*, Michigan, 2006, p.71

природа е разновидна. Соодветно на ова, проширен е и бројот на предмети на интерес за безбедносниот сектор. Во современиот свет, тероризмот, шверцот на оружје и средства за масовно уништување, организираниот криминал, илегалната имиграција, финансискиот криминал и сл., ги претставуваат безбедносните закани против кои мора континуирано да се дејствува. Проширувањето на безбедносната агенда ги зголемува побарувањата за повеќе податоци, што пак резултира со поголемата употреба и вреднување на отворените извори[50].

Вториот фактор е незапирливиот развој на технологијата. Еволуцијата на интернетот и појавата на мрежните системи ја потврдуваат својата вредност како нови алатки и технологии за проширување на знаењата за еден широк дијапазон на области. Пролиферацијата на интернет страници, портали, блогови и онлајн форуми отвора еден нов свет на податоци што може да се користи од страна на вработените во безбедносниот сектор. Благодарение на информатичката револуција, безбедносниот сектор не е веќе ограничен на традиционалните конспиративни и прикриени методи на работа за доаѓање на податоци од интерес.

Придобивките за безбедносниот сектор од користењето на отворените извори се многубројни. Подолу се наведени неколку од најзначајните, и е направена нивна кратка елаборација.

- **Имаат голема улога во формирањето на основата за одреден предмет на интерес.** Отворените извори обезбедуваат историски податоци, податоци за моменталните политички, економски, социјални, демографски, технички, природни и географски состојби кои се однесуваат на еден предмет на интерес, остваруваат одредено влијание врз тој предмет на интерес, или на некој начин ги насочуваат неговите активности. На тој начин, тие помагаат во формирањето на неопходната основа за природата и карактеристиките на одреден предмет на интерес. Оваа основа е неопходна за да може да се започне обработката на одреден предмет на интерес. Преку користењето на овие податоци многу брзо може да се воспостави што е веќе познато за предметот на интерес и ќе се овозможи насочување на приоритетите кон она што не е познато за тој предмет на интерес. Токму затоа, отворените извори треба да бидат вклучени во целиот

[50] Pallaris, Chris – *„OpenSource Intelligence: A Strategic Enabler of National Security"*, CSS Analyses in Security Policy, Zurich, 2008, p.1

процес на изготвување информација за одреден предмет на интерес, од прибирањето па сè до изготвувањето на конечната информација.[51]

- **Економичност во работата.** Достапноста и бројот на податоците кои можат да се добијат од отворени извори им овозможува на безбедносните институции да ги задоволат своите потреби за податоци без да користат ресурси кои се неопходни при употребата на специјализирани технички методи за прибирање податоци или користењето човечки извори. Отворените извори овозможуваат алокација на ограничените ресурси кон оние предмети на интерес кои е потешко да се пробијат. На пример, во денешниве услови електронски може да се порачаат огромен број публикации, сè поголем број радио и телевизиски станици ја емитуваат својата програма преку интернет, што ја укинува потребата од скапи опреми и антени за да се направат тие програми достапни. Корисни податоци може да се пронајдат на бројните форуми и блогови посветени на меѓународна политика, како и на страниците на водечките дневни весници. Високо квалитетни аерофотографски или сателитски податоци може да се добијат преку користењето на Google Earth или некои други слични провајдери. Исто така, економичноста се огледува во тоа што податоците прибрани на овој начин може да се разменуваат помеѓу безбедносните институции без користењето скапи заштитени информациско-комуникациски системи или ангажирањето на сертифицирани курирски служби.
- **Се зголемува квалитетот на информацијата.** Како дел од еден мултидисциплинарен пристап, користењето на отворените извори во комбинација со другите извори на податоци, дава голем придонес кон изработката на информацијата која треба да се достави до донесувачите на одлуки. Податоците прибрани од отворени извори може да имаат голема корист при валидирањето и разбирањето на податоците прибрани од други извори. Тие може да придонесат за посеопфатна интерпретација и контекстуализација на податоците прибрани преку човечки извори, но и да помогнат во интерпретацијата на технички податоци.
- **Можност за слободно користење.** Податоците добиени од отворени извори може слободно да се користат при истраги или судски процеси, бидејќи нема да предизвикаат откривање идентитети на лица кои соработуваат со службите или

[51] North Atlantic Treaty Organization – *„Open Source Intelligence Handbook"*, 2001, p.36

методологии на работа, што би било случај ако податоците се прибрани на конспиративен начин, и што го олеснува целиот процес, бидејќи нема да има потреба од безбедносни сертификати и други побарувања за сите вклучени во процесот.

- **Етичност во работата.** Друга позитивна карактеристика е што податоците добиени од отворени извори се прибираат преку законски и етички постапки и не предизвикуваат нарушување на општоприфатените норми и правила на однесување.
- **Овозможуваат насочување на активностите.** Мора да се истакне дека преку следењето на отворените извори се доаѓања до сознание за тоа кои податоци за одреден предмет на интерес се достапни за јавноста и не се тајни, што пак овозможува да се процени кои податоци поврзани со тој предмет подлежат на заштита и да се планира како да се насочат активностите на безбедносните институции со цел да се дојде до нив[52].
- **Отсуство на ризик.** Не треба да се занемари и фактот дека процентот на ризик при користењето на отворени извори е скоро непостоечки во однос на конспиративните методи.
- **Постојана достапност на изворите.** Отворените извори се достапни постојано и може да бидат користени за прибирање, процена и обработка на податоците веднаш штом ќе се укаже каква било потреба.

Се смета дека споменатите придобивки и вредноста на отворените извори ќе им овозможи да имаат голема улога во работата на безбедносните институции. Меѓутоа, постојат неколку предизвици кои мора да се надминат.

Прво, мора да се надмине претпоставката дека податоците кои се прибрани од отворени извори немаат големо значење за донесувачите на одлуки, бидејќи тоа се податоци кои можат да се најдат во весниците или на телевизиските канали. Реалноста е дека податоците се прибираат од широк спектар на отворени извори и се многу позначајни и покомплексни отколку што се мисли дека се.

Второ, треба да се земе предвид дека опасноста од измама е секогаш присутна при користењето на овој метод. За разлика од некои други методи на прибирање податоци, овој метод ретко вклучува прибирање податоци преку директна опсервација и интеракција со предметот на интерес, туку се потпира на секундарни извори кои

[52] Ibid, p.2

пренесуваат податоци кои се однесуваат на предметот на интерес. Овие секундарни извори, како на пример печатените и електронските медиуми, можат намерно или ненамерно да додадат, да избришат, да модификуваат или на друг начин да ги филтрираат податоците пред да ги направат достапни за јавноста. Затоа е од големо значење да се познава историјата на тие извори и нивната наклонетост со цел да може да се направи разлика меѓу објективните, фактички податоци и оние што содржат предрасуди, субјективни ставови или се намерно формулирани со цел да го измамат лицето што ги следи. [53]

Трето, мора да се посвети внимание на предизвикот кој произлегува од недостатокот на јазичните капацитети на припадниците на безбедносните институции кои непосредно го употребуваат овој метод. Ваквата ситуација се појавува како резултат на индиферентноста која ја има безбедносниот сектор кон странските јазици и култури. Познавањето на странски јазици е еден од клучните предуслови за ефективно користење на отворените извори.

Четврто, за користење на отворените извори неопходно е и дополнително вложување во информатичка опрема. Безбедносните институции мора да работат во насока на организација на своите технички ресурси за да може да се справат со големиот обем на податоци кои се прибираат од отворени извори и се однесуваат на одреден предмет на интерес. Треба да се користат технички решенија кои ќе овозможат подобри пребарувачи, пребарување по клучни зборови, напредни софтвери за преведување, подобри програми за инкорпорирање на аудио и видео сегменти во информациите кои се изготвуваат и сл.

Петто, реално очекување е дека опсегот на податоци кои се добиваат од отворени извори може да доведе до презаситување на аналитичките капацитети на безбедносната институција, независно од нејзината големина. Токму затоа, мора да се воспостави ефективен менаџмент кој ќе успее да го избегне ваквото презаситување.[54]

Безбедносниот сектор мора да работи во насока на развивање на своите капацитети за користење на отворени извори. Слично како и за другите методи на прибирање податоци, потребно е да се вложи многу работа и ресурси за да се формира една компетентна структура за прибирање податоци од отворени извори, бидејќи тие

---

[53] Headquarters Department of the Army – *„FMI 2-22.9 - Open Source Intelligence"*, Washington DC, 2006, p.p.2-10

[54] North Atlantic Treaty Organization – *„Open Source Intelligence Handbook"*, 2001, p.18

претставуваат значаен ресурс кој мора да биде инкорпориран во работата на безбедносниот сектор. Фактот е дека иднината на методот за прибирање податоци од отворени извори е многу светла и има многу простор за негово унапредување и признавање. Подобрата соработка и вклучувањето на отворените извори во целокупниот процес на прибирање податоци ќе придонесе за формирање информации кои ќе бидат од големо значење за донесувачите на одлуки. Овој метод секогаш ќе има големо значење и за него секогаш ќе има место во работата на безбедносниот сектор.

Прибирање податоци од затворени извори

- Прибирање податоци со користење човечки извори

а) Метод на инфилтрирање во структурата на предметот на интерес

Овој метод претставува организирано и планско тајно вградување на оперативен работник, кој е професионален припадник на некоја од институциите кои го сочинуваат безбедносниот сектор, во организациската структура на предметот на интерес, со користење адекватна легенда, а со цел да прибира и доставува податоци[55].

Инфилтрирањето оперативец во предметот на интерес е еден од најделикатните методи за прибирање податоци. Прво, треба да се земе предвид дека со самото донесување на одлуката за инфилтрација, се признава дека сите други достапни методи за прибирање податоци се или исцрпени или неприменливи. Ова е воедно и еден од најризичните методи, бидејќи инфилтрацијата треба да се спроведе во објект чија основна карактеристика е тајноста и недовербата кон надворешни лица, како, на пример, противничка разузнавачка служба, терористичка група, организирана криминална група или насилна група. Токму затоа, потребен е многу внимателен избор на оперативец кој ќе биде инфилтриран, и кој треба да биде соодветно обучен, добро психофизички подготвен, да има исцрпно познавање на предметот на интерес и да има подготвено одлична и веродостојна легенда. Таа мора да биде внимателно осмислена и без празнини. Датумот на раѓање, местото на раѓање, образовните институции и

[55] Баткоски, Томе – *„Разузнавачка и безбедносно-контраразузнавачка тактика",Скопје, 2008,* стр.30

поранешните работни места кои ги вклучува легендата мора добро да бидат разработени и проучени. Оперативецот мора детално да ја познава и безгрешно да ја извршува професијата или занаетот според кој се легендира. Покрај основната легенда, треба да постои и алтернативна легенда, која се користи во итни случаи кога основната легенда е разоткриена.

Уште еден важен сегмент при примената на овој метод е комуникацијата и остварувањето контакт на инфилтрираниот припадник со матичната институција, со цел пренесување на прибраните податоци и добивање нови задачи. Остварувањето контакт е неопходен елемент при употребата на овој метод, во кој на посреден или на непосреден начин се предаваат документи и другите материјали и се пренесуваат известувања за текот на добиената или извршената задача. Најважно е овие контакти да останат незабележани од припадниците на предметот на интерес и да се одржуваат само во случај кога се неопходни, но и да бидат навремени со цел навремено примање на податоците.

б) Агентурен метод

Агентурниот метод на работа е класичен метод за прибирање и пристап до податоците кои се однесуваат на предметот на интерес[56]. Преку агентурниот продор се прибираат податоци за глобалните трендови кои можат да имаат импликации врз националната безбедност, како и податоци кои на творците на националната политика ќе им користат за подготвување навремени и темелни политички одлуки.

Широко распространет став во безбедносната практика е дека најважните податоци може да бидат добиени преку човечки извор, односно преку оној човек што е во непосреден контакт со потребните податоци или со предметот на интерес и дека агентурниот метод на работа дава најдобри и најсигурни резултати[57]. Неговото

---

[56] Според Љубомир Стајић „Агентурниот метод е илегален начин за прибирање информации и подразбира користење на тајни соработници на разузнавачката служба за запознавање со состојбата, можностите и намерите на противникот.“ – Стајић, Љубомир – *„Основи безбедности“*, Београд, 2004, стр.220

[57] Агентурниот метод го добива својот назив од поимот „агент”. Самиот збор агент доаѓа од латинскиот збор „agens” што значи „лице кое извршува некаква дејност”. Во согласност со тоа, агент е лице со строго одредени мотиви кое со умисла, тајно, организирано, непрофесионално и релативно долго време прибира податоци и извршува други активности за потребата на некоја разузнавачка служба – Милошевиќ, Милан – *„Систем државне безбедности“*,Београд, 2001, стр.106
Според Методија Дојчиновски и Фердинанд Оџаков „Агент претставува лице кое е регрутирано, обучувано, контролирано и ангажирано да собира информации и да пријавува и известува за

огромно значење се гледа во тоа што со негова помош може да се оствари оперативен (агентурен) продор во центрите на државно-политичко, воено, безбедносно, економско, научно и техничко-технолошко одлучување, каде се чуваат податоци и документи со највисок степен на класификација. Исто така, со овој метод може да се направи и продор во терористички и криминални групи, кој би бил од исклучително големо значење заради затворената природа на ваквите групи, и на тој начин да се дојде до витални податоци за нивната структура, начини на дејствување, идни планови, нивната логистика и сл.[58]

Агентурниот однос е секогаш двонасочен, бидејќи подразбира однос оперативец (професионален припадник на безбедносна институција) - агент. Оперативецот е субјект кој раководи со агентот, а агентот е тој што собира податоци или извршува други задачи по налог на оперативецот. Оперативецот е професионален припадник на безбедносна институција, односно тоа му е постојана работа за која прима плата и има професионална подготовка и тој е главниот носител на активностите врзани за прибирање податоци. За да ја процени ситуацијата правилно и да ја изврши задачата успешно, оперативецот треба да поседува високи морални и професионални квалитети, да е искусен доволно за да ја процени секоја постапка, да се справи со сите неповолности кои ќе се појават и да знае да најде излез од секоја компликувана ситуација. Доколку и покрај сето ова, како резултат на некои непредвидливи околности, неговата работа е откриена и штетата е неизбежна, тој треба да знае да го минимизира степенот на таа штета. Успешноста на работата на професионалниот припадник несомнено во најголема мера зависи од неговите лични и професионални квалитети. Оперативците кои работат со агенти треба да поседуваат: висок степен на оперативна подготвеност, индивидуални квалитети, висок степен на образование, познавање на агентурниот метод на работа, познавање на агентот со кој се работи, способност да се забележи присуство на контраразузнавачки и безбедносни органи и способност за промислено реагирање во опасни ситуации. Тие мора да бидат подготвени и способни успешно да се справат со променливите приоритети, односно

информации" – Дојчиновски, Методија и Оцаков, Фердинанд – *„Разузнавачки операции"*, Скопје, 2010, стр.243

[58] Во поново време, агентурниот метод се поврзува со многу институции кои се дел од безбедносниот сектор, како на пример Одделот за организиран криминал при Министерството за внатрешни работи, Дирекцијата за спречување на перење пари и финансирање тероризам, Царинската управа и Финансиската полиција. – Саздовска, Марина Малиш – *„Прирачник за разузнавачки циклус", Скопје, 2005,* стр.14

да бидат приспособливи, флексибилни и сензитивни во текот на својата работа.[59] Преку нивното искуство оперативците треба да постигнуваат константни подобрувања во природата и квалитетот на операциите кои ги спроведуваат, менаџирањето со човечките ресурси (агентите) и користењето на посебните технички средства. Исто така, потребно е да поседуваат знаења од областа на криминалистиката, криминологијата, социологијата, психологијата, историјата и сл.[60]

Агентурниот метод се состои од три фази, од кои секоја со своите специфичности и карактеристики претставува посебна целина и чие успешно совладување резултира со реализацијата на поставената задача.

Почетната фаза е процесот на врбување на агентот. Оваа фаза вклучува комплетирање на специфични и меѓусебно поврзани постапки, со цел да се придобие одреден граѓанин да стапи во соработнички однос со безбедносните органи.[61]

Процесот на врбување на агентот ги подразбира следниве постапки:

- Истражување и детално запознавање на предметот кој е од интерес за безбедносните органи - предметот на интерес мора квалитетно и сеопфатно да се анализира и да се одлучи дали интересот на безбедносната институција во однос на тој предмет налага неопходност од примена на агентурен метод. Мора детално да се согледаат сите можности, врз основа на кои потенцијалниот агент оптимално и ефикасно би можел да ги добие податоците кои се од интерес. Паралелно со ова, мора да се утврди дали постојат и какви се условите за примена на агентурниот метод.;
- Одредување лице што може да биде потенцијален агент и детално запознавање на неговата личност и карактеристики - кандидатите за врбување мора да се наоѓаат во позиција да обезбедат податоци со соодветна важност и мора да имаат можност да ги пренесат тие податоци.;
- Одредување мотив врз основа на кој ќе се врбува кандидатот за агент - следен чекор што го презема службата е одредување на мотивите според кои ќе се врбува кандидатот и запознавање со слабостите на кандидатот кои ќе се

---

[60] Ibid, стр.48

[61] При изборот на кандидатите треба да се обрне големо внимание, а тоа значи дека треба да се избираат стабилни и ладнокрвни луѓе, кои не се стремат кон популарност и кои не им кажуваат на сите за својата врска со странската разузнавачка служба. Освен тоа, неопходно е тие луѓе да се оптимисти, да се дисциплинирани и одговорни, да имаат способност за чување на тајни (да се конспиративни), и да имаат способност за брзо и лесно приспособување во нови средини со цел да стекнат доверба. – Цуклески, Гоце - *„Прирачник за соработничка мрежа", Скопје, 2005,* стр.31.

употребат како мотив за неговото врбување. Бидејќи однесувањето на секој човек е водено од различни мотиви, повеќе од неопходно е нивно прецизно определување. Токму затоа, за најдобро да се согледаат мотивите врз основа на кои би се врбувал кандидатот за агент, треба да се разгледа еден исклучително корисен концепт. Концептот „ПИКЕ", односно **П**ари – **И**деологија – **К**омпромитирање - **Е**го (во превод од англискиот акроним MICE - **M**oney, **I**deology, **C**ompromise (или **C**oercion), **E**go (или **E**xcitement) потекнува од американското контраразузнавање, и е воведен со цел да се објаснат мотивите на потенцијалните агенти. Едноставноста на овој концепт се согледува во тоа што тој ги вклучува сите мотиви кои предизвикуваат една личност да ја предаде својата група, организација или држава и да почне да работи за туѓи интереси.;

- Изнесување на предлогот за врбување на кандидатот за агент - има два главни методи на врбување, имено директен пристап и постепен пристап. Директниот пристап ја претставува највисоката класа на работа со агенти. Безбедносната институција му дозволува на својот припадник да изведе таква операција само доколку тој изнесе задоволителни аргументи за преземањето на еден таков ризик. Директниот пристап има голем број предности. Контактот со потенцијалниот агент се случува само еднаш, наместо да има многу состаноци за неколку месеци, како што е случај со постепениот пристап. По првиот контакт, свежо врбуваниот агент сам ќе се грижи за својата безбедност и за одржување на тајноста на агентурниот однос. Постепениот метод, и покрај своите недостатоци е најчесто употребуван. Во најголемиот број случаи, не може без директни контакти со кандидатот да се дознаат сите податоци кои се потребни за да се донесе одлуката за негово врбување. За таа цел, се организираат ситуации во кои оперативецот и кандидатот „случајно" ќе остварат контакт и ќе почнат да комуницираат. Откако познанството помеѓу нив веќе преминало во пријателство и откако се направени неколку меѓусебни услуги за одредени потреби, тогаш веќе темите на разговор може да почнат да се движат кон предметите на интерес за безбедносната институција. Во голем број случаеви, формален предлог за врбување воопшто не се ни прави, бидејќи кандидатот несвесно веќе работи за безбедносната институција. Откако самиот ќе стане свесен за ова, дури тогаш оперативецот му објаснува дека тоа е всушност и суштината на нивното пријателство, и тогаш сè влегува во нова фаза.

По успешното врбување на агентот, следи втората фаза, односно процесот на работење со агентот. Под процес на агентурна работа се подразбираат вкупните активности на агентот од моментот на воспоставување на агентурниот однос до неговото завршување. Процесот на работа со агентот подразбира три основни делови:

- Запознавање на агентот со основите на агентурната работа и негово обучување - обуката на агентот е многу важна, бидејќи преку неа агентот се запознава со основите на агентурната дејност, со методите и начините на работа. Исто така се укажува и на потребата од чување во тајност на агентурниот однос. Обуката на агентот се фокусира на негово детално запознавање со задачите што треба да ги реализира, како треба да се заштити од разоткривање, да му се објаснат тактичките постапки за извршување на агентурната работа, како и запознавање со оперативната техника која ќе ја користи (камери, микрофони, тајни мастила и сл.) и начинот на кој ќе се одржува врска со оперативецот.;
- Остварување на контакт со агентот - остварувањето на контакт помеѓу оперативецот и агентот е неопходен елемент во агентурниот однос, во кој на посреден или на непосреден начин, се поставуваат задачи за агентот, се предаваат документи и другите материјали (финансиски средства, технички средства) и се пренесуваат известувања за текот на добиената или извршената задача. Под непосреден контакт со агентот се подразбира остварување директна средба помеѓу него и оперативецот[62]. Посредните контакти на оперативецот со агентот подразбираат реализирање контакт помеѓу нив преку посредник. Тој посредник може да биде некое лице или пак да се искористат одредени средства кои се погодни за таква намена („мртва јавка"[63], телефонска и електронска комуникација, сигнални средства и сл.).;
- Реализирање на добиените задачи - ова е еден циклус што постојано, со обновена и збогатена содржина, се продолжува во рамките на генералната цел што е поставена во однос на даден предмет на интерес. Со цел да се обезбеди

---

[62] Нацев, Александар – *„Непосреден контакт со агентот"*, Годишник на Факултетот за безбедност, Скопје, 2010, стр. 140

[63] „Мртвите јавки" се најчесто користените елементи на непосреден контакт. Тие имаат најуниверзална употреба бидејќи во нив може да се стават сите оние работи што се потребни за работата на агентот: документи, пари, радиоуреди, специјална опрема за фотографирање и друго. Тие претставуваат однапред договорено место помеѓу разузнавачот и агентот и се користат за разменување материјали помеѓу нив. Познати се илјадници видови „мртви јавки", од надгробни споменици до специјално дизајнирани магнетни кутии во најразлични форми.

успешна работа на агентот, оперативецот мора добро да го насочи агентот кон предметот на интерес, редовно да одржува контакти со него, да му дава инструкции и да му врши дообука кога за тоа ќе се појави потреба.

Последната фаза на агентурниот метод е прекинот на соработката со агентот. Ова е исклучително сложено и чувствително прашање. Најдобар случај е кога соработката ќе заврши по реализирањето на сите задачи кои биле цел на агентурниот однос, односно агентот успешно ја завршил својата работа. Најважна работа при прекинувањето на контактите со агентот е да се одбегнат или да се елиминираат негативните појави поради кои се прекинува врската. Досието на агентот во безбедносната институција треба комисиски да биде уништено, за што треба да биде изготвен и соодветен службен документ. Притоа, одредени особено значајни податоци и пошироки сознанија од досието, што би биле потребни за натамошната работа на службата се издвојуваат и засебно се архивираат.

На крај, со посебно внимание треба да се разгледа и постапката кога доаѓа граѓанин (домашен или странски) и самоиницијативно изјавува дека сака да работи за некоја од институциите на безбедносниот сектор. Колку и да изгледа чудно ова, сепак ова е многу чест случај што треба да биде подложен на детална анализа. Овие личности се нарекуваат доброволни кандидати за агенти, и се една од најнепредвидливите форми на агентурен однос[64].

Прибирање податоци со користење технички средства

Методот на прибирање податоци со користење технички средства подразбира користење различни технички направи со чија помош може да се дојде до посакуваните податоци. Постои широк дијапазон на технички направи кои може да се користат при примената на овој метод. Тоа може да бидат различни модели на направи за аудио и видео снимање, разни видови камери и фотоапарати, направи за привлекување и снимање електромагнетни зрачења, разни видови на радари и радарски

[64] Во англоамериканската терминологија се употребува терминот „walk-in", а во советската терминологија терминот „dobrozhelatel".

Еклатантен пример за ваков случајот е кога еден човек од Мајами донел во разузнавачката служба на САД една кутија која ја купил на аукција на пратки запленети од царинската управа на САД. Бидејќи тој ја отворил кутијата дури кога стигнал дома, се запрепастил кога видел дека во неа има преку 2 000 негативи на кубанска антиамериканска пропаганда.

апарати, направи за аерофото и сателитско снимање, компјутерски програми за пробивање на заштита на компјутерски системи и сл. Во денешниве услови на унапредување на техниката и информациско-комуникациското поле, експоненцијално се зголемуваат и можностите за користење технички средства за прибирање податоци.

Постојат две варијанти на собирање податоци со примена на технички средства[65].

Првата варијанта е прибирање податоци преку користење технички средства кои се тајно поставени во непосредна близина или внатре во предметот на интерес од страна на професионални припадници или агенти на безбедносната институција. Тајното поставување и користење на техничките средства претставува специфична операција со висок степен на ризик, бидејќи средствата треба да се наоѓаат во одредена просторија, дел од просторот или во одредено превозно средство што го користат припадниците на предметот од интерес, а притоа да не бидат лесно воочливи или откриени од нивна страна. Исто така, уште еден од условите што мора да се исполни за да биде успешен овој метод е техничкиот квалитет на податоците кои ќе се прибераат со помош на техничките направи. За негова ефективна примена, потребно е најпрво многу внимателен избор на техничките направи кои ќе се користат, како и детално планирање на постапките преку кои ќе се изврши нивно поставување или вградување во објектите кои се од интерес за безбедносниот сектор, а секако и за начинот на кој ќе се изврши трансмисијата на потребните податоци од техничките направи до службата.

Втората варијанта е употребата на технички средства кои директно или индиректно се насочени кон предметот на интерес, но не се во непосреден контакт со него. Пример за ова се различните системи за извидување радиосообраќај, за пресретнување електронски пораки од секаков вид, телеметриско прибирање податоци, користење радари и радарски системи, системи за аерофото и сателитско снимање и сл. Во зависност од видот и начинот на кој се користат техничките средства, во безбедносната литература и практика се издиференцирани неколку различни дисциплини кои се занимаваат со прибирање на податоци. Со цел подобро разбирање на секоја од овие дисциплини, подолу е направен еден обид за нивна класификација и објаснување.

---

[65] Буцаковски, Стефан – *„Разузнавање - контраразузнавање, деловно бизнис разузнавање, безбедносни системи“* , Охрид, 2005, стр.205

Дисциплини за техничко прибирање податоци

Постојат три основни дисциплини кои се прифатени во безбедносната практика, како од самите институции кои ги применуваат, така и од академските кругови кои се занимаваат со проучувањето на безбедносните, разузнавачките и контраразузнавачките појави: SIGINT (Signals Intelligence), IMINT (Imagery Intelligence) и MASINT (Measurement and Signature Intelligence)[66].

1. **SIGINT** (Signals Intelligence) е дисциплина која се користи за прибирање податоци преку пресретнувањето и декодирањето на комуникациски, електронски и телеметриски емисии[67]. Ваквото пресретнување може да се реализира преку користењето бродови, авиони, сателити или копнени станици. Трите категории на SIGINT се[68]:
   - COMINT (Communications Intelligence) - е прибирање на податоци преку мониторирање (следење) на комуникација и пораки од различен вид. Овие податоци може да бидат во форма на гласовни трансмисии, Морзеова азбука, факсови и сл. Во современата безбедносна практика, најголемиот дел на комуникациите се криптирани и за нивно декриптирање се потребни софистицирани компјутерски технологии.;

---

[66] Освен овие три, како резултат на постојаното усовршување на техничко-технолошките и информациско-комуникациските полиња, некои автори предлагаат и проширување на бројот на дисциплини. Поради сè поголемиот развој и поширокатa употреба на информатичката технологија, потребно е да се прифати уште една дисциплина, наречена ITINT (Information Technology Intelligence) која ќе се занимава со прибирање податоци преку информацискатa технологија, а како нејзина категорија треба да се прифати HACKINT (Hackers Intelligence) која служи за прибирање податоци преку неовластени пробивања во заштитени компјутерски системи. – Баткоски, Томе – *„Разузнавачка и безбедносно-контраразузнавачка тактика",Скопје, 2008,* стр.129

Уште една дисциплина која е потребно да се спомене, и која веќе е прифатена како засебна од страна на Централната разузнавачка агенција на САД (ЦИА), е дисциплината GEOINT (Geospatial Intelligence) со која се добиваат податоци преку користењето слики кои ја претставуваат површината на Земјата, а се однесуваат на безбедносни појави од големи размери (појава на природни катастрофи, детонација на нуклеарно оружје и сл.) – Central Intelligence Agency – *„The Work of a Nation"* - https://www.cia.gov/library/publications/additional-publications/the-work-of-a-nation/work-of-the-cia.html [05.12.2013]

[67] Margolis, Gabriel – *„ The Lack of HUMINT: A Recurring Intelligence Problem"*, Global Security Studies, Volume 4, Wilmington NC, 2013, p.46

[68] Central Intelligence Agency – *„The Work of a Nation"* - https://www.cia.gov/library/publications/additional-publications/the-work-of-a-nation/work-of-the-cia.html [05.12.2013]

- ELINT (Electronic Intelligence) - податоци кои се добиваат преку пресретнувањето на електромагнетни сигнали (кои не претставуваат вид на комуникација), како, на пример, радарска емисија на сигнали или современи системи за управување со ракетни системи. Ова овозможува идентификување на локацијата на емитерот и одредување на неговите карактеристики. Постојат две поткатегории на ELINT, и тоа RADINT (Radar Intelligence) која се користи за прибирање податоци кои се емитираат од радари или радарски системи и TELINT (Telemetry Intelligence) - прибирање податоци преку мерење од далечна локација и трансмисија на мерките кон опремата што треба да ги прими, како на пример прибирањето податоци за движењето на наведуваните ракетни системи.;
- FISINT (Foreign Instrumentation Signals Intelligence) – податоци кои се прибираат при тестирањето и изведувањето современи странски воздушни, копнени или подземни оперативни системи, преку следење сигнали или на видео линкови. Пример за ова е пресретнување сигнали при тестирањето на некое ново оружје или нов вид летало, со што би можело да се одредат неговите карактеристики, како, на пример, потрошувачка на гориво, краен домет и сл.

2. **IMINT** (Imagery Intelligence) е дисциплина што се користи за прибирање податоци преку користење фотографии, инфрацрвени сензори и сл. IMINT се реализира со помош на специјализирани авиони, беспилотни летала и сателити кои имаат можност да произведат квалитетни слики[69].
3. **MASINT** (Measurement and Signature Intelligence) е дисциплина што се користи за прибирање податоци преку употреба на специјализирани сензори, кои може да се употребуваат во секоја околина, а чија цел е да ги забележат метричките параметри и специфичните карактеристики на предметот на интерес, кој може да биде специјална опрема (нов тип на летало, прототип на ракетен систем), нов тип на оружје и сл. Категории на MASINT се следниве[70]:

---

[69] Оваа дисциплина, која во минатото беше позната како PHOTINT (Photo Intelligence), била употребувана уште многу одамна, дури за време на Граѓанската војна во САД, кога војници биле сместувани во балони со цел да извидуваат од височина и да ги забележат позициите на непријателот. – Federal Bureau of Investigations – „Intelligence Collection Disciplines" - http://www.fbi.gov/about-us/intelligence/disciplines [04.12.2013]

[70] Lerner, K. Lee and Lerner, Wilmoth Brenda – *„Encyclopedia of Espionage, Intelligence and Security Vol.2"*, Farmington Hills MI, 2004, p.253

- ACINT (Acoustic Intelligence) – прибирање податоци од звучни бранови. Најчесто се користи за одредување на положбата на воени бродови или подморници преку користењето подводни сонари (**SO**und **NA**vigation and **R**anging).;
- LASINT (Laser Intelligence) – прибирање податоци со помош на ласерски зраци. Ласерот (**L**ightwave **A**mplification by **S**timulated **E**mission of **R**adiation) претставува екстремно тесен, моќен и насочен зрак на светлина. Во контекст на LASINT, со користење на ласер кој е насочен кон затворена просторија, тој може да се искористи да ги забележи вибрациите кои се произведуваат од звучните бранови.;
- OPINT (Optical Intelligence) – ги вклучува сите податоци кои се дел од крајниот спектар на оптичкиот видеокруг, односно оние што не се видливи со голо око.;
- IRINT (Infrared Intelligence) – прибирање податоци преку технички средства кои детектираат инфрацрвени зраци, односно кои го користат инфрацрвеното поле како медиум за трансмисија на пораки.;
- RINT (Unintentional Radiation Intelligence) - вклучува следење на гама зраци (кои се емитираат на пример од радиоактивниот материјал кој се користи во софистицираните нуклеарни направи), кои го претставуваат највисокото енергетско ниво од електромагнетниот спектар.;
- NUCINT (Nuclear Intelligence) – прибирање податоци преку следење на степенот на радијација кој доаѓа од радиоактивните извори (нуклеарни централи, складишта на нуклеарно оружје и сл.).[71]

3.4.3 Обработка и анализа на податоците

По успешното прибирање на податоците, потребно е да се почне со нивна обработка и анализа, а потоа и последната фаза од информациониот циклус, изработка на информацијата и нејзино доставување до крајните корисници.

---

[71] Chia Eng Seng, Aaron – „MASINT – The intelligence of the future“, DSTA Horizons 2007, Singapore

Обработка на прибраните податоци

Без разлика на изворите на податоци и методите за прибирање податоци кои се употребени, прибраните податоци мора внимателно да бидат обработени пред да се искористат за изработката на конечната информација. Методите кои ќе се употребат за обработката на податоците може да варираат во зависност од карактеристиките на податоците, но нивна заедничка цел е да ги подготват тие податоци во форма која ќе може да биде употреблива за аналитичарите. Во состав на оваа фаза се прави конверзија на суровите податоци во форма која ќе биде соодветна за понатамошна обработка, која, на пример, може да вклучува развивање и интерпретација на сателитски податоци, обработка на снимките добиени со употребата на висококофистицирани технички средства, преведување текстови и прилози добиени од странски медиуми, декриптирање на криптирани пораки, транскрипт од аудиоснимка и сл. Бидејќи некои од прибраните податоци се добиваат во искористлива форма, треба да се напомене и дека овој процес не се применува на сите прибрани податоци, туку само на оние за коишто има потреба.

Овој процес вклучува употреба на различни постапки што треба да се преземат пред да се почне со анализа на податоците и врши нивно подредување. Некои од тие постапки се следниве:

- проценување на релевантноста на податокот во однос на предметот на интерес;
- оценување на веродостојноста на изворот и на податокот;
- подредување на податоците според нивната содржина во однос на предметот на интерес;
- одредување на меѓусебните врски на податоците;
- споредување на податоците кои се однесуваат на ист аспект од предметот на интерес, а се добиени од различни извори;
- проценување на употребливоста на податоците во изработката на конечната информација;
- одредување на потребата за дополнителни податоци за предметот на интерес[72].

[72] Mathams, R.H. - "The Intelligence Analyst's Notebook," in *Strategic Intelligence: Theory and Application*, eds. Douglas H. Dearth and R. Thomas Goodden, 2d ed. (Washington, DC: Joint Military Intelligence Training Center, 1995), p.85-86.

Евалуација на веродостојноста на прибраните податоци

На прибраните податоци мора да им се направи евалуација со цел да се одреди нивната релевантност, веродостојноста на изворот и точноста на информацијата. Ваквата евалуација вклучува низа различни постапки за валидирање на нивната вредност. Мора да се одреди дали податоците се релевантни во однос на предметот на интерес, дали има потреба од такви податоци и дали имаат одредена вредност во моментот.

Изворите на податоци и начините на прибирање на податоци исто така се оценуваат за веродостојност. Податоците се оценуваат и во поглед на нивната точност со цел да се утврди дали настаните или случувањата на кои се однесуваат податоците навистина се случиле, и дали тие може да се потврдат со податоци добиени од други извори. Без разлика на изворот од кој се добиени, точноста на податоците мора да биде проверена. Детаљното проучување на изворот на податокот и применливоста на податокот имаат значајна улога во тоа дали тој податок ќе продолжи да се користи понатаму, односно во изработката на конечната информација. При евалуацијата на податоците, тие се разгледуваат од два различни агли. Првиот агол е веродостојноста на изворот преку кој е добиена информацијата, а вториот агол е точноста на податокот.

Во однос на првиот случај, логично е дека со најголема внимателност ќе се пристапува кон податоците добиени од извори со кои нема претходно позитивно искуство и на нив треба да им се пристапи најкритички. Доколку податоците се добиени од претходно проверен извор, на нив треба да им се пристапи со повеќе доверба, но сепак и тие треба да бидат проверени и споредени со податоците кои се однесуваат на истиот предмет на интерес, но кои се добиени од друг извор.

Од друга страна пак, при проценувањето на точноста на податоците, се зема предвид веројатноста, која означува дали еден податок е одреден, неодреден или пак невозможен. Ова може да се покаже преку следниве две матрици, кои всушност претставуваат шеми, шаблони со кои на табеларен начин се прикажува одреден сооднос, односно корелација помеѓу точно утврдени параметри .[73]

[73] Field Manual (FM) 2.22-3 Appendix B, Source and Information Reliability Matrix

ик	Оцена	Објаснување
	Веродостојно	Не постои сомнеж за автентичноста, вистинитоста или компетентноста, и во сите поранешни случаи податоците биле веродостојни
	Вообичаено веродостоен	Постои минимален сомнеж за автентичноста, вистинитоста или компетентноста, но во најголемиот број поранешни случаи податоците биле веродостојни
	Прилично веродостоен	Постои сомнеж за автентичноста, вистинитоста или компетентноста, но има доставено веродостојни податоци во минатото
	Непостојано веродостоен	Постои значаен сомнеж за автентичноста, вистинитоста или компетентноста, но има доставено веродостојни податоци во минатото
	Неверодостојно	Недостаток на автентичност, вистинитост и компетентност
	Не може да се процени	Нема основа за заклучување[74]

Дијаграм бр.3 - Оцени за веродостојноста на изворот на податокот

При разгледувањето на содржината на податокот, односно точноста на податокот, треба да се земе предвид веројатноста, која означува дали еден податок е одреден, неодреден или пак невозможен. Еден податок се смета за вреден само кога е употреблив, а неговата употребливост зависи од целовитоста, прецизноста и навременоста. Секогаш треба да ја имаме предвид и можната измама која лежи во навидум веродостојните податоци.

[74] Field Manual (FM) 2.22-3 Appendix B, Source and Information Reliability Matrix

к	Оцена	Објаснување
	Потврдено	Потврдено од други независни извори, логично само по себе, конзистентно со други податоци за тој предмет
	Веројатно е вистинито	Непотврдено, но логично само по себе, конзистентно со други податоци за тој предмет
	Може да биде вистинито	Непотврдено, возможно, се согласува со други податоци за тој предмет
	Сомнително	Непотврдено, возможно, но нелогично, нема други податоци за тој предмет
	Невозможно	Непотврдено, нелогично, контрадикторно со другите податоци за тој предмет
	Не може да се процени	Нема основа за заклучување[75]

Дијаграм бр.4 - Оцени за точноста на податоците

За илустрација на претходно наведеното може да послужат следниве хипотетички ситуации. Оцена „А“ означува несомнено доверлив извор, како на пример професионален припадник на сопствената безбедносна институција. Овој извор е комплетно веродостоен, но доколку тој пресретне порака која претставува дезинформација и која има за цел лажно известување, пораката ќе има оцена „5”, односно дека таа е невозможна. Во еден ваков случај, пресретнатата порака ќе се означи како „А-5”. Исто така, може да се сретнеме и со случаи каде и покрај тоа што изворот е веродостоен, неговата оцена ќе се намали доколку тој известува за појава која е од техничка природа и не ја познава доволно за да даде исцрпно известување. Во друг случај може да се користиме со услугите на агент кој е патолошки лажго, но сепак дава доволно податоци за да продолжиме со негово користење. Неговата оцена за

[75] Field Manual (FM) 2.22-3 Appendix B, Source and Information Reliability Matrix

веродостојност ќе биде „Д", но доколку податокот е темелно проверен и потврден, ќе биде означен како „Д-1".

Објективното и совесно приоѓање при оценувањето на податоците е неопходно, бидејќи секоја лоша процена во оваа фаза ќе има негативни импликации врз точната интерпретација на конечната информација.[76] По успешната верификација на податоците, потоа следува нивно подредување и поврзување со претходно добиените податоци кои се однесуваат на конкретен предмет. Ова не значи дека новодобиените податоци ќе претставуваат хронолошко поврзување на еден предмет кој се обработува. Може да има случај кога ќе се добијат податоци кои се однесуваат на ситуација што се случила многу порано, а кои му недостасувале на аналитичарот во неговото следење на конкретниот предмет. Ваквите податоци кои објаснуваат нешто што се случило пред определено време може да фрлат ново светло врз некои настани кои аналитичарот не можел да ги објасни или да ги поврзе, и да му ја формираат комплетната слика за предметот на интерес.

Анализа на прибраните податоци

По подредувањето и верификацијата на податоците, следи нивно анализирање. Анализата на податоците е процесот кој е најважен за изготвување на конечната информација, бидејќи преку овој процес се врши конверзија на суровите податоци во информација[77]. Таа треба да даде комплетен опис за предметот кој се истражува, притоа земајќи ги предвид сите релевантни варијабли и преку интерпретација на значењето и ефектите на неговите засебни елементи. Преку успешното реализирање на овие постапки, треба да се стигне до примената на синтеза и ефективно познавање на предметот на интерес, што пак треба да резултира со негова соодветна процена. На крај треба да се развијат логични хипотези кои се однесуваат на предметот на интерес, и секоја од нив треба да биде тестирана, со цел да се откријат индикациите кои би

---

[76] Баткоски, Томе – *„Разузнавачка и безбедносно-контраразузнавачка тактика", Скопје, 2008,* стр.129

[77] Анализата не е само реорганизација на податоците во нов формат. Анализата е процес преку кој податоците се трансформираат во информација. Ова се прави преку расчленување на еден проблем на неколку составни делови и вклучува детално испитување на тие делови и на нивната меѓузависност. – Krizan, Lisa - *„Intelligence essentials for everyone"*, Joint Military Intelligence College, Washington DC, 1999, p.29
Анализата е процес на селектирање, интегрирање и интерпретирање на податоци кои се однесуваат на даден предмет на интерес - McDowell, Don - *„Stretegic Intelligence & Analysis – Guidelines on Methodology & Application"*, The Intelligence Study Centre, 1997, p.17

настанале доколку таа хипотеза се покаже како валидна. Ова е процес кој не ветува непогрешливост, меѓутоа врши пополнување на голем број на празнини во знаењето за одреден предмет на интерес и ја намалува несигурноста при донесувањето одлуки поврзани со тој предмет. Целта на анализата е да им помогне на крајните корисници во проширувањето на нивните знаења за одреден предмет на интерес и неговите карактеристики.

Најчесто, со анализата се разработува можноста за остварување одредено сценарио. Ваквата постапка не треба да се смета како предвидување на иднината, бидејќи таква ситуација е практично невозможна. Правилниот начин да се карактеризира анализата е како еден тип на прогноза, поткрепена со експлицитни факти и веројатни претпоставки, која ќе ги претставува оформените ставови и убедувања на аналитичарот кој ја изработил. Некои од карактеристиките на овој процес се:

- аналитичкиот процес мора да вклучува детално познавање на предметот на интерес кој се истражува и да придонесе кон негово детално запознавање и разбирање;
- аналитичкиот процес мора да ги познава потребите на крајните корисници;
- аналитичкиот процес мора да биде активен учесник во развивањето на интегрираната стратегија за одредување на потребите за податоци и прибирањето на податоците, со цел да може да даде добра анализа;
- аналитичкиот процес не смее да се задоволи само со податоците кои ги добива, туку треба да постави свои побарувања за податоци кои му се потребни во неговата работа.

Успешната анализа има огромна вредност – за самата информација, за институцијата која ја подготвила таа анализа, за целокупниот безбедносен сектор и за крајните корисници на информацијата – во поглед на репутацијата и сè поголемите побарувања кои се поставуваат пред изготвувачите на анализите[78]. Успешни анализи се оние кои даваат реални предвидувања или ставови за предметот на интерес и коишто се изработени со ригорозна примена на научните методи кои се користат за стигнување до одредени заклучоци и кои се употребуваат при истражувањето на општествените, а во таа рамка, и на безбедносните појави. Имено, станува збор за:

[78] *„Bringing Intelligence About: Practitioners Reflect on Best Practitioners„* – Center for Strategic Intelligence Research, Joint Military Intelligence College, 2003. p.102

- Аналитичко-синтетскиот метод;
- Методот на анализа на содржина;
- Методот на набљудување;
- Компаративниот метод;
- Историскиот метод;
- Дедуктивниот и индуктивниот метод;
- Статистичкиот метод;
- Методот на докажување и негирање;
- Методот на примероци;
- Студијата на случај;
- Методот на апстрахирање;
- Методот на генерализација;
- Методот на логичко поврзување на фактите[79].

Клучна во оваа фаза е улогата на аналитичарот. Аналитичарите треба да бидат професионалци кои се одлично обучени за да ја проценат точноста, веродостојноста и релевантноста на податоците. Успешните аналитичари мора да имаат детални и сеопфатни познавања за полето кое го работат и да бидат во можност да ги искористат податоците добиени од најразлични извори, како отворени, така и затворени. Тие вршат интеграција на податоците, ги стават податоците во одреден контекст и формираат еден продукт кој вклучува процени и прогнози за одредени настани и ситуации. Како придружен ефект на нивната работа, тие ја одредуваат и потребата за нови, дополнителни податоци кои треба да се приберат за предметот на интерес, со цел да се зголеми прецизноста и сеопфатноста на информацијата која ја подготвуваат. Со цел да се обезбеди што поголема ефикасност на аналитичарите и поголем квалитет на самата анализа, неопходно е да се исполнат следниве услови кои имаат директно влијание врз конечниот резултат:

- **Силни аналитички капацитети** – овој прв услов ја акцентира потребата од компетентни аналитичари, кои всушност се главните актери во оваа фаза на обработка на информациите[80]. Аналитичарите треба да поседуваат висок степен на аналитичка подготвеност, индивидуални квалитети, висок степен на образование и широки

[79] Баткоски, Томе – *„Разузнавачка и безбедносно-контраразузнавачка тактика", Скопје, 2008,* стр.133

[80] Саздовска, Марина Малиш - *„Прирачник за разузнавачки циклус", Скопје, 2005,* стр.25

познавања од различни области. Сите предности кои ги пружаат важните податоци може да се искористат само од аналитичар кој одлично ја познава својата работа.;

- **Постојан прилив на податоци** – за да може да биде успешна една анализа, на аналитичарите им е потребен постојан прилив на податоци, по можност од различни извори. Доколку аналитичарот има постојан прилив на нови податоци, тој многу полесно може да ја комплетира целосната слика за конкретниот предмет на интерес и многу попрецизно да ја направи својата анализа. Уште една предност од постојаниот прилив на податоци е тоа што многу лесно ќе можат да се елиминираат погрешните податоци и намерно пласираните лажни податоци.;

- **Систематизација во работата** – работата на еден аналитичар ќе биде многу поуспешна доколку тој се фокусира само на одреден вид предмети на интерес. Одредувањето на работата врз основа на линиски или територијален пристап, во голема мера ќе ја олесни работата на аналитичарот, и ќе му овозможи да се фокусира единствено на своето поле на работа, со што ќе стекне поголеми знаења токму за тоа поле и ќе изготвува попрецизни анализи.;

- **Постојана обука и дообука на аналитичарите** – современиот начин на живот и постојаниот напредок на технологијата ја условува потребата од постојана обука на аналитичарите на различни полиња кои имаат допирни точки со нивната работа.

Ефективната анализа подразбира комбинирање на експертиза за одреден предмет со иновативен пристап и интуиција кон неговото разбирање, и има огромно значење за успешната примена на информацијата.

3.4.4 Изработка на информацијата и нејзино доставување до крајните корисници

Сите претходно опишани процеси се неопходни прекурсори на изработката на информацијата, и токму со овој процес се постигнува функционалноста на целиот циклус. Променливата природа на очекувањата на донесувањето одлуки има големо влијание за изработката на информацијата. За да ја исполни својата цел, конечната информација мора да биде подготвена во формат што ќе придонесе за нејзина максимална употреба. За да се исполни овој формат, информацијата треба да ги поседува следниве карактеристиките:

- Јасно да идентификува кој е нејзиниот краен корисник.;
- Да го елаборира предметот на интерес и прецизно да е насочена кон него.;
- Да ги содржи токму оние елементи што се од интерес за корисникот, и да биде ослободена од сите непотребни делови, а ако се укаже потреба, јасно да се нагласат или да се обележат најважните делови. Исто така, пожелно е во текот на нејзината изработка, аналитичарот да може да ги предвиди потенцијалните прашања и нејаснотии кои би ги имал крајниот корисник, и да се посвети поголемо внимание токму на тие делови.;
- Да дава корисни и прецизни прогнози и препораки кои се во согласност со извршената анализа и да се избегнат сите можности за контрадикторни ставови и тврдења.;
- Логичка презентација на ставовите преку јасна транзиција помеѓу речениците и параграфите, без да се додаваат непотребни информации кои ќе претставуваат дистракција.;
- Да е претставена во конзистентна, јасна и естетска форма и да се внимава на граматичките и синтактичките елементи.;
- Доколку се покаже како потребно, да се нагласи кои анализи се направени врз основа на податоци добиени од отворени извори. Во исклучителни случаи, може да се укаже потреба да се наведат и методите и изворите за прибирање податоци. До кој степен на транспарентност ќе се оди овде, сепак треба да биде внимателно промислено. Исто така, во информацијата може да биде вклучен коментар на аналитичарот и на оној кои ги прибрал податоците за веродостојноста и кредибилитетот на изворот.;
- Доколку има случај различни параграфи да бидат со различна класификација, потребно е јасно и читливо да се обележи секој параграф посебно. Информацијата да се изработи на начин што ќе овозможи разделување на класифицираните од некласифицираните делови, доколку има случај таа информација да се дисеминира на повеќе лица што имаат безбедносни сертификати со различен степен.;
- Да ги идентификува временските граници за кои е употреблива.;
- Доколку е тоа случајот, да се наведе врската со друга информација која се однесува на истиот предмет на интерес.

Еден од моментите на кој треба да се посвети особено внимание при изработката на информацијата е одлучувањето дали ќе се класифицира таа информација, и доколку се одлучи потврдно по ова прашање, кој степен на класификација да се употреби. Класификацијата на информацијата е многу важен елемент затоа што има големо влијание врз нејзината понатамошна циркулација. Меѓутоа, донесувањето на одлуката дали одредена информација ќе се класифицира и со кој степен, не е воопшто едноставна работа, бидејќи мора да се земат предвид многу фактори.

Дисеминацијата како важен предуслов за ефективно искористување на информацијата

За да може една информација да го достигне својот полн капацитет, неопходно е да се изврши нејзина ефективна дисеминација. Дисеминацијата претставува одлучување за тоа кому ќе му се достави одредена информација. Класификацијата на една информација и нејзината евалуација всушност претставуваат механизми за да се олесни процесот на дисеминација. Без соодветна дисеминација, голем дел од вредноста на информацијата се губи.

Потребно е да се направи прецизна процена за тоа кому ќе му биде доставена одредена информација, а од неопходно значење за ваквата процена е да се знае кои потенцијални корисници на таа информација ги исполнуваат принципите „потребно е да знае“ и „има право да знае“. Овие принципи се користат за да се осигура дека одредена информација ќе стигне кај оние лица што имаат вистинска потреба и овластувања да ја добијат таа информација, и да донесуваат одлуки врз основа на неа. Според принципот „има право да знае“ корисникот има службено овластување и соодветен безбедносен сертификат за да ја добие информацијата. Принципот „потребно е да знае“ значи дека корисникот има потреба од таа информација со цел извршување на своите редовни работни обврски.[81]

---

[81] *„Criminal Intelligence File Guidelines”* – Law Enforcement Intelligence Unit, http://www.leiuhomepage.org [03.12.2013]
Потребно е да знае е принцип според кој се утврдува корисникот кој има потреба за пристап до класифицирани информации заради извршување на функцијата или службените задачи - *„Закон за класифицирани информации“*, Службен весник на Република Македонија бр.9/04 од 27.02.2004 година.

Интегритетот на информацијата може да се одржи само преку строго придржување кон насоките за дисеминација. Пред да се достави одредена информација со крајните корисници, потребно е да се забележи на кое лице му се доставува таа информација, дали тоа лице ги исполнува горенаведените принципи и име на институцијата за која работи.

Потребата за остварување повратна врска помеѓу крајните корисници и изготвувачите на информацијата

Крајните корисници се зависни од службите кои им доставуваат информации во една филтрирана форма и кои ги содржат само оние елементи што им се од интерес. Информацијата претставува продукт на успешната анализа, што треба да ги задоволи потребите и очекувањата на корисниците. Таа е корисна само доколку успеала да им даде на крајните корисници (донесувачите на одлуки) одредена асистенција при преземањето на одредени активности. Таа го прави тоа преку проширувањето на знаењата на крајните корисници за одреден предмет на интерес, понудата на прогнози и процени за одреден предмет, различни решенија за одредена ситуација, како и можните импликации кои ќе настанат доколку се направи одредена одлука за дејство.

Донесувачите на одлуки во полињата на државната политика и безбедносната политика мора да ги знаат приоритетите кои бараат континуирано унапредување, и токму затоа е потребен регуларен и константен дијалог со безбедносниот сектор [82]. Тие мора активно да се вклучат во процесот и да имаат реални очекувања за тоа колку една информација може да придонесе во нивната работа. Многу е важно да се избалансира односот помеѓу изготвувачите на информацијата и крајниот корисник. И двете страни мора да ги разберат комплексните параметри на оваа врска, да го пронајдат вистинскиот начин за изградба на конструктивна соработка и да имаат заемна почит и разбирање за соодветните обврски.[83]

---

[82] Lahneman, J. William - *„The Future of Intelligence Analysis"*, Center for International and Security Studies at Maryland, Maryland, 2006, p.62

[83] Ford, A. Christopher - *„Relations between Intelligence Analysts and Policymakers: Lessons of Iraq"*, Hudson Institute, Washington, 2005, p.5

Фазата на доставување на информацијата на крајните корисници треба да биде проследена со дијалог помеѓу изготвувачот на информацијата и крајниот корисник. Изготвувачите на информацијата имаат потреба од добивање повратна врска од крајните корисници, со цел да дознаат дали информацијата им била од корист и дали се задоволни од начинот на кој е презентирана таа информација[84]. Ова се прави за да можат изготвувачите да ја унапредат својата работа во иднина и да подготвуваат информации кои во целост ќе ги задоволат потребите на крајните корисници. Повратната врска помеѓу корисникот и изготвувачот треба да даде одговор на прашањата за употребливоста, релевантноста и навременоста на доставената информација. Добрата комуникација во поглед на овие прашања ќе придонесе кон порефинирани информации, нивна поголема употреба од страна на корисниците и унапредување и зајакнување на повратната врска.

Според донесувачите на одлуки, информацијата им е корисна за време на три фази во кои е активен предметот на интерес:

- на самиот почеток кога одреден предмет станува предмет на интерес, но многу е веројатно дека во оваа фаза ќе има многу малку информации за тој предмет;
- во самиот момент кога треба да се донесе одлука за одреден предмет на интерес; во оваа фаза, донесувачите на одлуки бараат од информацијата да им понуди повеќе алтернативи, меѓутоа информацијата нуди само опис на предметот и прогнози и претпоставки во врска со него;
- кога донесувачите на одлуки веќе се одлучиле како да постапат и нивната одлука се совпаѓа со добиената информација. Доколку информацијата не се совпаѓа со нивната одлука, тие најчесто покажуваат сомнеж во нејзината веродостојност[85].

Корисниците сакаат добиените информации да им бидат од помош при донесувањето важни оперативни или стратегиски одлуки. Тие може да имаат ограничено познавање за процесите преку кои тие информации стигнале кај нив во готова форма, и да имаат свои сомнежи во вредноста на тие информации. Многу често,

---

[84] Krizan, Lisa - *„Intelligence essentials for everyone"*, Joint Military Intelligence College, Washington DC, 1999, p.46

[85] Treverton, Gregory – *„Reshaping National Intelligence for an Age of Information"*, Cambridge, Cambridge University Press, 2001, p.185

корисниците ги гледаат информациите како само мала помош при донесувањето на своите одлуки, и повеќе доверба имаат во некои попознати и потрадиционални влијанија. Меѓутоа, треба да се напомене дека информацијата мора да остане независна и објективна, и како таква, најчесто не е непогрешлив факт, туку е претпоставка, прогноза, но не и совет што мора да се прифати. Таа не му кажува на корисникот каква одлука да донесе, туку само ги идентификува факторите кои се во игра, и објаснува како различните акции може да влијаат врз исходот.

Глава 4

Споделување информации

4.1. Општо за процесот за споделување информации

Пролиферацијата на потенцијалните закани и информатичката револуција имаа влијание врз очекувањата на донесувачите на одлуки во поглед на информациите кои ги добиваат од безбедносниот сектор. Донесувачите на одлуки не само што бараат нови информации за нови предмети на интерес, за чие добивање треба да се користат нови извори, туку сè почесто користат и отворени извори, кои претставуваат одредена конкуренција за информациите добиени од безбедносниот сектор. Како резултат на ова, безбедносниот сектор се соочува со уште еден предизвик, а тоа е губењето на својот примат во снабдувањето на донесувачите на одлуки со потребните информации. За да ја задржи својата ефективност, безбедносниот сектор мора да се натпреварува во оваа многу компетитивна средина и да ги искористи сите свои ресурси за да го задржи својот епитет на незаменливост кога е во прашање доставувањето информации на донесувачите на одлуки. Од многу голема помош во остварувањето на оваа цел може да биде споделувањето информации помеѓу институциите кои го сочинуваат безбедносниот сектор [86].

Безбедносните закани со кои е соочено едно современо општество се од различна природа, а безбедносниот сектор се справува со нив преку нивно проучување, анализирање и нивно разбирање. Активностите на безбедносниот сектор во прв ред мора да бидат насочени кон антиципација и превенција на овие безбедносни закани, а не кон реакција откако тие го манифестирале своето антиопштествено дејство. Ова значи дека институциите кои го сочинуваат безбедносниот сектор мора да поседуваат колку што е можно поголем број информации за овие закани, со цел успешно да се справат со нив.

Споделувањето информации од доменот на безбедноста го претставува трансферот на релевантни и веродостојни факти или сознанија, кои се однесуваат на актуелни и идни безбедносни инциденти или закани, како и на активности кои може да се сметаат како прекурзори на ваквите негативни појави. [87]

---

[86] Lahneman J. William - *„The Future of Intelligence Analysis"*, Center for International and Security Studies at Maryland, Maryland, 2006, p.4

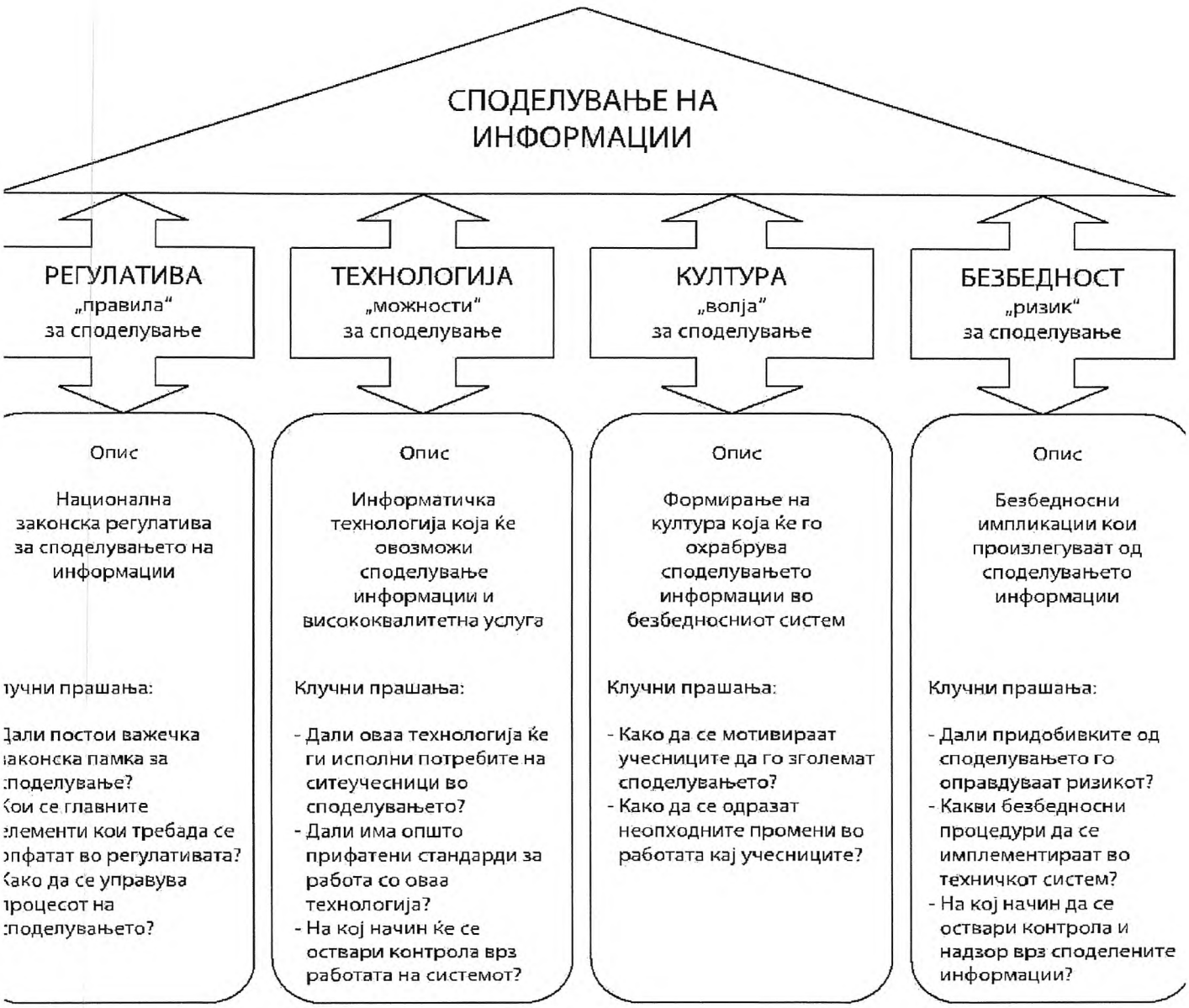
[87] Treglia, Joseph – *„Three Essays on Law Enforcement and Emergency Response Information Sharing and Collaboration: An Insider Perspective"*, Dissertation, Syracuse University Surface, NY, 2013, p.127

Споделувањето информации и координацијата помеѓу институциите е од големо значење за формирањето сеопфатни и практични пристапи и решенија за справување со безбедносни закани, и е од голема помош за вработените во безбедносните институции при проучувањето на овие закани, како и развивањето на соодветни технички и организациони решенија за нивна превенција и справување со нив. На пример, поседувањето информации за одредена закана или настан со кој веќе била соочена друга институција од безбедносниот сектор овозможува да се идентификуваат нејзините појавни облици, да се разбере ризикот што го претставува таа закана и да се одредат превентивните мерки што ќе се применат. Исто така, сеопфатната и навремена информација за одредена безбедносна закана може да помогне при разбирањето на таа закана, навременото предупредување и изборот на постапки со кои ќе се спречи нејзината манифестација. Споделувањето информации кои се однесуваат на терористички и криминални групи, може да го спречи нивното влегување во границите на нашата земја, како и нивното слободно движење и дејствување на наша територија.[88]

Споделувањето информации се базира врз неколку столбови кои ја формираат неговата архитектура. Секој од овие столбови е неопходен за беспрекорно функционирање на процесот на споделување информации и има интерактивен однос со другите столбови.

Потребно е да се утврдат и да се постигнат соодветни очекувања и активности во поглед на споделувањето на информации кои ќе го опфатат дејствувањето на безбедносниот сектор како целина и делокругот на работа на секоја од неговите посебни институции. Преку успешното спроведување на овие активности ќе се осигура сеопфатно планирање и примена на механизми кои ќе резултираат со успешност на безбедносниот сектор во остварувањето на своите функции.

[88] Dacey F. Robert and Hite C. Randolph - *„Homeland Security:Information Sharing Responsibilities, Challenges, and Key Management Issues"*, Testimony Before the Committee on Government Reform, House of Representatives, Washington, 2003, p. 10



Дијаграм бр.5 – Споделување информации

4.2. Придобивки од споделувањето

Споделените информации може да имаат одлучувачко влијание врз перспективите на донесувачите на одлуки во поглед на проблемите со кои се соочуваат и одлуките кои ги донесуваат. Можеби најголемата придобивка од споделувањето за оној што ги прима информациите е здобивањето со ново знаење кое е од големо

значење за него, а тоа знаење не можело да се добие на друг начин по прифатлива цена. Споделените информации може да се покажат како многу вредни доколку се однесуваат на важни безбедносни или надворешно-политички теми[89]. Примачот има интерес за добивање точни информации кои ќе се покажат како комплементарни со оние што веќе се во негов посед, односно оние кои се резултат на неговите напори.

Придобивките кои ги нуди споделувањето се очигледни:

- обезбедува зголемен и забрзан пристап и добивање нови информации, како и идентификување нови извори на податоци, кои може да придонесат кон успешно справување со безбедносни закани и предизвици;
- придонесува кон посеопфатното разбирање и искористување на една информација;
- ги пополнува празнините во знаење за одредени безбедносни закани и ги идентификува новите закани пред кои е исправен безбедносниот сектор;
- претставува предуслов за навремено и успешно одлучување за одредени постапки;
- носи предности и во спречувањето на дуплирање на активностите на различните институции, како и за економичност на ресурсите;
- придонесува за заемно насочување на активностите на различните институции;
- помага во справувањето со транснационални безбедносни закани.

Робусната и цврста соработка помеѓу безбедносните институции на полето на споделување и координираната интеракција помеѓу нив која ги зголемува знаењата за предметите на интерес ќе ја осигураат успешноста во работата на безбедносниот сектор.

4.3. Препреки за споделувањето информации

И покрај напорите да се воспостави успешно споделување информации, се чини дека овие напори се соочуваат со тешкотии, бидејќи недостасува една јасна

[89] Walsh Igoe, James – *„Defection and Hierarchy in International Intelligence Sharing"*, Cambridge University Press, UK, 2007, p.157

идентификација на препреките кои се исправени пред споделувањето. Идентификација на тие препреки и нивното проучување и разбирање е првиот чекор што ќе придонесе кон формирањето стратегија и преземањето постапки за нивното надминување. Овие препреки имаат влијание врз споделувањето и индивидуално и колективно, и секоја категорија има посебни карактеристики, меѓутоа сите четири категории се меѓусебно зависни и заеднички влијаат врз споделувањето. Постапките во насока на унапредување на споделувањето треба да се концентрираат врз овие категории на препреки и да понудат применливи решенија кои ќе ја опфатат секоја перспектива.

1. Препреки кои произлегуваат од учесниците во процесот на споделување информации:
   - недостатокот на доверба помеѓу учесниците во споделувањето;
   - организациона култура и различните работни практики на институциите.
2. Препреки кои произлегуваат од карактеристиките на информациите кои се споделуваат
   - критичноста на информацијата;
   - квалитетот на информацијата;
   - степенот на класификација на информацијата.
3. Препреки од техничка природа:
   - интероперабилноста на системите;
   - функционирање на системот;
   - безбедносни мерки и контрола на системот.
4. Препреки кои произлегуваат од недостатокот на утврдени законски регулативи и процедури за споделување:
   - непостоењето на законска регулатива за споделување информации;
   - отсуството на централизирано тело што ќе го управува споделувањето.

4.3.1. Препреки кои произлегуваат од учесниците во процесот на споделување информации

Недостатокот на доверба помеѓу учесниците во споделувањето

Довербата е многу значаен фактор за споделувањето, бидејќи институциите кои треба да ги споделат информациите може да имаат одбивност кон споделувањето,

бидејќи немаат доверба во оние на кои им ги доставуваат дека успешно ќе ги заштитат информациите и нема да ги злоупотребат.

Може да се издвојат три типови на доверба во контекст на споделувањето информации:

- Доверба која се базира на пресметка. За довербата која се базира на пресметка, основно е донесувањето одлука дали со споделувањето на одредена информација која ќе придонесе во работата на примачот, испраќачот ќе оствари некаква потенцијална придобивка (на пример, можноста да се оствари реципроцитет во споделувањето).;
- Доверба која се базира на идентитетот на лицата со кои се врши споделувањето. Довербата која се базира на идентитет се формира преку личното познанство со лицата со кои се споделуваат информациите.;
- Доверба која се базира на репутацијата на институцијата. Довербата која се базира на институцијата е онаа доверба кога испраќачот има почит за репутацијата на примачот и знае дека споделените информации ќе бидат правилно искористени и нема да бидат злоупотребени [90].

Може да се забележи дека сите типови на доверба се субјективни и зависат од индивидуалните перцепции и впечатоци.

На институционално ниво, различните институции може да немаат доверба во другите институции кои се дел од безбедносниот сектор, и да имаат одредени задршки при споделувањето информации. Тие може да одлучат да не споделуваат информации воопшто или да споделуваат само некорисни информации, бидејќи немаат доверба во другите институции кои се дел од безбедносниот сектор. Оваа недоверба може да се должи на меѓусебниот натпревар за репутација или за одобрување поголем буџет и други ресурси, и има големо значење за нивната мотивација за споделување, бидејќи тие ги гледаат своите сопствени интереси. Недовербата на институционално ниво потекнува од следниве две ситуации.

Првата ситуација е кога постои ризик дека споделените информации ќе се споделат понатаму со трета страна, бидејќи институциите немаат контрола што се случува понатаму со информациите кои ги споделиле, и токму ова може да се покаже како извор на недоверба. Ова се должи и на различните стандарди кои ги имаат

---

[90] Treglia, Joseph – *„Three Essays on Law Enforcement and Emergency Response Information Sharing and Collaboration: An Insider Perspective"*, Dissertation, Syracuse University Surface, NY, 2013, p.39

различните институции за одржување на безбедноста на информациите. Имено, секоја од институциите треба да има утврдено директиви и упатства за административна, физичка, персонална и информатичка безбедност на информациите со кои ракува.

Втората ситуација е кога постои ризик дека нема да се заштитат информациите од неовластен пристап и неовластено објавување. Довербата на персонално и институционално ниво е идентификувана како еден од најважните фактори за успешно споделување. Со цел зголемување на довербата, потребно е да се размислува во насока на формирање на еден модел кој ќе го опфати балансот помеѓу ризикот од споделувањето и довербата. Преку овој модел ќе се одреди дали за испраќачот е прифатлив ризикот и ранливостите кои ќе произлезат од евентуалната злоупотреба на информацијата во однос на придобивките од споделувањето.

Организационата култура и различните работни практики на институциите

Организационата култура, исто така, има големо влијание врз споделувањето. Таа има големо влијание за ограничување или охрабрување на споделувањето одредени информации. Воспоставувањето соработка и протоколи за споделување информации помеѓу институциите на безбедносниот сектор може да се покаже како тешка задача. Ако во одредена институција има клима на недоверба или анимозитет (кои се резултат на најразлични причини, како, на пример, традиционална компетитивност и нетрпеливост, лоши односи на раководителите на институциите, лоша соработка и негативни искуства и сл.) кон институцијата со која треба да се споделат одредени информации, најверојатно е дека споделувањето нема да биде охрабрувано или ќе биде сведено на минимум. Ова се неколку од препреките кои се јавуваат како резултат на различните работни практики на институциите:

- **Затворената организациона култура на институциите** - постигнувањето успешна соработка на полето на споделување информации не е едноставна задача, бидејќи се конфронтира со затворената организациона култура на некои од институциите на безбедносниот сектор, кои цврсто инсистираат на својата независност. Проблемот е што институциите, според нивните овластувања и дизајн, не се структурирани за соработка. Овде треба да се напомене и дека безбедносните институции го користат своето право за заштита на информациите кои ги поседуваат од неовластен пристап, и се однесуваат кон тие информации како да се нивна сопственост. Ова право го остваруваат преку класификација на информациите,

побарување за поседување безбедносен сертификат доколку некој сака да ја добие таа информација и воспоставување на принципот „потребно е да знае“. Предизвикот е како да се поттикнат различните институции и кај нив да се создаде една волја за споделување информации, во целината која е составена од посебни институции кои се одлучни да ја задржат својата изолираност, како мерка за одржување на својата моќ и контрола. Се чини дека само силната и континуирана посветеност на раководителите на различните институции кон споделувањето на информации ќе придонесе многу за надминувањето на оваа препрека и ќе поттикне поефективно споделување на информации кои се однесуваат на националната безбедност.;

- **Борбата за зголемување на репутацијата** - во поглед на меѓуинституционалната соработка во безбедносниот сектор, ривалството помеѓу институциите, односно желбата секоја институција да се докаже повеќе со цел да ја зголеми својата репутација и да ја акцентира својата незаменливост, да се здобие со престиж и (можеби најважната причина) да добие што повисоки буџетски примања од државата, претставува сериозна препрека за споделувањето информации.;

- **Асиметричните приоритети на безбедносните институции** - ова всушност значи дека службите кои треба да споделуваат информации имаат различни приоритети, на кои им посветуваат поголемо внимание и за кои трошат повеќе ресурси. На пример, најголем предизвик за едната служба може да биде справувањето со тероризам, а за другата служба тоа да биде организираниот криминал во неговите најразлични форми. Ваквата асиметрија најчесто предизвикува важни информации да останат несподелени бидејќи службата која ги поседува не им дава големо значење, бидејќи не се однесуваат на нејзините приоритет, додека тие информации би биле од круцијално значење за другата институција. Различните приоритети или интереси на безбедносните институции варираат значајно според полето на работа на одредена институција. Оваа ситуација може да се покаже како препрека доколку секоја од институциите тежнее да го задржи своето ексклузивно право за пристап до одредена информација, за којашто таа смета дека е релевантна само во нејзината работа.;

- **Разлики во методите на работа** – ова првенствено се однесува на начините за прибирање податоци, воспоставените практики при анализата на податоците и изработката на конечната информација. Потребно е да се направи усогласување помеѓу институциите на делот што се однесува на заштита на изворите на податоци и на методите на прибирање, како на пример идентитетот на инфилтрирани или врбувани агенти, тајната употреба на технички средства и сл., бидејќи постојат разлики во

методите за прибирање податоци. Некои служби се фокусираат повеќе на користење човечки извори, додека други повеќе приоритет им даваат на техничките методи на прибирање. Обврските на институциите кои се дел од безбедносниот сектор треба да вклучуваат и усогласување на терминологијата и форматот за изработка на информациите со цел полесно пребарување, пронаоѓање и искористување на информациите кои се споделуваат. Исто така, потребно е и усогласување на степените на класификација на информациите кои се однесуваат на ист предмет на интерес, кој се обработува од различни институции.;

- **Преклопување на јурисдикцијата и овластувањата** - заедничките одговорности, работата во слични области и преклопувањето на јурисдикцијата имаат големо влијание врз соработката помеѓу институциите. Подоброто разбирање на областа на работа и целите на различните институции може да придонесе кон подобро разбирање и усогласување на активностите на безбедносните институции и да ја унапреди нивната соработка на многу полиња, вклучително и на полето на споделување информации.[91].

4.3.2. Препреки кои произлегуваат од карактеристиките на информациите кои се споделуваат

Критичност на информацијата

Критичноста на информацијата се однесува на итноста на информацијата и на потенцијалната штета што може да настане доколку информацијата не се сподели со *оние што мора да ја добијат што побргу. На пример, одредена безбедносна институција* преку свои извори добива информација дека за одредено време ќе се случи терористички напад на одредена локација (фреквентна локација или јавно превозно средство). Оваа информација има висок степен на критичност, бидејќи ако не се сподели во најкус можен рок (ова е всушност елементот на итноста) со институцијата која се занимава со антитероризам, штетата што ќе настане ќе биде катастрофална[92].

[91] Ibid, p.82

[92] Ibid, p.62

Штетата што може да настане доколку не се постапи навремено по одредена информација, има критично влијание за споделувањето на таа информација и треба да дејствува како поттик за споделување. Навременоста на информацијата, исто така, е поврзана со нејзината критичност. Некои информации се временско-чувствителни (итни) и ова се одразува на нивното споделување. Треба да се напомене и дека за информациите кои имаат сомнителна содржина, препорачливо е да се потврди нивната веродостојност и точност пред да се споделат. Како се доближува моментот кога информацијата ќе биде бескорисна доколку не се сподели, одлуката дали да се сподели или не треба да се донесе.

Квалитетот на информацијата

Квалитетот на информацијата исто така се одредува во зависност од перспективата и улогата на испраќачот. Информација која е многу квалитетна за една институција, може да се покаже како информација со мал квалитет и вредност за друга институција. Квалитетот на информацијата се дефинира како степенот до кој одредена информација ги исполнува потребите на нејзиниот корисник. Квалитетната информација треба да ги поседува следниве карактеристики: навременост, точност, комплетност, конзистентност и релевантност во однос на предметот на интерес за кој се однесува[93].

Степенот на класификација на информацијата

Доколку информацијата има одреден степен на класификација, споделувањето на таа информација е многу покомплексно. Имено, согласно степенот на класификацијата, таа информација може да се доставува само до лица кои поседуваат најмалку соодветен степен на безбедносен сертификат. Исто така, треба да се земе предвид и принципот „потребно е да знае“, бидејќи таа информација ќе се сподели само со оние лица што имаат службена потреба и овластувања да ја добијат таа информација. Затоа слободно може да се каже дека степенот на класификација ја отежнува дисеминацијата и споделувањето на информацијата, но позитивна страна е пак што поставува конзистентни стандарди за пристап, кои мора да се почитуваат.

[93] Ibid, p. 63.

4.3.3. Препреки од техничка природа

Развивањето и имплементацијата на соодветни информатичко-технолошки решенија може да придонесе за поефективното споделување информации. Мора да се надмине недостатокот на соработка и интероперабилност помеѓу институциите кои се дел од безбедносниот сектор. Нови технологии за интеграција и споделување на информации може да им помогнат на институциите да го надминат овој недостаток без да има потреба од радикални промени[94]. Ваквата ситуација би им овозможила на институциите кои се дел од безбедносниот сектор да работат заедно, но сепак да ја задржат својата автономија, и да се надминат сите препреки кои се исправени пред ова практично решение. Употребата на вакви технолошки решенија значително ќе ги олесни идентификувањето, интеграцијата и процесирањето информации кои треба да бидат споделени помеѓу луѓето и институциите во безбедносниот сектор. Безбедносниот сектор мора да се насочи кон развивањето на информатичка технологија која ќе даде решение за беспрекорно споделување информации, ќе овозможи непрекината транспарентна и висококвалитетна услуга, ќе овозможи заштита на приватноста и безбедноста на информациите и ќе инсталира доверба и желба кај учесниците за понатамошно учество и соработка[95].

Системот за споделување информации треба да обединува информации од повеќе извори и да им овозможи на донесувачите на одлуки подобро да ги разберат и да донесат вистински одлуки за безбедносните закани. Тој ја користи технологијата со цел да ја унапреди будноста и соработката во неколку дисциплини преку поврзување на аудио, видео и дата комуникации, без разлика дали се класифицирани или не, и за да оствари брзо поврзување на различните организации кои учествуваат во безбедносниот сектор, со цел да се разменуваат информации, сознанија за потенцијални напади и извештаи во реално време. Системот треба да придонесе за пополнување на празнини, зајакнување на врските помеѓу институциите и да овозможи иновативност, брзина и флексибилност во споделувањето корисни информации. Преку употребата на соодветна технологија, овој систем треба да претставува рамка за поврзување на

---

[94] Dacey F. Robert and Hite C. Randolph - *„Homeland Security:Information Sharing Responsibilities, Challenges, and Key Management Issues"*, Testimony Before the Committee on Government Reform, House of Representatives, Washington, 2003, p. 37

[95] Treglia, Joseph – *„Three Essays on Law Enforcement and Emergency Response Information Sharing and Collaboration: An Insider Perspective"*, Dissertation, Syracuse University Surface, NY, 2013, p.115

неколку системи за прием и доставување на информации, и да биде платформа за поврзување на различните институции и нивните уникатни гледишта и ставови.

За да се реализира споделувањето, од неопходно значење е да се намали влијанието на (или целосно да се отстрани) одредени технички препреки кои го отежнуваат споделувањето. Овие препреки, всушност претставуваат одредени технички предуслови кои треба да се исполнат, со цел техничкиот систем кој се користи за споделувањето да биде едноставен, евтин, безбеден и да може лесно да се вклопи во оперативната средина. Подолу се елаборирани главните предуслови кои треба да се исполнат.

Интероперабилност на системите

Интероперабилноста е критично прашање бидејќи различните институции користат различни информациски системи и програми. Ова останува еден од главните предизвици, бидејќи недостатокот на стандардни системи претставува сериозна пречка за споделувањето. Ситуацијата дополнително се комплицира бидејќи со постојаното одложување за донесувањето на овие стандарди, институциите во меѓувреме вложуваат во нови или надградба на постојните системи.

Функционирање на системот

Потребно е да се обезбеди воспоставување, одржување и функционалност на информациски систем на единствена методолошка и технолошка основа. Главната цел на овој систем е да даде поддршка на безбедносните институции на Република Македонија во борбата против сите појавни форми на безбедносни закани кои можат да ја нарушат националната безбедност. Тој систем треба да поседува доволен капацитет (брзина на работа, пребарување, автоматско детектирање на можни совпаѓања, складирање на податоци и сл.) за изведување на неговите функции на висококвалитетно ниво, што ќе им овозможи ефикасна соработка на институциите кои го користат за споделување информации. Исто така, тој треба да биде едноставен за користење, односно информациите мораат да бидат ажурирани и класификувани согласно потребите и приоритетите на корисниците, како и да овозможува координација на различните институции вклучени во неговото користење.

Безбедносни мерки и контрола на системот

Од неопходно значење е да бидат опфатени сите аспекти на безбедноста, да бидат евалуирани и интегрирани во системот, осигурувајќи притоа нормално функционирање, поткрепено со соодветни контролни механизми, вклучувајќи ги следниве активности:

- неопходно да се утврдат оперативни процедури кои детално ќе ги уредуваат операциите кои ќе се преземаат;
- идентификација на корисници и следење на сите реализирани оперативни маневри, како и евиденција за времето на логирање на корисниците (влез и излез);
- пропишани постапки за соодветна реакција во случај на проблеми или нарушувања на безбедноста на системот;
- утврдување на процесот за криптирање на информациите: кои информации да се криптираат, како да се менаџираат шифрите за криптирање, како да се реагира во случај на проблеми кои се поврзани со криптирањето и сл.

Контролата за пристап, користење и вршење промени на системот и на информациите во него се смета за еден од најважните фактори во одлуката да се споделуваат информации. Губењето контрола врз информацијата, или менувањето на нејзината содржина откако ќе се сподели, претставува голема грижа за оној што ја споделил таа информација. Неопходно е да се врши следење и регистрирање на секое користење и дисеминација на одредена информација, што ќе придонесе за зголемување на сигурноста и довербата на сите страни кои учествуваат во процесот.[96]

Информациите треба да останат под целосна контрола на институцијата која ги изработила и споделила (создавачот) и другите учесници не треба да имаат овластувања да ја менуваат таа информација. Создавачот е одговорен за точноста на информацијата, нејзиното ажурирање и ограничувањата за периодот на нејзиното чување во системот. Овој систем треба да обезбедува голем опсег на споделување информации, почнувајќи од комплетен пристап до информациите на некоја од другите институции преку пристап до информации на кои содржината им е читлива, но само податоците за изворите или за методите на прибирање се отстранети, па сè до презентирање само на заклучоци од одредена информација кои се важни за

[96] Ibid, p.68

институцијата која ги прима. Исто така, со помош на техничките системи може да се согледаат и заедничките полиња на интерес на различните институции и соодветно на ова да се воспостави комуникација и да почне заеднички да се работи во насока на унапредување на работата.

Безбедноста на системот мора да биде планирана однапред и да биде спроведена во текот на еволуцијата на проектот согласно потребното и договореното ниво на безбедност меѓу релевантните институции кои ќе учествуваат во неговото користење. Исто така, безбедносната инфраструктура мора да овозможува натамошна надградба во повисоко ниво на безбедност.

Во однос на информатичко-технолошките решенија, безбедносниот сектор на Република Македонија не располага со безбеден и модерен систем, кој ќе овозможи електронски трансфер на информации помеѓу институциите внатре во безбедносниот сектор, и помеѓу безбедносниот сектор и останатите институции. Неопходно е да се работи на пронаоѓање на едно такво решение, затоа што основата за успешно споделување, и внатре во безбедносниот сектор и надвор од него, ја формираат современи, безбедни и лесни за користење компјутерски системи.

4.3.4. Препреки кои произлегуваат од недостатокот на утврдени законски регулативи и процедури за споделување

Законски регулативи

Регулативите, директивите и процедурите кои се однесуваат на споделувањето се многу комплексни. Ова претставува сериозен проблем за оние институции кои веќе ги имаат согледано придобивките од споделувањето, и кои инсистираат за негово унапредување. Бидејќи одредени институции немаат јасни насоки за споделување информации, тие може да изберат да играат на сигурно и воопшто да не споделуваат информации, со цел да се заштитат од одговорноста.

Постоењето на јасни регулативи кои се спроведуваат одговорно ќе резултира со зголемување на бројот на споделени информации, а како дополнителна придобивка ќе биде и сè поголемото запознавање со, и почитување на тие регулативи. Процедурите кои се однесуваат на улогите и одговорностите треба да бидат јасно дефинирани и прифатени од сите институции кои се вклучени во процесот на споделување. Овие

процедури треба да обезбедат конзистентност, да ги дефинираат одговорностите, да ја намалат несигурноста и воочените недостатоци, и да придонесат за професионализација на целата операција.

Управување со споделувањето

Институциите дејствуваат независно една од друга и во насока на сопствените интереси, како и на колективната безбедност на државата. Бидејќи споделувањето информации може да придонесе за нивна поуспешна работа, тие треба да донесат одлука да се вклучат во тој процес и да работат на негово унапредување. Постоењето на централизирано тело кое ќе го уредува споделувањето е од големо значење и е значаен фактор во тоа унапредување, но за да се формира тоа тело и за успешно да функционира потребно е да бидат исполнети следниве предуслови: одлично разбирање на процесот на споделување и на неговите препреки и придобивки, законските регулативи кои се однесуваат на споделувањето, моменталната состојба по институциите во однос на споделувањето, познавање на потребите и побарувањата за информации, одлично познавање на работата на безбедносните институции посебно и безбедносниот сектор како целина, препознавање на област на работа на институциите и нивните цели.

4.4. Решенија за унапредување на споделувањето

Многу е важно секоја од институциите кои се вклучени во процесот да ја поддржи, активно да се вклучи и да ја препознае важноста на споделувањето информации. Целта е да се трансформира безбедносниот сектор на начин кој ќе резултира со зголемена и поефикасна комуникација помеѓу неговите компоненти, која ќе придонесе кон поквалитетно и поприменливо споделување и поефикасна употреба на споделените информации[97].

Што може да се направи за да се надминат препреките кои го спречуваат споделувањето? Дали фокусирањето на проблемот преку една заедничка концептуална

[97] United States Intelligence Community – „ *Information Sharing Strategy*", Office of the Director of National Intelligence, Washington DC, 2008, p.4

рамка ќе овозможи увид кој ќе помогне во унапредувањето на теоријата и практиката? Бидејќи погоре беа идентификувани најзначајните препреки за споделување информации, подолу се дадени препораки кои ги опфаќаат активностите кои треба да се преземат со цел надминување на тие препреки. Некои од препораките се општи и се однесуваат генерално на процесот на споделување, додека некои се однесуваат конкретно на соодветните препреки. Подолу се дадени некои препораки кои може да го унапредат споделувањето.

4.4.1. Генерални препораки за успешно споделување информации

- Развивање на сеопфатен и координиран национален план за подобрување на споделувањето на информации во безбедносниот сектор, кој треба јасно да ги дефинира улогата и одговорностите на секоја од институциите на безбедносниот сектор, да се дефинираат целите и задачите и да се одреди временска рамка за реализација на тој план.;
- Да се изработи една сеопфатна архитектура за целиот процес на споделување која ќе ги опфаќа моменталните и очекуваните состојби и да се прави редовно ажурирање за секоја постапка која се презема во однос на унапредување на процесот, со цел да се координираат и да се менаџираат иницијативите.;[98]
- Ефикасната алокација на ресурсите и правилното насочување на трошоците се едни од најефикасните постапки кои треба да се преземат за да се спроведе споделувањето[99]. Се очекува дека намалувањето на трошоците ќе биде резултат на побрзата реакција кон безбедносните закани и од подготвеноста за евентуални напади.;
- За подобро да се разбере вредноста на споделувањето информации, потребно е да се спроведат обуки и семинари на кои ќе се направи размена на искуства и ќе се нагласат сите предности кои ги нуди споделувањето.;

---

[98] U.S. Department of Justice Office of the Inspector General Audit Division – *„ The Federal Bureau of Investigation's Efforts to Improve the Sharing of Intelligence and Other Information"*, Audit Report 04-10, 2003, p.20

[99] European Network and Information Security Agency (ENISA) – *„Incentives and Challenges for Information Sharing in the Context of Network and Information Security"*, Heraklion, Greece, 2010, p.16

- Постојано да се нагласува потребата за одговорно споделување и да се акцентираат придобивките кои произлегуваат од споделувањето.;
- Да се бараат нови начини и да се покренуваат нови иницијативи со цел унапредување на процесот (преку воочени проблеми, анализа на досега постигнатото, остварени искуства, заеднички предлози и сл.).;
- Да се уредат прашањата кои се однесуваат на заштитата на граѓанските права и слободи (како, на пример, заштитата на личните податоци, правото на приватност и сл).

4.4.2. Препораки за надминување на препреките кои произлегуваат од учесниците во процесот на споделување информации

- Идентификување на начини за подобра оперативна соработка помеѓу учесниците.;
- Воспоставување на позиција на офицери за врска во најважните конституенти на безбедносниот сектор.;
- Потребата од меѓусебна доверба е многу значаен фактор. Довербата мора да се гради постепено и преку добри персонални односи; одржување редовни состаноци; градење на една перцепција дека учесниците имаат слични желби и намери; како и преку препорака од почитувани соработници. И покрај тоа што личната интеракција е многу важна за создавањето доверба, таа може да се воспостави и на институционално ниво, благодарение на сличните професионални интереси и познавања на одредени појави и предмети. Исто така, од круцијално значење е и воспоставувањето и конзистентната употреба на заеднички прифатени начини на однесување, кои ќе го минимизираат ризикот за нарушување на безбедноста и дополнително ја зголемуваат довербата.;[100]
- Воспоставување ефикасни и безбедни механизми за комуникација помеѓу институциите.;
- Дизајн и имплементација на мерки и активности за заштита на безбедноста на споделените информации.;

[100] Ibid, p.20

- Зголемување и интеграција на способностите за идентификување, разбирање и споделување на информации кои се однесуваат на конкретен предмет на интерес.;
- Успешните претходни соработки можат да ја намалат несигурноста при идните споделувања;
- Да се пронајдат начини да се зајакнат напорите за споделување информации преку учеството во национални иницијативи (работни групи, комисии, заеднички единици). ;[101]
- Припадниците на институциите кои го сочинуваат безбедносниот сектор треба да се поттикнуваат да развијат професионални односи со своите колеги од другите институции.;
- Да се формираат работни групи, кои ќе придонесат кон промоција на соработката и воспоставувањето продуктивни релации преку изградувањето пријателски врски и меѓусебна доверба.

4.4.3. Препораки за надминување на препреките кои произлегуваат од карактеристиките на информациите кои се споделуваат

- Усогласување на форматот и стандардите за изработка на информациите, со цел нивна полесна употреба при споделувањето.;
- Имплементација на систем за дисеминација на информациите кон соодветните корисници.;
- Идентификување и усогласување во поглед на видот на информации кои ќе бидат споделувани помеѓу институциите.;
- Споделувањето квалитетни информации е најдобриот начин да се согледа вредноста на споделувањето и да се изгради меѓусебна доверба. Информациите мора да бидат навремени и веродостојни, но и релевантни за институцијата која ги добива.

[101] U.S. Department of Justice – „National Criminal Intelligence Sharing Plan - *Solutions and approaches for a cohesive plan to improve our nation's ability to develop and share criminal intelligence"*, U.S. Department of Justice's Global Justice Information Sharing Initiative, Washington DC, 2003, p.10

4.4.4. Препораки за надминување на техничките препреки

- Развивање информатичка технологија која ќе даде решение за беспрекорно споделување информации и ќе овозможи непрекината транспарентна и висококвалитетна услуга.

4.4.5. Препораки за надминување на препреките кои произлегуваат од недостатокот на утврдени законски регулативи и процедури за споделување

- Донесување нови и хармонизација на постојните законски акти и стандарди за работа кои се однесуваат на добивањето, пристапот, употребата, споделувањето и чувањето на информациите.;[102]
- Изработка на упатства и процедури за споделување, кои ќе вклучуваат насоки за тоа кои типови на информации треба да се споделуваат, и под какви околности.;
- Да се направи напор за надминување на несигурностите кои се однесуваат на разликите помеѓу законските регулативи во различните институции и да се формира заедничка рамка за соработка.;
- Процедурите, процесите и системите кои се користат за споделување информации мора да бидат во согласност со воспоставените директиви и упатства за работа кои се донесени.

Напорите за унапредување на споделувањето може да се согледаат и од друг аспект, односно од аспект на учесниците во споделувањето. Имено, тие се разгледуваат на три нивоа, и тоа на индивидуално, на институционално и на државно:

- на индивидуално ниво затоа што кај секое лице кое е вклучено во процесот на споделување, треба да се всади една одговорност која ќе му помогне да почувствува и да знае кога и со кого треба да се сподели одредена информација;
- институционално затоа што донесувањето процедури и упатства им помага на институциите во разбирањето на правилата на игра, и ја олеснува распределбата на работните задачи и обврски;

[102] United States Intelligence Community – *„Strategic Intent for Information sharing 2011-2015“*, Office of the Director of National Intelligence, Washington DC, p.9

– на државно ниво, затоа што токму највисоките државни органи треба активно да го поддржат процесот на споделување информации[103].

Надминувањето на препреките кои го отежнуваат споделувањето мора да биде еден постојан напор што бара силна посветеност од сите нивоа на безбедносниот сектор. Овие напори не треба да бидат статични активности кои ќе бидат покренати и потоа заборавени. Напротив, тие треба да бидат еден континуиран напор што ќе успее целосно да го интегрира споделувањето информации во организационата култура, вредностите, работните обврски и упатствата за работа на секоја од институциите кои го сочинуваат безбедносниот сектор. Тие треба да ги поддржуваат и да ги унапредуваат иницијативите кои треба да се преземат на секое ниво, да понудат практични објаснувања за предизвиците кои се појавуваат и да понудат мулти-институционална перспектива која е потребна за да се исполнат целите на споделувањето.

Безбедносниот сектор мора да работи во насока на воспоставување интегриран национален систем за споделување информации, со цел да осигура дека оние на кои им се потребни информации за да ја заштитат нашата држава од безбедносни закани ќе ги добијат тие информации и оние што ги поседуваат тие информации ќе имаат обврска да ги споделат. Преку зајакнувањето на културата за споделување информации и преку обезбедувањето директиви, процедури и технички можности да ја поддржат таа култура, безбедносниот сектор креира една клима неопходна за неговите припадници целосно да ја прифатат улогата на споделувањето информации и да го продлабочат нивното сфаќање за неговата значајност во одржувањето на националната безбедност.

4.5. Модел за споделување

Споделувањето е најкорисно кога ќе биде организирано на начин при кој сите институции се подредени како дел од една интегрирана мрежа, која ќе ги надминува традиционалните организациони граници и ќе придонесе кон побрзо и појасно разбирање на безбедносните закони.[104]

---

[103] European Network and Information Security Agency (ENISA) – *„Incentives and Challenges for Information Sharing in the Context of Network and Information Security"*, Heraklion, Greece, 2010, p.14

[104] Pfeifer W, Joseph – *„Network Fusion: Information and Intelligence Sharing for a Networked World"*, Homeland Security Affairs, Vol.8, US, 2012, p.2

Институциите мора постојано да ја балансираат потребата за споделување чувствителни информации со потребата да се заштитат тие информации од неовластено објавување во јавност. Напорите да се промовира поефективно споделување безбедносни информации мора да ја земе предвид и потребата за заштитување на тие информации. Донесувањето модел за насочување и интегрирање на големиот број на активности од кои треба да се состои процесот на споделувањето е неопходно и оваа обврска треба да биде заедничка за сите институции кои ќе се вклучат во процесот.[105]

Главните елементи во овој модел се насочени кон унапредување на процесот на споделување и вклучуваат јасна делинеација на улогите и одговорностите на сите учесници во процесот, дефинирање на очекуваните цели.

Овој модел функционира врз основа на следниве два постулати:

1. Безбедно споделување - ги вклучува физичките, техничките и процедуралните мерки кои треба да обезбедат заштита на информацијата, нејзин безбеден пренос и чување од неовластено објавување и неовластен пристап и

2. Одговорно споделување - подразбира дејствување во согласност со законските регулативи и процедури, конзистентност во остварувањето на зацртаните стратегиски и оперативни цели, притоа земајќи ги предвид заштитата на изворите и методите кои се користат, заштитата на основните човекови права и заштитата на приватноста.[106]

Предложениот модел е составен од неколку стратегиски и оперативни компоненти. Секоја од нив има свое значење за неговото беспрекорно функционирање, а нивниот однос е интерактивен и меѓузависен. Функцијата на овој модел е да им обезбеди поддршка на институциите од моментот на прибирање на податоците, изработката на крајните информации и донесувањето на одлуката за споделување. Безбедносниот сектор мора да им обезбеди максимална достапност и пристап на своите компоненти до сите информации кои се однесуваат на националната безбедност. За да се оствари тој пристап до што повеќе информации, потребно е да се усвојат конзистентни практики за пристап, да се воспостават унифицирани стандарди за безбедност на информациите, и различните институции да бидат подготвени да се

---

[105] United States Government Accountability Office (GAO) – *„Information Sharing - The Federal Government Needs to Establish Policies and Processes for Sharing Terrorism-Related and Sensitive but Unclassified Information"*, Report to Congressional Requesters, Washington DC, 2006, p.3

[106] United States Intelligence Community – *„Strategic Intent for Information sharing 2011-2015"*, Office of the Director of National Intelligence, Washington DC, p.7

вклучат во процесот на споделување. Веродостојноста на информациите кои се споделуваат, степенот на меѓусебна доверба помеѓу институциите кои споделуваат информации, мерките и активностите за заштита на информациите и начинот на кој ќе бидат употребени информациите се есенцијалните елементи на воспоставувањето на околина на доверба. Моделот за споделување мора да ги земе предвид овие елементи за да обезбеди слободен проток на информации помеѓу учесниците во процесот.

Исто така, овој модел вклучува и еден осврт на принципот „потребно е да знае", кој во некои случаи може да претставува пречка за споделувањето. Уште од самото формирање на безбедносните институции, принципот „потребно е да знае", со кој се обезбедува заштита на изворите и на методите, има голема примена. Користењето на овој принцип е базиран на два важни фактори: (1) да се намали ризикот од неовластено објавување чувствителни информации и да се спречи ситуацијата да завршат во погрешни раце и (2) потребата да се заштитат изворите на податоци и методите кои се користат, со цел да се минимизира какво било нивно компромитирање.[107]

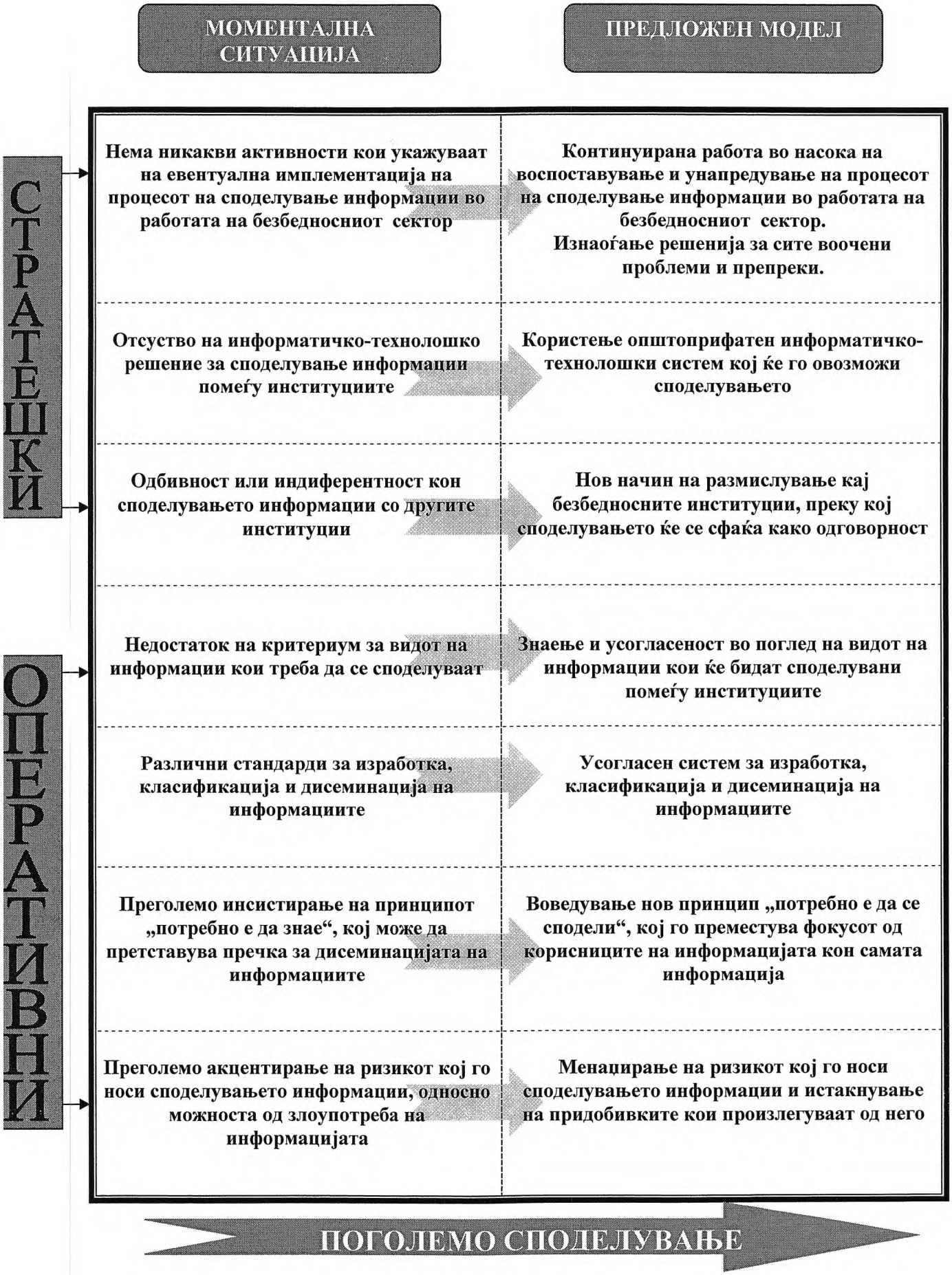
Меѓутоа, различните институции имаат воспоставено свои правила и процедури за дисеминација, кои резултираат со неконзистентност во споделувањето. Затоа предложениот модел за споделување воведува еден нов принцип, наречен „потребно е да се сподели", кој ќе биде насочен кон унапредувањето на споделувањето информации. Во денешната сложена безбедносна средина, ризикот од несподелувањето информации може да доведе до пропуштање на важни сознанија кои се однесуваат на одредени антиопштествени дејства, кои може да предизвикаат загуба на човечки животи и да ја загрозат националната безбедност. Оваа нова средина бара од безбедносниот сектор да работи во насока на создавање една култура која ќе промовира одговорност за споделување, и која треба да осигура дека сите компоненти на безбедносниот сектор имаат волја, можности и инфраструктура за споделување. Новиот принцип ќе придонесе токму во таа насока, притоа функционирајќи како воспоставена практика во донесувањето одлука дали една информација да се сподели.

Воспоставувањето култура која ќе го охрабрува одговорното споделување информации е неопходно за успехот на моделот. Треба да се спроведат обуки кои ќе стават акцент на одговорноста за споделување, и кои ќе придонесат за разбирањето на импликациите за заштита на изворите и методите, како и за заштитата на граѓанските права и слободи. Доколку учесниците во процесот можат да препознаат дека нивниот

[107] United States Intelligence Community – *„ Information Sharing Strategy"*, Office of the Director of National Intelligence, Washington DC, 2008, p.8

професионален успех делумно зависи и од нивното учество во споделувањето информации, тоа ќе биде огромен поттик за процесот за споделување. Со промовирањето на култура за споделување информации, учесниците во процесот самите ќе работат во насока на отстранување на пречките и во изнаоѓањето подобри методи и алатки за споделување.

Овој модел за споделување претставува една оригинална намера, преку која треба да се направи унапредување и зацврстување на клучните стратегиски и оперативни цели за споделување информации на кои треба да се фокусира безбедносниот сектор во наредните години. Овие стратегиски цели треба да се разгледуваат долгорочно, при што нивната реализација треба да се гледа како индикатор за успешното остварување на целите кога е во прашање споделувањето информации. Со цел да заживее овој модел, мора да се идентификуваат предизвиците и грешките кои ќе се појават, да се унапреди културата во безбедносниот сектор во однос на промоција и препознавање на предностите кои ги нуди споделувањето и да се усвои пристап кој ќе вклучува менаџирање на безбедносните ризици кои го носи споделувањето.



Дијаграм бр.6 – Модел за споделување информации

4.6. Споделување информации помеѓу безбедносниот и приватниот сектор

Со цел да ја исполни својата функција, потребно е безбедносниот сектор да оствари ефикасна соработка со сите други субјекти во општеството чијашто дејност директно или индиректно е поврзана или има допир со превенцијата и сузбивањето на безбедносните закани. Споделувањето информации помеѓу државните органи и приватниот сектор е многу моќен механизам за подобро разбирање на константно променливата безбедносна средина и разбирање на сериозните ризици, ранливости и закани, како и пронаоѓањето решенија за нив. Ова партнерство функционира преку споделувањето информации за сајбер напади, справување со природни катастрофи и физички закани. Поттик за ова споделување треба да претставуваат предностите со кои ќе се стекнат учесниците преку соработката во однос на заедничките проблеми и пристапот до информации кои не можат да ги добијат на друг начин, освен преку учеството во процесот на споделување.[108]

Со оглед на тоа дека поголемиот дел од критичната инфраструктура во државата (а и во светот), како на пример енергетското производство и дистрибуција, финансиските услуги, транспортот, нафтата и природниот гас, како и електронските комуникации, е во посед и под контрола на приватниот сектор, општо прифатен став е дека заканите со коишто се соочуваат овие есенцијални општествени двигатели може да бидат минимизирани доколку сите релевантни организации и институции – и од државниот и од приватниот сектор – споделуваат информации кои се однесуваат на слабостите (ранливостите) што ги имаат и безбедносните закани и ризици со кои се соочуваат.[109] Тие се сметаат за критична инфраструктура бидејќи прекинот на нивното функционирање ќе има сериозен ефект врз виталните општествени функции.

Мора да се направи еден заеднички напор со цел да се дојде до ситуација во која споделувањето меѓу државните и приватните организации ќе биде сметано како неопходна компонента во одржувањето на националната безбедност на државата.

---

[108] European Network and Information Security Agency (ENISA) – *„Good Practice Guide – Network Security Information Exchanges"*, Heraklion, Greece, 2009, p.10

[109] European Network and Information Security Agency (ENISA) – *„Incentives and Challenges for Information Sharing in the Context of Network and Information Security"*, Heraklion, Greece, 2010, p.8

Некои од постапките кои треба да се преземат се следниве:

- треба да се направи една платформа за споделување која ќе ги опфати сите постапки и процедури која ќе придонесе кон подобро разбирање на безбедносните димензии на критичната инфраструктура, како и делинеација на улогите и одговорностите на државните и на приватните учесници во процесот на споделување;
- координација на ваквата платформа помеѓу учесниците во поглед на обезбедување минимални безбедносни стандарди и рационални пристапи кон проценките на безбедносните ризици;
- да се стави акцент на двонасочното споделување информации помеѓу државниот и приватниот сектор (споделувањето да не биде едностранo) и да се работи во насока на унапредувањето на меѓусебната доверба меѓу нив;
- споделувањето да ги вклучува сите оние што може да придонесат за безбедноста и нормалното функционирање на критичната инфраструктура, притоа балансирајќи го големиот број учесници во процесот со менаџирањето на ризикот од неовластен пристап или објавување на информации;
- безбедносниот сектор и приватниот сектор треба да воспостават формални начини за споделување информации кои ќе ја унапредат заштитата и издржливоста на критичната инфраструктура.

И покрај тоа што државните органи имаат пристап до голем број информации, постојат голем број процедурални и организациони препреки кои ја спречуваат соработката на полето на споделување информации со приватниот сектор. Се добива впечаток дека државните институции имаат интерес од добивањето информации, но не и од споделувањето на информациите кои ги поседуваат.[110] Токму затоа треба да се има предвид дека приватниот сектор има одредени забелешки кога е во прашање споделувањето информации со безбедносните органи, а во овој контекст не треба да се заборават и дополнителните напори кога е во прашање издавањето безбедносни сертификати за приватните компании, како и на лицата кои се вработени во нив.

Исто така, треба да се нагласи и фактот дека компаниите од приватниот сектор кои учествуваат во споделувањето информации имаат голем интерес во заштитата на својата репутација и на информациите кои ги споделуваат. Нарушувањето на безбедноста на споделените информации или неовластениот пристап до нив од страна

[110] Ibid, p.33

на конкурентска компанија може да има катастрофален ефект врз работата на компанијата (дури и врз нејзиното натамошно постоење) која ги споделила информациите.

4.7. Споделување информации со други држави

Во денешниот современ свет, ризиците, слабостите и заканите за безбедноста се глобални. Споделувањето информации само на национално ниво нема да има пресуден ефект кога се во прашање горенаведените фактори. Успешното спроведување на процесот на споделување информации на национално ниво претставува едно своевидно поплочување на патот кој треба да води кон поширока соработка и развивање на процесот на споделување информации на билатерално и мултилатерално ниво. Ова партнерство треба да се развива на тактичко и на стратегиско ниво преку споделувањето информации кои се однесуваат на безбедносни инциденти, слабости и ранливости на системот, безбедносни закани и мерки и активности кои треба да се преземат. Исто така, треба да се преземат и сите мерки и активности за надминување на препреките кои се испречени пред процесот на споделување.[111]

Споделувањето информации е форма на меѓународна соработка која овозможува барем една од државите учеснички да добие поголем број или поквалитетни информации.[112] Информациите се споделуваат билатерално и мултилатерално.

Билатералната соработка го вклучува споделувањето информации за предмети кои се од заеднички интерес. Таквиот вид соработка се темели на quid pro quo соработка, бидејќи безбедносните институции се однесуваат заштитнички кон своите извори и методите што ги користат за прибирање податоци, и не се баш расположени да ги споделат тие информации доколку со тоа не остварат одредена корист. Директен резултат на оваа транспарентност е зголемувањето на довербата помеѓу институциите, што пак придонесува до унапредување на процесот на споделување. Бидејќи некои

[111] European Network and Information Security Agency (ENISA) – *„Good Practice Guide – Network Security Information Exchanges"*, Heraklion, Greece, 2009, p.9-10

[112] Walsh Igoe, James – *„Defection and Hierarchy in International Intelligence Sharing"*, Cambridge University Press, UK, 2007, p.155

безбедносни институции од помалите држави имаат ограничени ресурси и не секогаш имаат еднакви можности споредено со институциите од поголемите држави, не може секогаш да се постигне еднаков реципроцитет. Меѓутоа, тие можат да дадат придонес на други начини, како на пример овозможување на пристап до информации за некои појави и региони кои се покажале како ненадминлива пречка за институцијата со која се врши споделувањето.[113] Исто така, овој вид на соработка вклучува воспоставување на офицери за врски помеѓу безбедносните институции на двете држави. Друг случај е овозможувањето на заеднички пристап кон информациите преку комуникациско-информациски системи, како на пример електронски бази на податоци.

Друг тип на соработка се мултилатералните договори. Ова се најчесто договори помеѓу повеќе држави кои се соочени со слични безбедносни предизвици и на кои им оди во прилог да ги обединат своите сили во борбата против заедничкиот непријател (на пример, меѓународна терористичка група која дејствува на територите на повеќе соседски држави, или организирана криминална група која користи територии на повеќе држави за остварување на својата криминална активност, како, на пример, трговија со дрога или оружје).[114] Мултилатералната соработка се користи за справување со транснационални појави како организиран криминал и меѓународен тероризам, чиешто спречување во една држава ќе претставува успех за сите држави кои соработуваат на тоа поле, и ќе претставува еден поттик за државите уште повеќе да вложат во таа соработка, а ќе претставува и своевидна мотивација за други држави да се вклучат во споделувањето информации. Мултилатералното поврзување во поглед на споделувањето информации може да вклучува и поставување офицери за врска и развивање заеднички комуникациско-информатички решенија за споделување информации.[115]

---

[113] Geneva Center for the Democratic Control of Armed Forces (DCAF) – *„Contemporary Challenges for the Intelligence Community"*, Geneva, Switzerland, 2006, p.4

[114] Одличен пример за мултилатерално споделување претставува договорот UKUSA кој го уредува споделувањето на разузнавачки информации прибрани преку употреба на технички методи. Освен Велика Британија и САД, во овој договор учесници се и Канада, Австралија и Нов Зеланд. Овој договор вклучува мерки кои ги штитат интересите на сите страни кои се вклучени во споделувањето. На пример, се претпоставува дека овој договор содржи и правила за тоа колку широко може да биде дисеминирана една информација, во него со воспоставени заеднички безбедносни процедури, техничките поими кои се употребуваат се стандардизирани и усогласени, а постои и спецификација за тоа кои типови на информации ќе се споделуваат, а кои не. - Walsh Igoe, James – *„Intelligence Sharing in the European Union – Institutions are not enough"*, JCMS, Vol.44, No.3, 2006, p.631

[115] Geneva Center for the Democratic Control of Armed Forces (DCAF) – *„Contemporary Challenges for the Intelligence Community"*, Geneva, Switzerland, 2006, p.5

Бидејќи билатералните договори за споделување информации се доминантната форма на соработка кога е во прашање споделувањето информации помеѓу држави, и најголемиот број карактеристики на билатералното споделување се присутни и во мултилатералното споделување, во натамошниот текст ќе се стави акцент на дескрипцијата на билатералното споделување.

4.7.1. Карактеристики на билатералното споделување информации

Релации се развиваат помеѓу две држави кои имаат заеднички вредности и заеднички интереси и очекуваат дека преку споделувањето корисни информации ќе ги остварат своите интереси и цели. Со цел да постои успешно споделување, потребно е да се воспостави високо ниво на доверба помеѓу двете држави и помеѓу нивните безбедносни институции. Соработката помеѓу безбедносните институции веќе може да се смета како една константа во меѓународните односи.

За да биде соработката корисна и за двете страни, мора да има подеднакви нивоа на споделување и оваа врска мора да биде двонасочна. Доколку споделените информации придонесуваат кон успешноста и ефективноста во работата на безбедносните институции на државата која ги добила тие информации, тогаш мора да се воспостави реципроцитет за да може да се продолжи таа релација и да биде корисна. За да биде успешно споделувањето, мора да постои баланс во споделувањето на информациите, бидејќи асиметричното споделување е контрапродуктивно и најчесто се завршува неуспешно. Воспоставувањето симетрично споделување е во најдобар интерес на двете држави кои учествуваат во споделувањето. Секако, земајќи ги предвид променливите геополитички движења, во одредени периоди оваа соработка може да изгледа како едностранa. Но, со цел да се превенира прекин на соработката, повторното воспоставување на балансот во најскоро можно време треба да биде приоритет.

Слично како и во процесот на споделување информации внатре во безбедносниот сектор на една држава, и во билатералното споделување се појавуваат неколку препреки кои имаат одлучувачко влијание врз исходот на споделувањето. Идентификувани се три препреки:

- веродостојноста и квалитетот на информациите кои се споделуваат;

- одржување на безбедноста на информациите кои се споделуваат;
- споделување на добиените информации со трета страна.

Овие препреки стануваат сè покомплицирани ако се земат во предвид динамиките на меѓународните односи, кои секако ги вклучуваат и прашањата околу безбедноста и суверенитетот на државата.

Веродостојноста и квалитетот на информациите кои се споделуваат

Првата препрека произлегува од претпоставката дека донесувачите на одлуки се соочени со значајна несигурност во однос на важните аспекти од надворешно-политичките или безбедносните проблеми, како, на пример, вистинските намери или идните планови на значајните фактори во овие полиња и можните последици од преземањето на одредени активности. Донесувачите на одлуки имаат потреба од информации кои ги добиваат од домашните безбедносни институции, но и од оние што може да ги добијат преку споделувањето со други држави, затоа што колку повеќе информации имаат за еден предмет на интерес, толку повеќе се намалува несигурноста при донесувањето одлуки во врска со него. Бидејќи оваа потреба наметнува голема побарувачка на информации, испраќачот може да ја злоупотреби својата положба и да сподели неточни, некомплетни или фабрикувани информации. За примачот, оваа препрека има големо значење, бидејќи тој не е во можност да ја одреди точноста и веродостојноста на добиените информации. Ова ја остава отворена можноста дека испраќачот може намерно да направи измени во информациите кои се споделуваат со цел да влијае при донесувањето одлуки кај државата на прием во насока на своите сопствени интереси[116].

Несигурноста кај учесниците во споделувањето во поглед на веродостојноста и квалитетот на споделените информации е мотивиран од неколку фактори.

Прво, информациите кои се споделуваат се изработуваат врз основа на прибрани податоци, кои се анализираат и се стават во одреден контекст и се употребуваат за да се извлечат заклучоци за карактеристиките на одредени предмети на интерес и да се направи прогноза на нивните идни манифестации или постапки.

[116] Walsh Igoe, James – *„Defection and Hierarchy in International Intelligence Sharing"*, Cambridge University Press, UK, 2007, p.152

Најчесто, информациите кои се споделуваат претставуваат готови извештаи, анализи и процени, кои се изготвени врз основа на тие податоци. Можноста за злоупотреба на процесот од страна на испраќачот е многу поголема при споделувањето на готови информации, отколку при споделувањето на суровите податоци.

Второ, информациите се составени од податоци кои се прибираат и од отворени и од затворени извори, и најчесто затворените извори не се наведени во информациите кои се споделуваат. Безбедносните институции многу ретко ги откриваат деталите за своите извори, слично како и методите за прибирање на податоците. Оваа практика му овозможува на испраќачот да ги измени или да ги фабрикува информациите кои се добиени преку затворени извори. Исто така, испраќачот може да ја пренагласи веродостојноста на своите извори, тврдејќи дека преку нив добива точни и корисни податоци, но тоа да не е случај.

Трето, испраќачот може да биде во ситуација да поседува одредени информации кои се точни и од големо значење за примачот, но да одлучи да не ги сподели. Мотивот за задржување на информациите е да не му се овозможи на примачот да донесе одлуки врз основа на тие информации (доколку би биле споделени), бидејќи тие одлуки би биле спротивни на интересите на испраќачот.

Одржување на безбедноста на информациите кои се споделуваат

Оваа препрека произлегува од ризикот за нарушување на безбедноста на информацијата и нејзиното неовластено објавување. Започнувајќи од моментот кога една информација ќе му биде отстапена на примачот, испраќачот нема гаранција дека со таа информација ќе се постапува одговорно и адекватно ќе се заштити. Доколку информациите не се чуваат адекватно може да дојде до ситуација да се компромитираат изворите и методите, кои се исклучително значајни при прибирањето на податоци, и да му нанесе голема штета на испраќачот.

Споделување на добиените информации со трета страна

Оваа препрека е многу значајна за одлуката дали ќе се споделат одредени информации со друга држава. И покрај тоа што општоприфатена практика е договорот за споделување да содржи провизии кои се однесуваат на забрана за споделување со трета страна, примачот може да донесе одлука да ги сподели добиените информации со

трета страна. Во ваков случај, примачот смета дека е во негов интерес да ги сподели информациите со трета страна (држава или меѓународна институција), како би имал влијание при донесувањето на некои безбедносни или политички одлуки кај третата страна. Мотивот на примачот може да биде преку тие споделени информации да ги насочи активностите на третата страна во насока на своите сопствени интереси или против интересите на некој негов противник.

4.7.2. Препораки за надминување на препреките за споделување информации со други држави

Како што може да се увиди од објаснувањето на препреките, во основата на секоја од нив лежи недовербата кон потенцијалниот партнер во споделувањето. Проблемот е како да се избалансира оваа недоверба со придобивките од споделувањето?

За да се минимизира недовербата и да се унапреди споделувањето информации помеѓу две држави, потребно е воспоставување механизам што ќе ги заштити и двете страни кои учествуваат во процесот. Воспоставувањето на овој механизам претставува особено тешка задача, која треба да започне со анализа на ризикот од споделувањето и на придобивките од споделувањето. Ова е неопходен почеток за донесувањето одлука дали ќе се започне со споделување и оваа анализа треба да обезбеди една листа на потенцијални придобивки и негативни последици кои може да се остварат со споделувањето информации.[117]

Државите учеснички можат да го структурираат договорот за споделување на начин на кој ќе ги минимизираат можностите и трошоците во случај на прекршување на довербата од страна на едната учесничка. Има неколку постапки, со чиешто преземање значително ќе се намали ризикот од учество во споделувањето.

Прво, како механизам за и двете страни да бидат сигурни дека со споделените информации се постапува одговорно (не се споделуваат со трета страна, заштитени се од неовластен пристап и сл.), договорот за споделување може да вклучува одредени активности кои ќе овозможат увид во ракувањето, чувањето и дисеминацијата на споделените информации. Ова може да вклучува воспоставување офицери за врска во

[117] Ibid, p.155

безбедносните институции меѓу кои ќе се врши споделувањето, како и уредување безбедносни мерки за контрола и користење на информатичко-технолошкиот систем кој ќе се користи за споделување информации, и нивна имплементација од страна на овластени лица на двете држави[118].

Второ, може да се ограничи споделувањето само на информации кои се однесуваат на специфични полиња каде што интересите на двете држави најмногу се преклопуваат, а да не се споделуваат информации кои се однесуваат на области во кои двете страни имаат спротивставени или воопшто немаат никакви интереси. Ваквото ограничување на одредени области кои се од заеднички интерес во голема мера го намалува ризикот од недоверба или нарушување на правилата. Во оваа насока, може да се размислува и точно да се идентификуваат областите и настаните за кои ќе се споделуваат информации, што ќе придонесе за воспоставување на еден стандард што ќе се користи при одлучувањето дали одредена информација ќе се сподели или не. Се разбира, за да се направи такво нешто, и двете страни најпрво мора да бидат убедени дека партнерот има пристап до корисни и точни информации, бидејќи ова е примарната придобивка од соработката.

Трето, треба да се уредат ситуациите во кои може да се укаже потреба покрај конечната информација да се побараат и суровите податоци, како и објаснување за тоа на кој начин се прибрани тие податоци и да се побара мислење за веродостојноста на изворите.Ова ќе му овозможи на примачот да се увери во веродостојноста на одредена споделена информација и да биде уште посигурен во своите анализи и процени[119].

Придобивките од споделувањето информации се многу повеќе видливи кога има што поголема фреквенција на информации кои се споделуваат, како и со обемот на предмети на интерес кои ги вклучува договорот за споделување.

---

[118] Ibid, p.162

[119] Walsh Igoe, James – *„Intelligence Sharing in the European Union – Institutions are not enough"*, JCMS, Vol.44, No.3, 2006, p.630

Глава 5

Заштита на информациите за безбедносниот сектор

5.1. Класификација на информациите

Со класификација на информацијата се определува степенот на заштита на информацијата кој треба да биде соодветен со степенот на штетата што би настанала со неовластен пристап или неовластена употреба на информацијата. Информациите кои се предмет на класификација се однесуваат особено на: јавната безбедност; одбраната; надворешните работи; безбедносни, разузнавачки и контраразузнавачки активности на органите на државната управа; системи, уреди, проекти и планови од важност за јавната безбедност, одбраната, надворешните работи; научни истражувања; технолошки, економски и финансиски работи.[120]

Класификацијата на информациите е комплексна активност, бидејќи треба да постои дефинитивна и видлива причина или рационализација зошто одредена информација се класифицира. Постојат два критериуми кои треба да ја претставуваат основата за одлучување дали една информација ги исполнува условите за заштита, односно дали треба да се класифицира. Тие се:

- **интегритетот на информацијата** – таа е релевантна, веродостојна, прецизна и комплетна и
- **чувствителноста на информација** – таа содржи факти кои имаат големо значење и кои е потребно да се одржат во тајност за да може да се оствари некоја важна цел. Треба да се ограничи пристапот до оваа информација, затоа што доколку дојде до нејзина јавна циркулација, може да се предизвика сериозна штета за интересите на државата или граѓаните.

Овие критериуми се земаат предвид при изработката на проценатa на ризикот и заканите. Целта на оваа процена е да идентификува колкава е веројатноста или изгледите од остварувањето на ризиците и каков ефект ќе има нарушувањето или губењето на интегритетот и чувствителноста на информацијата. И покрај тоа што треба да се постигне некој баланс помеѓу ризиците кои ги носи класификацијата и придобивките кои ги нуди пред да се донесе одлуката за класифицирање, многу е тешко да се пронајде тој баланс. За да се постигне тој баланс, потребно е да се има точна идентификација и процена на ризиците и придобивките за да се донесе вистинската одлука. Меѓутоа, многу ретко ризиците и придобивките можат да се

[120] *„Закон за класифицирани информации"*, Службен весник на Република Македонија бр.9/04 од 27.02.2004 година.

сведат на објективни, недвосмислени и квантифицирани факти, кои ќе придонесат за објективно одлучување. Скоро секогаш постојат несигурности или дилеми при проценувањето на ризиците и придобивките. [121]

Пред да се класифицира одредена информација, треба да се одговори и на прашањето „Дали некласифицирањето на оваа информација или нејзиното неовластено објавување ќе предизвика штета по националната безбедност?“. Одговорот на ова прашање треба да се гледа од два аспекта. Првиот е дали нејзината циркулација во јавност може да предизвика штета за националната безбедност? Нормално, овде ќе треба да се идентификува и специфичната штета која би настанала. Вториот аспект е колкава е веројатноста да настане таа штета. Значи, одговорот за тоа дали ќе настане одредена штета од неовластеното објавување на таа информација треба да се има уште пред да се донесе одлуката за класификација. Исто така, донесувањето на одлуката за класификација не треба единствено да биде базирано врз концептот на настанување на штета врз националната безбедност, туку треба да се земат предвид и финансиските импликации кои произлегуваат од класификацијата. Една информација треба да се класифицира само кога придобивките за националната безбедност ги надминуваат трошоците кои произлегуваат од таа класификација.

Ако се земат предвид погоре наведените критериуми, ќе се дојде до заклучок дека донесувањето одлука за класифицирање на една информација не е воопшто лесна работа. Бидејќи ова не е една егзактна постапка за која има прецизни и унифицирани насоки кои се применуваат автоматски, таа бара донесување субјективни одлуки од оние што ја одредуваат класификацијата. За да се донесе правилна одлука за класификација, оној што ја класифицира информацијата (во понатамошниот текст создавачот), мора да исполнува одредени предуслови:

- Мора да има одлични познавања за областа на која се однесува информацијата. Создавачот се здобива со познавањата за областа на која се однесува информацијата преку формално образование, специјални обуки и работно искуство. Тој мора одлично да ја познава областа на која се однесува информацијата, и да може да ја претпостави потенцијалната штета што би настанала ако таа информација стане достапна во јавноста (како резултат на тоа

[121] Quist S, Arwin – „Security Classification of Information, Volume 2. Principles for Classification of Information“,Oak Ridge K-25 Site, Oak Ridge National Laboratory, Tennessee, 1993, p.68

што воопшто нема да се класифицира или ако се компромитира) и внимателно да размисли за својата одлука.;

- Мора да има поминато адекватни обуки и да ја познава материјата на која се однесуваат информациите. Создавачот мора детално да ги познава сите регулативи кои се однесуваат на класифицирани информации и да има посетувано специјализирани обуки и курсеви кои се однесуваат токму на оваа тематика.;
- Мора да ги разбира и да ги применува принципите за класификација. Најчесто, одлуките за класификација е многу тешко да се донесат. Потребни се објективни принципи кои ќе помогнат во донесувањето на одлуката. Постојните насоки за класифицирање мора да бидат експлицитно идентификувани, објаснети и формирани така што создавачот да знае дека тие постојат, да ги разбере комплетно, и да ги употребува со цел да донесе ефективна и конзистентна одлука за класифицирање. Од еднаква важност е овие принципи да имаат солидна основа и рамка, кои ќе овозможат класифицирање на информации само кога тоа е неопходно. Разбирањето и примената на принципите за класификација се стекнуваат преку работното искуство и самостојното усовршување на полето на класифицираните информации.

Освен овие предуслови кои се однесуваат на создавачот, потребно е да се земат предвид и некои други работи. Имено, мора да постои законска регулатива која ќе го уредува класифицирањето на информациите и која ќе нуди прецизни насоки кои ќе му бидат од помош на создавачот, и која ќе помогне во воспоставувањето на еден систем за класифицирање на информации кој ќе придонесе за унификација на класифицирањето и кој ќе се применува во сите институции кои создаваат класифицирани информации.[122] Системот за класификација на информациите треба да

---

[122] Законската регулатива која се однесува на заштитата на класифицираните информации во Република Македонија ја сочинуваат:

- Законот за класифицирани информации, кој е објавен во „Службен весник на Република Македонија“ број 9/04 од 27.02.2004 година, а влезе во сила на 05.03.2004 година.
- Уредбите за административна, физичка и безбедност на лица, објавени во „Службен весник на Република Македонија“ број 82/04 од 19.11.2004 година.
- Уредбите за информатичка и индустриска безбедност, објавени во „Службен весник на Република Македонија“ број 16/05 од 11.03.2005 година.
- Законот за изменување и дополнување на законот за класифицирани информации, кој е објавен во

биде еден од фундаменталните компоненти на процесот кој треба да обезбеди успешна заштита на информациите. Неговата цел е јасно да ги идентификува информациите кои мора да се заштитат заради нивната важност за националната безбедност, но и да ги идентификува информациите за кои не е потребна таква заштита. Овој систем ќе асистира во одредувањето на вредноста и чувствителноста на информациите, како и за безбедносните мерки кои треба да се преземат.

Во отсуство на воспоставен систем за класификација, постои ризик дека:

- сите информации може да се сметаат за класифицирани, при што трошоците за нивна заштита се пропорционално значително поголеми од нивната вредност и чувствителност;
- некои информации кои се многу вредни и чувствителни нема да бидат адекватно заштитени.

Кога сите предуслови ќе бидат исполнети и кога ќе се донесе одлука да се класифицира одредена информација треба да се пристапи кон нејзино обележување. Имплементацијата на конзистентни методи за класификација и обележување на информациите овозможува нивно безбедно користење. Создавачот на класифицираната информација на видно место на класифицираната информација го обележува називот на институцијата и ознаките за класификација. Ознаките за класификација мора да бидат унифицирани и поставени на таков начин што нема да има никаков сомнеж за класифицираната природа на информацијата и степенот на заштита кој треба да се обезбеди. Кога се врши класификацијата на информацијата, доколку е возможно, создавачот треба да одреди временски период за кој таа информација ќе биде класифицирана, и кој треба да биде одреден врз основа на проценатa за времетраењето на чувствителноста на информацијата. Ова носи со себе и одреден ризик, бидејќи доколку времетраењето на класификацијата се покаже како прекратко, со нејзиното предвремено објавување во јавност може да се уништат сите придобивки кои се постигнале со нејзиното класифицирање, и да дојде до настанување

„Службен весник на Република Македонија" број 113/07 од 20.09.2007 година, а влезе во сила на 29.09.2007 година.

Со донесувањето на овие прописи е заокружена законската и подзаконска регулатива во областа на заштитата на класифицираните информации во Република Македонија. Во сите наведени прописи се соодветно вградени стандардите и директивите на Европската унија и на НАТО и кореспондираат со современите решенија на прописите од оваа област во најголемиот број европски земји.

на првично одредената штета. Токму затоа, создавачот мора да биде внимателен при одредувањето на рокот за декласификација и да земе предвид многу фактори.

5.2. Одредување на степенот на класификација

Еден од најважните чекори за заштита на информациите е одредувањето на степенот на класификација. Кога ќе се одлучи дека една информација ќе се класифицира, треба да се донесе и одлука со кој степен ќе се класифицира. Степенот на класификација го определува создавачот на информацијата и треба да е соодветен на штетата која би настанала со неовластен пристап или употреба.[123] При утврдувањето на степенот на класификацијата се земаат предвид показатели кои поблиску укажуваат на степенот на евентуалната штета што би настанала со неовластен пристап до или со неовластена употреба на информацијата.

Степенот на класификација го означува релативното значење што го има таа информација во однос на националната безбедност и ги одредува специфичните безбедносни побарувања за нејзина заштита. Во принцип, информациите се заштитуваат пропорционално со нивната вредност и чувствителност. Сите мерки и активности кои се преземаат за да се заштити една информација се одредуваат врз основа на нејзиниот степен на класификација, кој го диктира изборот и имплементацијата на адекватните безбедносни мерки и активности.[124]

Треба да се има еден конзистентен и структуриран пристап во одредувањето на степенот на класификација, бидејќи секој степен поставува соодветни побарувања за административни, физички, персонални или информатички безбедносни мерки и активности кои треба да обезбедат соодветно ниво на заштита на информацијата. Степените на класификација се основните индикатори за вредноста на одредена информација и потребата од нејзина заштита. Степенот на класификација се утврдува во однос на ризиците кои може да се остварат, бидејќи тие ризици го одредуваат

---

[123] *„Закон за класифицирани информации“*, Службен весник на Република Македонија бр.9/04 од 27.02.2004 година.

[124] Информацијата која е одредена со степен на класификација нема да се смета за класифицирана информација ако со неа се прикрива кривично дело, пречекорување или злоупотреба на функцијата или некој друг незаконски акт или постапка. - *„Закон за класифицирани информации“*, Службен весник на Република Македонија бр.9/04 од 27.02.2004 година.

обемот на штетата која ќе настане доколку се наруши безбедноста на информацијата. Колку е поважна една информација за националната безбедност (колку е поголем степенот на штетата од нејзиното компромитирање), толку треба да биде повисок степенот на класификација на таа информација. Степенот на штетата и веројатноста од настанувањето на таа штета е важен елемент при одредувањето на степенот на класификација на информацијата. Исто така, во одредувањето на степенот на класификација на информацијата, одредена улога треба да има и дисеминацијата на таа информација. Веројатноста за неовластено објавување на една информација експоненцијално се зголемува со зголемувањето на бројот на лица кои имаат пристап до таа информација. На пример, нема да се смета за разумно ако се стави степен „ДРЖАВНА ТАЈНА“ на информација која ќе биде дисеминирана на 1 000 луѓе, бидејќи таквата екстензивна дисеминација ќе ја зголеми веројатноста за компромитирање на таа информација. Следствено на ова, дисеминацијата на одредена информација треба да се смета како значаен фактор при одредувањето на степенот на класификација на информацијата.

На крај, треба да се разгледа и ситуацијата во која создавачот не може да донесе цврста одлука за тоа кој степен на класификација да го употреби. Се чини дека најбезбедно решение за оваа несигурност е да се стави повисокиот степен од двата помеѓу кои е двоумењето, а доколку во наредниот период се појават нови фактори кои укажуваат дека таа информација е прекласифицирана, да се направи промена на степенот.

Степенот на класификација на информациите се врши според нивната содржина. Од круцијално значење е да се направи реална класификација, односно реално одредување на степенот на класификација. Одредувањето на превисок степен ќе има значителен ефект врз користењето и споделувањето на таа информација, и ќе бара скапи безбедносни мерки и активности за нејзина заштита. Одредувањето на пренизок степен ќе резултира со несоодветна заштита на информацијата и ќе го зголеми ризикот од компромитирање на таа информација.

Создавачот на класифицираната информација го означува на видно место степенот на нејзината класификација. Степенот на класификацијата се обележува на секоја страница и страниците се обележуваат со реден број од вкупниот број страници. Информацијата се определува со еден од степените на класификација:

- ДРЖАВНА ТАЈНА;

- СТРОГО ДОВЕРЛИВО;
- ДОВЕРЛИВО и
- ИНТЕРНО.

Со степен „ДРЖАВНА ТАЈНА" ќе се класифицираат само оние информации или материјали чие неовластено откривање или употреба би можело да им наштети на трајните интереси на државата. Неовластеното откривање или употреба на ваквите информации можат:

- директно да го загрозат уставниот поредок, независноста и територијалниот интегритет;
- директно да ја загрозат внатрешната стабилност;
- директно да доведат до масовни човечки губитоци;
- да причинат непоправливи штети на оперативната ефикасност или безбедност или на ефикасноста на исклучително вредни одбранбени безбедносни или разузнавачки операции или на операции преземени за справување со неконвенционални закани, особено со тероризмот;
- да причинат непоправливи штети на основните слободи и права на човекот и граѓанинот, демократијата и владеењето на правото;
- да причинат непоправливи штети на унапредувањето и развојот на економијата, на заштитата на сопственоста, слободата на пазарот и претприемништвото, хуманизмот, социјалната правда и солидарноста;
- да причинат непоправливи штети на заштитата и унапредувањето на животната средина;
- да нанесат тешки долготрајни последици на унапредувањето и развојот на локалната самоуправа;
- директно да го загрозат остварувањето на целите на меѓународната политика или да нанесат непоправливи штети на меѓународните односи или на односите со странска земја или меѓународна организација[125].

Класифицираната информација со степен „СТРОГО ДОВЕРЛИВО" е информација создадена од државните органи, органи на единиците на локална самоуправа и други институции која е од значење за јавната безбедност, одбраната, надворешните работи и безбедносните и разузнавачките активности на органите на

[125] *„Уредба за административна безбедност на класифицирани информации"*, Службен весник на Република Македонија бр.82/04 од 19.11.2004 година.

државната управа, а чие неовластено откривање би предизвикало исклучително сериозна штета за виталните интереси на државата. Со степен „СТРОГО ДОВЕРЛИВО" ќе се класифицираат само оние информации или материјали чие неовластено откривање или употреба би можело да им наштети на државните виталните интереси и тоа:

- да причинат исклучително сериозна штета на независноста и територијалниот интегритет;
- директно да го загрозат животот или исклучително сериозно да влијаат врз јавниот ред или врз личната безбедност или слобода на човекот и граѓанинот;
- да причинат исклучително сериозна штета на оперативната ефикасност или безбедност или на ефикасноста на исклучително вредни одбранбени безбедносни или разузнавачки операции или на операции преземени за справување со неконвенционални закани, особено со тероризмот;
- да причинат исклучително сериозна материјална штета на финансиските, монетарните, економските и стопанските интереси;
- да причинат исклучително сериозна штета на животната средина;
- да нанесат исклучително сериозни последици на унапредувањето и развојот на локалната самоуправа;
- исклучително сериозно да наштетат на остварувањето на целите на меѓународната политика или на меѓународните односи или на односите со странска земја или меѓународна организација;
- да предизвикаат притисоци на меѓународната заедница[126].

Класифицираната информација со степен „ДОВЕРЛИВО" е информација создадена од државните органи, органи на единиците на локална самоуправа и други институции која е од значење за јавната безбедност, одбраната, надворешните работи и безбедносните и разузнавачките активности на органите на државната управа, а чие неовластено откривање би предизвикало сериозна штета за важните интереси на државата. Со степен „ДОВЕРЛИВО" ќе се класифицираат само оние информации или материјали чие неовластено откривање или употреба би можело да им наштети на важните државни интереси, и тоа:

- да причинат сериозна штета на мирот, демократските основи на правната

[126] *„Уредба за административна безбедност на класифицирани информации"*, Службен весник на Република Македонија бр.82/04 од 19.11.2004 година.

држава и развојот на мултиетничко општество;

- да причинат сериозна штета за животот, здравјето, имотот и личната безбедност или слободата на човекот и граѓанинот;
- да причинат сериозна штета на оперативната ефикасност или безбедност или на ефикасноста на вредни одбранбени безбедносни или разузнавачки операции или на операции преземени за справување со неконвенционални закани, особено со тероризмот;
- да причинат сериозна штета или да се значително во спротивност со финансиските, монетарните, економските и стопанските интереси;
- да причинат сериозна штета на животната средина;
- да причинат сериозна штета на унапредувањето и развојот на локалната самоуправа;
- да причинат сериозна штета или да се значително во спротивност со политичко-одбранбената, економската и безбедносна интеграција во колективните системи за безбедност;
- сериозно да го спречува развојот или операциите утврдени во меѓународните договори кои се склучени со странски земји или меѓународни организации;
- сериозно материјално да им наштети на меѓународните односи, така што ќе предизвика формален протест или други санкции;
- да ги прекине или на друг начин значително да ги оневозможи значајните активности на меѓународен план или активностите на странска земја или меѓународна организација на планот на соработка[127].

Класифицираната информација со степен „ИНТЕРНО" е информација чие неовластено откривање би предизвикало штета за работењето на државните органи, единиците на локалната самоуправа и други институции кои се од значење за јавната безбедност, одбраната, надворешните работи и безбедносните и разузнавачките активности на органите на државната управа. Со степен „ИНТЕРНО" ќе се класифицираат само оние информации или материјали чие неовластено откривање или употреба би можело да им наштети на работата и ефикасноста на државните органите и тоа:

- да причинат штета или да влијаат врз условите за унапредувањето и

[127] *„Уредба за административна безбедност на класифицирани информации"*, Службен весник на Република Македонија бр.82/04 од 19.11.2004 година.

зачувувањето на внатрешно-политичката стабилност, безбедност и оперативната ефикасност;

- да причинат значително страдање на лица;
- да причинат штета на изградбата на праведна, социјална држава со еднакви можности за сите граѓани;
- да ги уназадат политичките, финансиските, монетарните, економските и комерцијалните преговори;
- да го спречуваат развојот или операциите утврдени во билатералните или мултилатералните договори кои се склучени со странски земји или меѓународни организации;
- да им причинат финансиска загуба или да им овозможат несоодветни достигнувања или предност на правните или физичките лица;
- да влијаат негативно на зачувувањето и заштитата на животната средина;
- да ги поткопуваат активностите на планот на зачувување и унапредување на мирот, стабилноста, безбедноста и сите форми на соработка со соседите, во регионот, Европа и светот, како и превенција и изградба на инструменти за рано предупредување на тензиите и кризите со цел за нивно навремено и ефикасно решавање по мирен пат;
- да ги поткопуваат активностите за зачувување и напредок на меѓународниот поредок заснован врз праведност, взаемно почитување на меѓународниот поредок втемелен во меѓународното право, како и политичка и економска рамноправност на државите;
- да влијаат негативно на меѓународните односи или на односите со странска земја или меѓународна организација[128].

Информациите кои не се наменети за јавна употреба, а со чие откривање би се намалила ефикасноста на работењето на државните органи, добиваат ознака „ЗА ОГРАНИЧЕНА УПОТРЕБА".[129]

Ако за поединечни страници, извадоци, додатоци, прилози и други придружни делови опфатени во една информација е потребен различен степен на класификација,

---

[128] *„Уредба за административна безбедност на класифицирани информации"*, Службен весник на Република Македонија бр.82/04 од 19.11.2004 година.

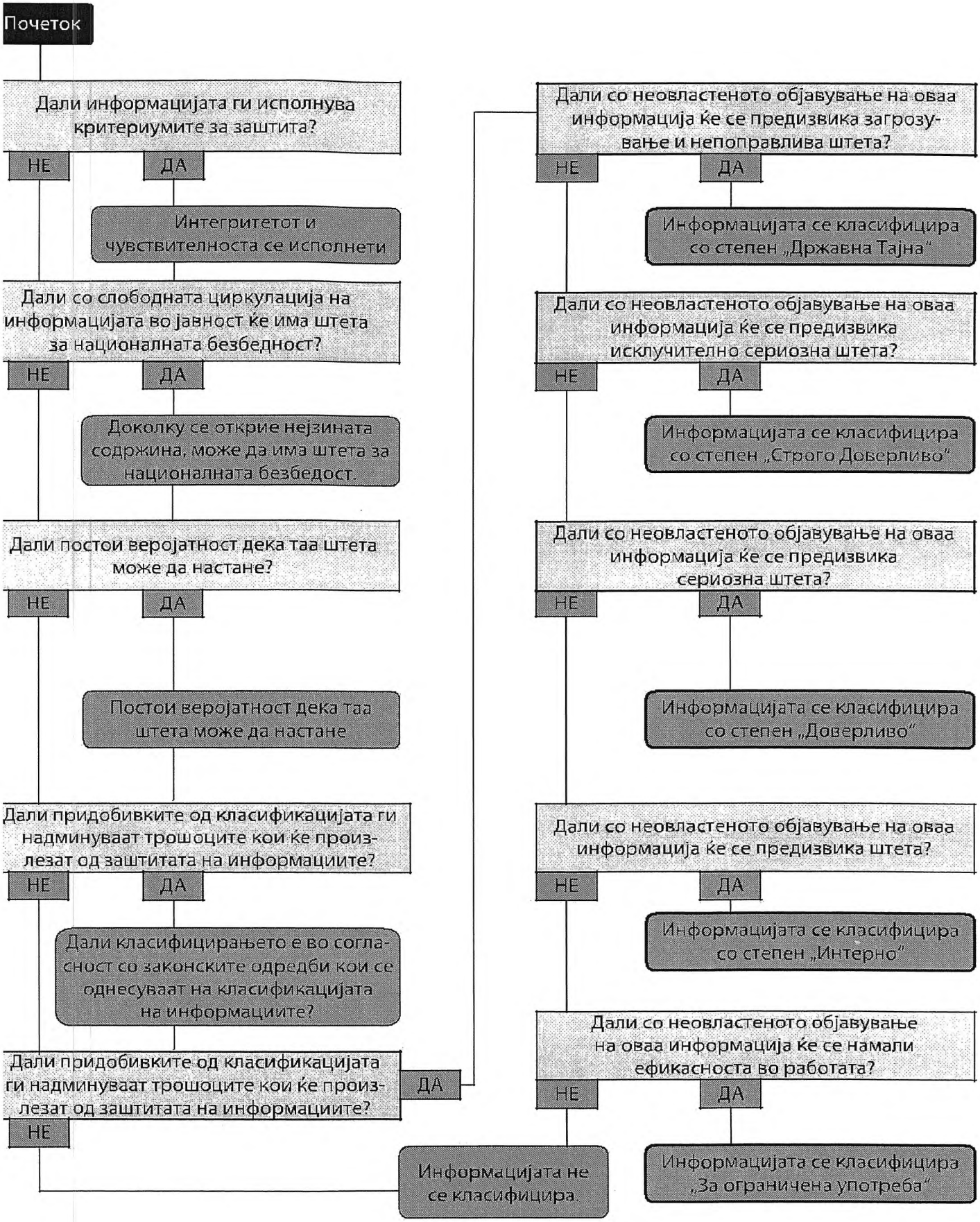
[129] *„Закон за класифицирани информации"*, Службен весник на Република Македонија бр.9/04 од 27.02.2004 година.

нивото на класификација на секој од нив посебно се определува од страна на создавачот и таа, како целина, ќе се класифицира според највисокиот степен на класификација што го носат споменатите делови што се опфатени во таа информација. Притоа, на насловната страна на материјалот се означуваат останатите делови со степени на класификација коишто припаѓаат кон информацијата. Кога има ваква ситуација, најчесто се настојува информацијата да биде составена така што почувствителните податоци би се разместиле како додаток на основниот документ со соодветен степен на класификација, со што основниот документ би можел и пошироко да се дистрибуира.

Доколку се укаже потреба за рекласификација на информацијата, односно потреба да се промени степенот на класификацијата, таквата промена ја врши создавачот, а со негова писмена согласност и друго овластено лице. За промената на степенот на класификација на информацијата задолжително се известуваат и корисниците на информацијата[130]. Рекласификацијата на информацијата може да се направи во две насоки, од понизок кон повисок степен, во случај кога се зголемила вредноста на таа информација и од повисок кон понизок, кога се намалила вредноста на таа информација, но не доволно за целосно да се тргне класификацијата.

Одредувањето соодветен степен на класификација и преземањето мерки и активноста за заштита на информацијата ги претставуваат основните препреки за потенцијалниот неовластен пристап и објавување на таа информација. Веднаш по одредувањето на степенот, мора да се започне со преземање на неопходните минимални стандарди за заштита на информацијата, чија функција е обезбедување на законско користење на класифицираните информации и оневозможување секаков вид незаконски пристап до нив.

[130] Корисник на класифицирана информација е правно или физичко лице кое има потреба за пристап до класифицирани информации заради извршување на функцијата, службените задачи или дејноста и кое има безбедносен сертификат. - *„Закон за класифицирани информации“*, Службен весник на Република Македонија бр.9/04 од 27.02.2004 година.



Дијаграм бр.7 – Класификација на информациите

5.3. Потребата за заштита на класифицираните информации

Во денешниов свет, заканите за безбедноста на информациите и информатичката технологија која се користи за ракување со нив и нивно чување се постојани. Заштитата на класифицираните информации е многу сложен предизвик, бидејќи заканите и ризиците за нивно компромитирање продолжуваат да се зголемуваат, и стануваат многу поконкретни и пософистицирани. [131] Во исто време, институциите со цел да ги остварат своите обврски се потпираат на користењето на најразлични информатичко-комуникациски уреди и компјутерски мрежи, а се зголемува и бројот на корисници на класифицирани информации. Комбинацијата од зголемени закани и побарувањата за што поголем пристап до класифицирани информации значително го зголемува ризикот од безбедносни нарушувања и компромитирања. Информациите мора да се заштитат од голем број закани кои доколку се манифестираат ќе резултираат со губење, неовластен пристап, неовластено објавување или промена на содржината на информациите. Заканите за кои зборуваме можат да се манифестираат преку ненамерни грешки и невнимателност на лицата кои ракуваат со нив, шпионски активности, неовластен упад во информатички систем и сл. Сите мерки и активности кои се преземаат за заштита на информациите имаат за цел да го заштитат интегритетот и чувствителноста на информациите.

Критериуми кои особено се земаат предвид при утврдувањето на мерките за заштита на класифицираните информации се: степенот на класификација, обемот и формата на класифицираната информација и проценета за закана на безбедноста на класифицираната информација. Има неколку принципи кои треба да бидат земени предвид при формулирањето на стратегијата за заштита на информациите. Институциите може да ги користат овие принципи при изборот, воспоставувањето и реализацијата на плановите и активностите, за да се обезбеди сеопфатност и ефикасност.

---

[131] Бидејќи во понатамошниот текст поимите ризик и закана за безбедноста на класифицираните информации екстензивно ќе се користат, потребно е да се направи нивно дефинирање и разграничување. Ризик е можноста дека ранливоста на кој било систем ќе биде експлоатирана од закана, односно можноста дека информациите, средствата, материјалните добра, комуникациите или информатичките системи ќе бидат злоупотребени или компромитирани.
Закана е потенцијална несреќа или намерно компромитирање на безбедноста, загуба на доверливоста или интегритет на класифицираната информација. Секој постоечки ризик претставува закана.

Тоа се следниве принципи:

- Одговорност. Одговорноста може да се разгледува на неколку нивоа. На институционално ниво, мора да се инсистира на одговорно ракување со класифицирани информации. Раководителите на институциите се одговорни за надзорот во поглед на заштитата на информациите и во поглед на почитувањето на правилата. Нивна обврска е да ги обучат своите вработени и кај нив да ја всадат одговорноста за почитување на воспоставените правила. Исто така, и сите корисници на класифицирани информации мора да се однесуваат одговорно при ракувањето со нив.;
- Адекватност. Преземањето на мерки и активности за заштита на информациите треба да биде соодветно со ризикот од нарушување на нивната безбедност. Степенот на заштита зависи од тоа колкава е веројатноста да се оствари одреден ризик, и колкав ефект ќе има тој ризик доколку се оствари. Треба да се земат во предвид веројатноста, фреквентноста и сериозноста на потенцијалните закани. Институциите треба да обезбедат соодветни ресурси (луѓе, време, опрема и буџет) за да може да се постигне и да се одржи задоволително ниво на безбедност на информациите.;
- Култура. Институциите мораат да бидат свесни и да ја разберат потребата за заштита на информациите. Сите вработени мора да бидат свесни за ризиците кои можат да ја нарушат безбедноста на информацијата и да ги познаваат процедурите и стратегиите за заштита на тие информации, соодветно на нивните работни места и одговорности. Исто така, потребно е да се обезбеди и обука на лицата на кои им се отстапуваат на користење одредени класифицирани информации.;
- Функционалност. Институциите треба во одредени временски интервали да направат реевалуација на постојните безбедносни мерки и активности, со цел да се одреди дали тие функционираат или не и дали ги даваат очекуваните резултати. Оваа постапка е многу корисна, бидејќи ќе овозможи свеж увид во моменталната ситуација, а ќе овозможи и ажурирање доколку за тоа се укаже потреба.;
- Издржливост. Ова се однесува на степенот до кој институциите можат да издржат во справувањето со заканите и да продолжат непречено да функционираат. Како пример, овде може да се посочат информатичките

системи кои содржат голем број информации кои треба да се заштитат, и кои постојано се под закана од неовластен упад. Издржливоста овде се гледа во способноста и покрај бројните закани, системот да продолжи да функционира нормално, или да се врати во функција колку што е можно побрзо по одреден напад;

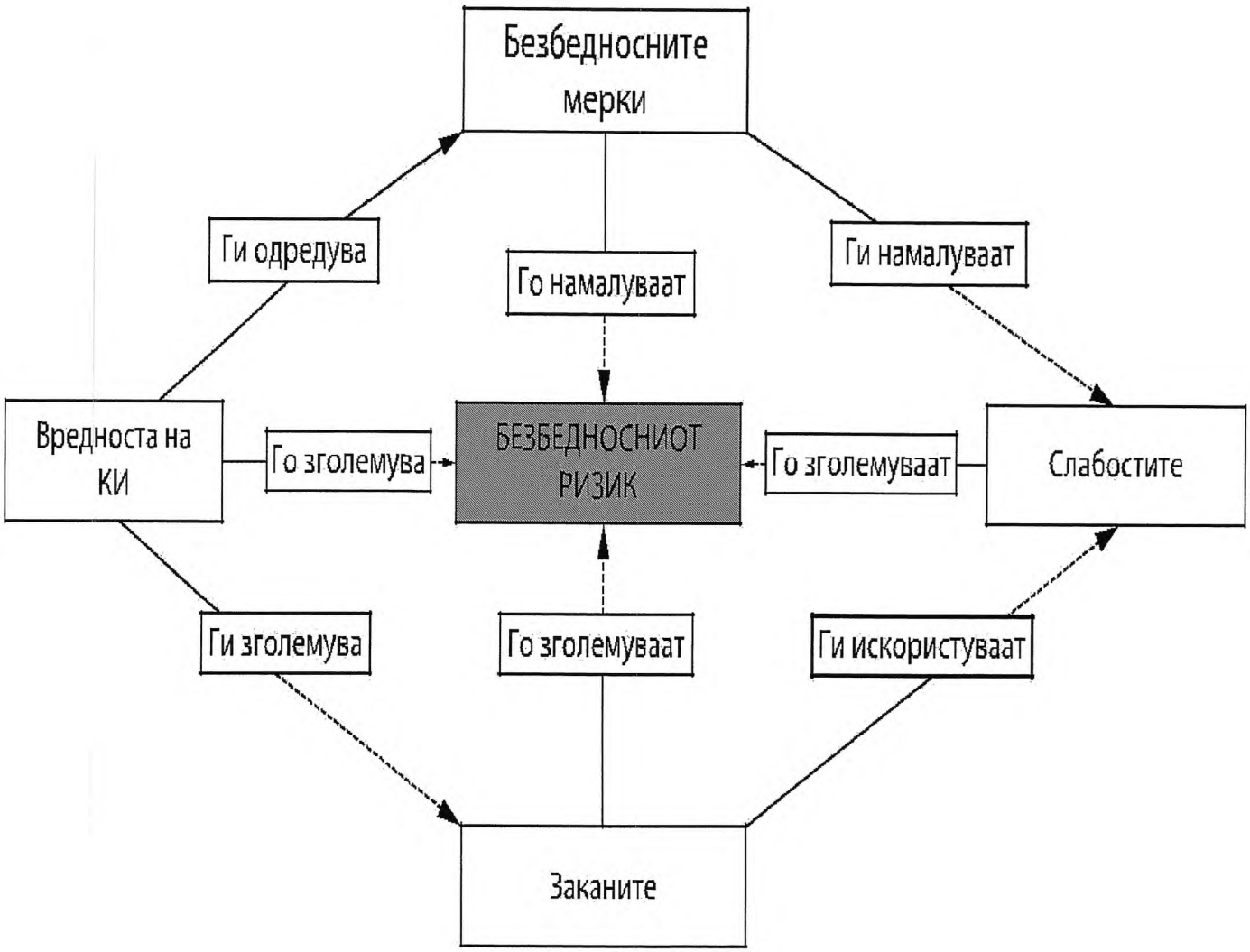
- Менаџирање со ризик. Институциите мора постојано да ги разгледуваат, да ги оценуваат и да ги модификуваат стратегиите за заштита на информациите како одговор на променливата природа на ризиците со кои се соочени. Тие треба да дојдат до решенија со кои ефективно ќе ги спречат заканите, како и да изработат планови како да ги заштитат своите најслаби точки. Притоа, секоја од институциите мора да ги земе предвид сопствените уникатни потреби, организационата култура, своите интереси и приоритети, како и своите буџетски ограничувања.

Се смета дека стратегијата е успешна, односно целта од примената на мерките и активностите за заштита на класифицираните информации е постигната ако:

- информацијата е достапна и употреблива кога ќе се појави потреба од неа;
- информацијата е заштитена соодветно со својот степен на класификација;
- пристап до информацијата имаат само оние лица што имаат соодветен безбедносен сертификат и го исполнуваат принципот „потребно е да знае“;
- информатичките системи кои се користат при ракувањето и чувањето на одредена информација се безбедни.

Како одговор на погоре споменатите побарувања, критериуми и предизвици, потребно е воспоставување на еден пристап кој ќе овозможи будност и ефективност во заштитата на информациите од неовластен пристап или објавување.

Заштитата на информациите бара мултидисциплинарен пристап, како и одредено искуство и вештина. Овој пристап инсистира на тоа дека веднаш откако ќе се одлучи дека една информација ќе се класифицира, треба да се почне со имплементацијата на безбедносните мерки и активности кои ќе ја заштитат таа информација. Овие безбедносни мерки и активности кои ги вклучуваат административната, физичката, персоналната и информатичката безбедност на класифицирани информации, носат со себе одредени организациони и финансиски побарувања.



Дијаграм бр.8 – Корелација на факторите кои влијаат врз безбедносниот ризик

5.4. Мерки и активности за административна безбедност на класифицирани информации

Административната безбедност на класифицираните информации вклучува неколку поврзани постапки, кои се одвиваат од првиот момент кога се донесува одлуката да се класифицира одредена информација, па сè до моментот на физичко уништување на таа информација или до моментот кога е донесена одлука за нејзина декласификација. Административната безбедност е составен дел на сиот животен век на класифицираната информација, затоа што ги вклучува скоро сите нејзини аспекти.

Во контекст на горекажаното, подолу се дадени мерки и активности за административна безбедност, кои дури можат да се подредат и хронолошки во однос на

својата интеракција со класифицираните информации, и кои вклучуваат:

- прием и евиденција на класифицираната информација;
- ракување со класифицираната информација и нејзино чување;
- изготвување копии, преводи и извадоци на класифицираната информација;
- остварување контрола врз распоредувањето и распространувањето на класифицираната информација;
- отстранување и уништување на класифицираната информација.

5.4.1. Прием и евиденција на класифицираната информација

Класифицираната информација се отстапува на користење по претходно добиена согласност за отстапување од создавачот. Кога ќе се добие одредена класифицирана информација потребно е да се пристапи кон нејзино евидентирање, со цел да се има контрола кога е добиена и од чија страна. Како и во секој сегмент од работата со класифицираните информации, и евиденцијата на класифицираните информации треба да биде усогласена помеѓу различните институции, со цел полесно следење на информацијата. Доколку при евиденцијата се користат деловодни книги, треба да се почитуваат донесените регулативи, според кои информациите класифицирани со степените „ДРЖАВНА ТАЈНА" и „СТРОГО ДОВЕРЛИВО" се евидентираат во еден деловодник, а информациите класифицирани со степените „ДОВЕРЛИВО" и „ИНТЕРНО" во друг деловодник. Во поново време, со развитокот на информатичката технологија, се овозможува и евиденцијата да се води електронски, преку користењето системи за автоматска обработка на податоци (АОП)[132].

Многу важен елемент кој треба да се запази при приемот и евиденцијата на класифицираните информации е тоа што тие ја задржуваат ознаката на создавачот и степенот на класификација.

---

[132] *„Уредба за административна безбедност на класифицирани информации"*, Службен весник на Република Македонија бр.82/04 од 19.11.2004 година.

5.4.2. Ракување со класифицираната информација и нејзино чување

Ракувањето со класифицираните информации мора да биде во согласност со воспоставените законски регулативи и работни практики. Имено, при ракувањето со нив мора да се внимава да не се загрози нивната безбедност, да се ракува со нив совесно и одговорно, да не се остават без надзор, да се ракува со нив во претходно определени административни и безбедносни зони, да се почитува принципот „потребно е да знае“ и по завршувањето на работата да се вратат на местата предвидени за тоа.

Кога станува збор за чувањето на класифицираните информации, треба да се напомене дека тие можат да се чуваат во печатена форма (на хартија, односно тврда копија) или во електронска форма (на компјутерски мемории за чување на податоци). Условите за чување (посебни зони, пристап, сефови и сл.) ќе бидат подетално обработени во делот кој ќе се однесува на физичката безбедност.

5.4.3. Изготвување на копии, преводи и извадоци на класифицираната информација

Копии, репродукции и преводи на класифицирани информации можат да бидат направени од страна на корисникот и под негов постојан надзор. Бројот на копиите, репродукциите и/или преводите се определува според принципот „потребно е да знае”. Безбедносните мерки кои се однесуваат на оригиналниот документ, се применуваат и на неговите копии, репродукции и/или преводи. Притоа, секоја копија се означува со посебен број (копирен број), а се евидентира и бројот на репродукциите и/или преводите, како и бројот на нивните копии[133].

По потреба, извадоци од поедини класифицирани документи можат да бидат вклучени во состав на други класифицирани документи. Извадокот од класифициран документ ја носи класификацијата на документот или делот од кој е издвоен, освен ако не е очигледно дека има друга класификација, и во тој случај се известува создавачот на оригиналниот или на повисокиот степен на класификација заради одредување на точната класификација на извадокот.

---

[133] *„Уредба за административна безбедност на класифицирани информации“*, Службен весник на Република Македонија бр.82/04 од 19.11.2004 година.

5.4.4. Остварување контрола врз распоредувањето и распространувањето на класифицираната информација

Класифицираните информации се распоредуваат на лица кои имаат безбедносен сертификат со степен за пристап до класифицирани информации најмалку еднаков со степенот на класификацијата на информацијата што им се доставува, согласно принципот „потребно е да знае". Почетната листа за распоредување на класифицираните информации до определени корисници се одредува од создавачот на информацијата.

Составен дел на распространувањето на класифицираните информации се и пакувањето и преносот на овие информации. Пакувањето на класифицираните материјали се врши на начин којшто оневозможува да се открие дека е во прашање материјал со соодветен степен на класификација. Класифицираните информации се пренесуваат спакувани во непросирна обвивка, ставена во дупли коверти, при што на надворешниот коверт не треба да се гледа класификација на информацијата што се доставува. Лицата кои кои се ангажирани за пренос на класифицираните информации (куририте) мора да имаат безбедносен сертификат со степен соодветен на степенот на класифицираните информации кои ги пренесуваат.

5.4.5. Отстранување и уништување на класифицирани информации

Класифицирани информации за кои ќе се утврди дека се непотребни за службена употреба, односно дека се вишок или се застарени или физички така оштетени што се неупотребливи, се уништуваат во согласност со листата на класифициран документарен материјал со рокови на негово чување[134].

Класифицираните информации кои се одредени за уништување треба да се уништат на начин кој ќе оневозможи нивна реконструкција и повторно користење. Методите и опремата кои најчесто се користат за уништување класифицирани информации вклучуваат: палење, сечење или хемиска декомпозиција.

За класифицираниот документарен материјал подготвен за уништување се

---

[134] *„Уредба за административна безбедност на класифицирани информации"*, Службен весник на Република Македонија бр.82/04 од 19.11.2004 година.

изготвува пописна листа која ги содржи сите релевантни податоци за целосна идентификација на класифицираната информација. За извршеното уништување се изготвува потврда која се чува заедно со пописниот лист за уништување. Потврдите за уништување и пописните листи за уништување треба да бидат составени така да овозможат правење процена за евентуално настанатата штета или за спроведување на безбедносна истрага при истекување или губење на класифицираните информации.

5.5. Мерки и активности за физичка безбедност на класифицирани информации

Како витален дел од процесот на заштита на информациите, физичката безбедност е фокусирана на одржувањето на физичките објекти и имплементацијата на мерки за контрола на пристап и спречување на неовластен пристап до класифицираните информации. Основните концепти кои ги користи физичката безбедност при заштитата на класифицираните информации се следниве:

- одвраќање – поставување и користење видливи безбедносни мерки кои ќе ги обесхрабрат и ќе ги одвратат лицата кои имаат намера да извршат неовластен пристап до класифицираните информации;
- отежнување и забавување – мерките за физичка безбедност треба да ги отежнат и да ги забават активностите на лицата кои имаат намера да извршат неовластен пристап, што ќе овозможи навремена реакција за спречување на пристапот;
- детектирање – да се забележат активностите кои укажуваат на неовластен пристап;
- известување – да се известат надлежните органи за неовластениот пристап;
- дејствување – преземање активности за спречување на неовластениот пристап;
- одбивање – справување со неовластениот пристап, односно негово оневозможување.

Почнувајќи од формирањето безбедносен појас и безбедносни зони, оценувањето на потребата за користење на чувари, па сè до организирање мерки и

активности за заштита од пожари, физичката безбедност опфаќа широк дијапазон на активности, кои вклучуваат:

- Изработка на процена за можно нарушување на безбедноста на класифицираната информација (процена за ризик).;
- Определување на безбедносен појас околу објектот во кој се ракува со класифицирани информации. Безбедносниот појас го претставува минималното растојание до објектот кое оневозможува, со примена на активни или пасивни средства, да се открие содржината на класифицираната информација.;
- Определување на безбедносни и административни зони.;
- Организирање на физичко обезбедување и примена на технички и други средства за обезбедување на објекти и простории во кои се наоѓаат класифицирани информации. Организацијата на физичката заштита, освен идентификација на локациите и објектите за кои е потребна заштита ги опфаќа следните повеќеслојни безбедносни мерки: безбедносна ограда, безбедносно осветлување, систем за откривање на недозволено физичко присуство на лица, интерен безбедносен систем за видео надзор, контрола на влез, движење и излез на лица и возила за пренос на класифицирани информации, контрола на посетители и одобрена опрема.;
- Контрола на пристап и издавање на дозвола за пристап во објекти и простории. Контролата на пристап се поставува во објект или објекти или во зони или простории во рамките на објектот. Контролата може да биде електронска, електро-механичка, со чувар или домар, или физичка.;
- Пренос на класифицирани информации надвор од безбедносните зони[135].

[135] *„Закон за класифицирани информации“*, Службен весник на Република Македонија бр.9/04 од 27.02.2004 година.

Дијаграм бр.9 - Корелација на основните концепти за физичка безбедност

5.5.1. Процена за можно нарушување на безбедноста на класифицираната информација

Проценатa за можното нарушување на безбедноста на класифицираните информации се врши од аспект на:

- бројност, степен, форма и проток на класифицираните информации;
- непосредната околина на објектот во кој се наоѓаат класифицирани информации и поставеноста на безбедносниот појас околу објектот; безбедносните и административните зони во објектот; физичката градба, ѕидовите, вратите и прозорците на објектот;
- состојбата на поширокатa околина на објектот;
- лицата кои работат во објектот;
- заканата од разузнавачки активности, саботажа, терористички или други криминални активности насочени кон класифицираните информации;
- постапките за работа со класифицираните информации и нивното чување во објектот[136].

[136] *Уредба за физичка безбедност на класифицирани информации*, „Службен весник на Република Македонија бр.82/04“ од 19.11.2004 година.

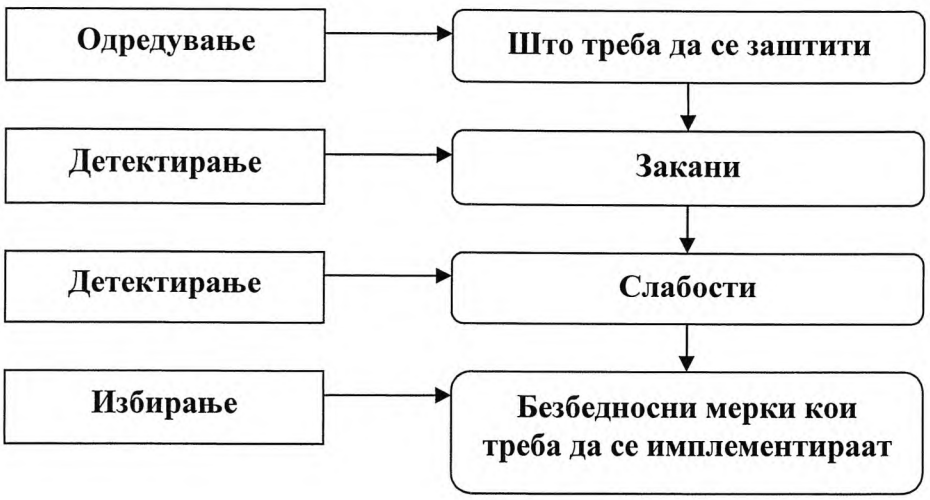
Оваа процена е инструментална за одредувањето на процедурите за идентификување и приоритизирање на заканите, како и за изборот на различните видови контролни механизми. Оваа процена треба да помогне во прецизната идентификација на ризиците и потенцијалните ефекти кои ќе ги има остварувањето на безбедносните ризици врз информациите, лицата и институциите кои се заштитуваат. Таа претставува развивање на ризикот за да се дојде до сознание колку тој во организацијата е значаен или не, и да се адресираат заканите и слабостите, со цел преземање превентивни мерки и активности. Пристапот кон изработка на проценатa ги содржи следниве фази:

- одредување на информациите, средствата и објектите кои треба да се заштитат;
- детектирање на безбедносните ризици и заканите за тие информации, средства и објекти;
- детектирање на слабостите кои можат да бидат искористени;
- развивање на ризиците со цел да се утврди дали нивното остварување е возможно;
- одредување дали со остварувањето на одреден ризик ќе се оствари штета;
- избор на безбедносни мерки кои ќе треба да се имплементираат.

Откако ќе се направи оваа процена, и ќе се одлучи дека некои ризици се едноставно неостварливи или дури и ако се остварат нема да имаат штетни ефекти, се пристапува кон следниот чекор, а тоа е менаџирањето со безбедносните ризици.

Менаџирањето на ризикот е постапка која опфаќа минимизирање на ризикот на прифатливо ниво и соодветна имплементација на безбедносни мерки и активности насочени кон целосно отстранувањето на тој ризик.

Менаџирањето треба да биде базирано врз проценатa за ризик која ги зема предвид сите остварливи закани и ранливости. Дури тогаш ќе биде возможно да се воспостават заштитни мерки за ефективно, ефикасно, практично и економично справување со идентификуваните ризици.



Дијаграм бр.10 - Постапки во проценатa за нарушување на безбедноста

Менаџирањето на ризиците ги содржи следните елементи:

- воспоставување на безбедносни мерки;
- прегледување и повторување на препорачаните контрамерки земајќи ги предвид минималните стандарди за превенција;
- елиминација на ризикот (тотална елиминација на вистинските или потенцијалните слабости преку имплементација на контрамерките);
- превенција на загуба (имплементација на контрамерките за да се спречи што е можно поголема загуба, имајќи предвид дека некои закани не можат да се елиминираат во оперативниот процес);
- ограничување на загубата (да се имплементираат контрамерките кои би ги намалиле загубите на задоволително ниво);
- прифатливост на загубите кои би настанале, а не би влијаеле врз функционалноста на системот;
- развивање на извештајот за управување на безбедносниот ризик што се состои од опис на контрамерки кои се имплементираат во работен план и опишувањето на „резидуалниот ризик"[137];

137 Резидуални ризици се ризици што остануваат по имплементирањето на безбедносните мерки во системот, имајќи предвид дека не е можно справување со сите закани и елиминирање или редуцирање на сите ранливости на системот.

- диригирање, насока и контрола на ресурсите (да се обезбеди и да се осигура дека ризикот е ставен во прифатливи граници).

5.5.2. Определување на административни и безбедносни зони

Една од активностите за физичка безбедност е и определувањето на административните и безбедносните зони во објектот во кој се ракува со класифицирани информации. Административна зона е простор или просторија во објектот во кои има или се чуваат класифицирани информации од степенот „ИНТЕРНО" и има потреба од соодветна физичка заштита. Безбедносна зона е простор или просторија во објектот во кои има или се чуваат класифицирани информации од степенот „ДОВЕРЛИВО" или повисок степен и има потреба од соодветна физичка заштита.[138] Во објектот се определуваат административни зони и безбедносни зони од прв и втор степен, кои мора да се обележат на видно место.

Административна зона се воспоставува околу или пред безбедносните зони од прв или втор степен. Оваа зона има јасно определен заштитен простор во којшто постојат можности за контрола на лица и возила. Во административните зони се ракува со информации класифицирани со степенот „ИНТЕРНО" како и со информации кои што се одредени „ЗА ОГРАНИЧЕНА УПОТРЕБА" .

Безбедносните зони во кои се ракува со информациите класифицирани со степен „ДОВЕРЛИВО" и повисоко можат да бидат од прв и втор степен, и треба да исполнуваат минимални безбедносни стандарди.

Безбедносните зони од прв степен треба да имаат:

- точно определен заштитен простор со строго контролиран влез и излез;
- систем на контрола, кој овозможува влегување само на лица со соодветна безбедносна проверка и кои се овластени за влегување во таа зона;
- спецификација на степенот на класификацијата и формата на информациите со кои се ракува во таа зона, односно информации до кои е дозволен пристап.

Безбедносните зони од втор степен треба да имаат:

- точно определен заштитен простор со строго контролиран влез и излез;

---

[138] *Закон за класифицирани информации*, „Службен весник на Република Македонија бр.9/04" од 27.02.2004 година.

– систем на контрола на влезот, којшто овозможува пристап само на лица, без придружба, кои се безбедносно проверени и овластени за влегување во таа зона, а за сите останати лица се обезбедува придружба или соодветна контрола за заштита на класифицираните информации и спречување на неконтролирано влегување во зоните што се предмет на техничка безбедносна контрола[139].

Степенот на физичкото обезбедување на просториите, информатичко-комуникациските уреди, уредите и средствата за умножување, обработување и чување на класифицирани информации треба да е соодветен на степенот на класифицијата на информацијата што тие уреди и средства ја содржат или за која се користат. Исто така, мора да има подготвено интерни планови за итно уништување или евакуација на класифицираните информации кои се чуваат во овие зони во случај на елементарни непогоди или насилен упад, со цел да се намали ризикот за нарушување на безбедноста на информациите. Деталноста на плановите, брзината на реакција и подготвеноста за дејствување во ваква ситуација зависи од карактеристиките на конкретниот ризик и веројатноста за остварување на ризикот.

Зоните заштитени од аудио прислушување се означуваат како технички обезбедени зони со посебно контролиран влез, и се заштитуваат од методи и средства за пасивно и активно прислушување, со преземање на мерки за физичка заштита на звукот и контрола на пристапот на местата каде постои таков ризик. За спречување на истекување на класифицирани информации преку жични микрофони, радио микрофони и други вградени средства се врши техничка и/или физичка безбедносна проверка на градбата на просторијата, нејзиното опремување и додатоците и канцелариската опрема вклучително и на канцелариските машини (механички или електрични) и средствата за комуникација. Мебелот или опремата, пред внесувањето во технички обезбедените зони, се проверува од соодветно обучени лица заради евентуално постоење на уреди за прислушување и притоа се запишува типот и серискиот број на инвентарот кој се внесува или изнесува од овие зони. Во технички обезбедените зони, по правило не се инсталираат телефони доколку тоа не е неопходно. Доколку телефонот е инсталиран, се опремува со дополнителен уред за прекинување на мрежата и напојувањето или со можност физички да се исклучи кога се зборува за класифицирани информации. Во технички обезбедени зони не се

---

[139] *Уредба за физичка безбедност на класифицирани информации*, „Службен весник на Република Македонија бр.82/04“ од 19.11.2004 година.

внесуваат мобилни телефони и други електронско-технички средства[140].

Физичката безбедност на класифицираните информации е многу важен сегмент од нивната заштита и мора да се работи интензивно во насока на целосно исполнување на стандардите за физичка безбедност.

5.6. Мерки и активности за персонална безбедност на класифицирани информации

Мерките и активностите кои се преземаат од доменот на персоналната безбедност за своја примарна цел имаат да обезбедат дека само лица кои се безбедносно проверени и за кои не постои сомневање дека можат да ја нарушат безбедноста на информациите до кои имаат пристап. За да се исполни оваа цел и за да се намали ризикот од неовластено објавување мора да се преземат сите разумни и соодветни активности, кои ќе осигураат дека само лица со соодветен безбедносен сертификат и кои го исполнуваат принципот „потребно е да знае“ имаат пристап до класифицирани информации.

Мерки и активности за персонална безбедност на класифицирани информации се:

- безбедносна проверка;
- издавање на безбедносен сертификат;
- брифирање на корисниците на класифицирани информации.[141]

---

[140] *„Уредба за физичка безбедност на класифицирани информации“*, Службен весник на Република Македонија бр.82/04 од 19.11.2004 година.

[141] *„Закон за класифицирани информации“*, Службен весник на Република Македонија бр.9/04 од 27.02.2004 година.

5.6.1. Безбедносна проверка

Исполнувањето на условите за издавање на безбедносен сертификат се утврдува преку безбедносна проверка. Таа се врши врз основа на претходна писмена согласност од лицето на кое треба да му се издаде безбедносниот сертификат.[142]

Безбедносната проверка започнува со пополнувањето на безбедносниот прашалник за соодветниот степен на безбедносна проверка.[143] Пополнетите податоци од безбедносниот прашалник претставуваат дел од содржината на безбедносната проверка.

Безбедносна проверка се презема пред издавање на безбедносен сертификат за пристап и користење на класифицирани информации, со цел да се утврди постоење или непостоење на околности или безбедносен ризик што го ограничуваат пристапот и користењето на класифицираните информации. При оценката за постоење на безбедносен ризик за лицето за кое се бара издавање на безбедносен сертификат, се проверува дали:

- сторило или се обидело да стори, самостојно или заедно со други лица, некое од кривичните дела содржани во Глава 28 од Кривичниот законик на Република Македонија;
- соработувало или сè уште соработува со разузнавачи, меѓународни терористи, саботери или лица за кои постои сомневање дека се во врска со странски разузнавачки служби или организации кои би можеле да ја загрозат безбедноста, освен во случаи кога е тоа во функција на службената должност на лицето;
- било или е член на организација или било или е приврзаник на организација која насилно, со субверзивни средства или на друг противзаконски начин дејствува против безбедноста на државата;
- намерно задржувало, погрешно интерпретирало или фалсификувало информации

---

[142] Ако лицето во текот на постапката писмено ја повлече својата согласност за проверка, повторна постапка за безбедносна проверка не може да се спроведе пред истекот на една година од денот на повлекувањето на согласноста. - *„Уредба за безбедност на лица корисници на класифицирани информации“*, Службен весник на Република Македонија бр.82/04 од 19.11.2004 година.

[143] За користење на класифицирани информации означени со степенот “ИНТЕРНО” не се врши безбедносна проверка. Физичкото лице се информира за обврската за заштита на класифицираните информации што му се дадени на увид, односно користење. - *„Закон за класифицирани информации“*, Службен весник на Република Македонија бр.9/04 од 27.02.2004 година.

од важност за безбедноста и одбраната на државата, или намерно дало неточни податоци во безбедносниот прашалник или при разговорот со овластени лица;
- има сериозни финансиски тешкотии или брзо се збогатило;
- постои зависност од алкохол, дрога и/или други психотропни супстанции;
- било или е инволвирано во активности кои можат да доведат до ризик за попуштање на лицето пред уцена или насилство;
- лицето преку постапки демонстрирало нечесност, нелојалност, недоверба или индискретност;
- се обидело или презело неовластени активности во однос на комуникациските и информатичките системи;
- боледувало или боледува од болести или ментални/емоционални состојби што можат да предизвикаат неправилности во проценувањето и да претставуваат ненамерен потенцијален ризик за безбедноста и
- е способно да го издржи притисокот на роднините или блиските соработници за оддавање на класифицирани информации на странски разузнувачки служби и организации, терористички групи или други слични организации или лица кои можат да ја загрозат безбедноста на државата.[144]

5.6.2. Издавање на безбедносен сертификат

За извршување на работните задачи, на лицата во државните органи, органите на единицата на локалната самоуправа, јавните претпријатија, јавните установи и служби, како и други правни и физички лица им се издава безбедносен сертификат за соодветен степен на класифицирана информација согласно со принципот „потребно е да знае".

Безбедносен сертификат се издава врз основа на претходно спроведена безбедносна проверка, и за соодветен степен на класифицирана информација.[145] За

---

[144] *Уредба за безбедност на лица корисници на класифицирани информации*, „Службен весник на Република Македонија бр.82/04" од 19.11.2004 година.

[145] Безбедносен сертификат за пристап и користење на класифицирани информации од сите степени, без претходна безбедносна проверка, заради вршење на функцијата од денот на изборот до крајот на мандатот, добиваат: претседателот на Република Македонија, претседателот на Собранието на Република Македонија, претседателот на Владата на Република Македонија, заменикот на претседателот на Владата на Република Македонија, претседателот на Уставниот суд на Република Македонија и

издавање на безбедносен сертификат за соодветен степен на класифицирани информации се поднесува писмено барање до Дирекцијата за безбедност на класифицирани информации.

Безбедносен сертификат се издава на физичко лице кое ги исполнува следните услови:

- да е државјанин на Република Македонија;
- да постои оправдана потреба за користење на класифицирани информации согласно со принципот „потребно е да знае“;
- да не постојат околности што го ограничуваат пристапот до класифицирани информации;
- физичкото лице да има деловна способност;
- лицето да наполнило 18 години, а за користење на класифицирани информации означени со степен „ДРЖАВНА ТАЈНА” да наполнило 21 година;
- да не му е изречена мерка на безбедност забрана за вршење на професија, дејност или должност;
- да е здравствено способно;
- да има потпишано писмена изјава дека совесно и одговорно ќе ги користи класифицираните информации;
- активностите на лицето да не укажуваат на постоење на безбедносен ризик за користење на класифицираните информации и
- да биде запознат со прописите кои се однесуваат на работата со класифицирани информации што се утврдува во разговор со кандидатот од страна на овластено лице пред издавањето на безбедносниот сертификат.[146]

Доколку се исполнети сите услови и е утврдено дека за лицето не постојат никакви индикации или сомневања кои би можеле да укажуваат на безбедносен ризик, му се издава безбедносен сертификат. Лицата на кои им е одобрен пристап до класифицирани информации, односно имаат добиено безбедносен сертификат, имаат одговорност за заштита на класифицираните информации со кои ракуваат и мораат да

претседателот на Врховниот суд на Република Македонија. - *Закон за класифицирани информации*, „Службен весник на Република Македонија бр.9/04“ од 27.02.2004 година.

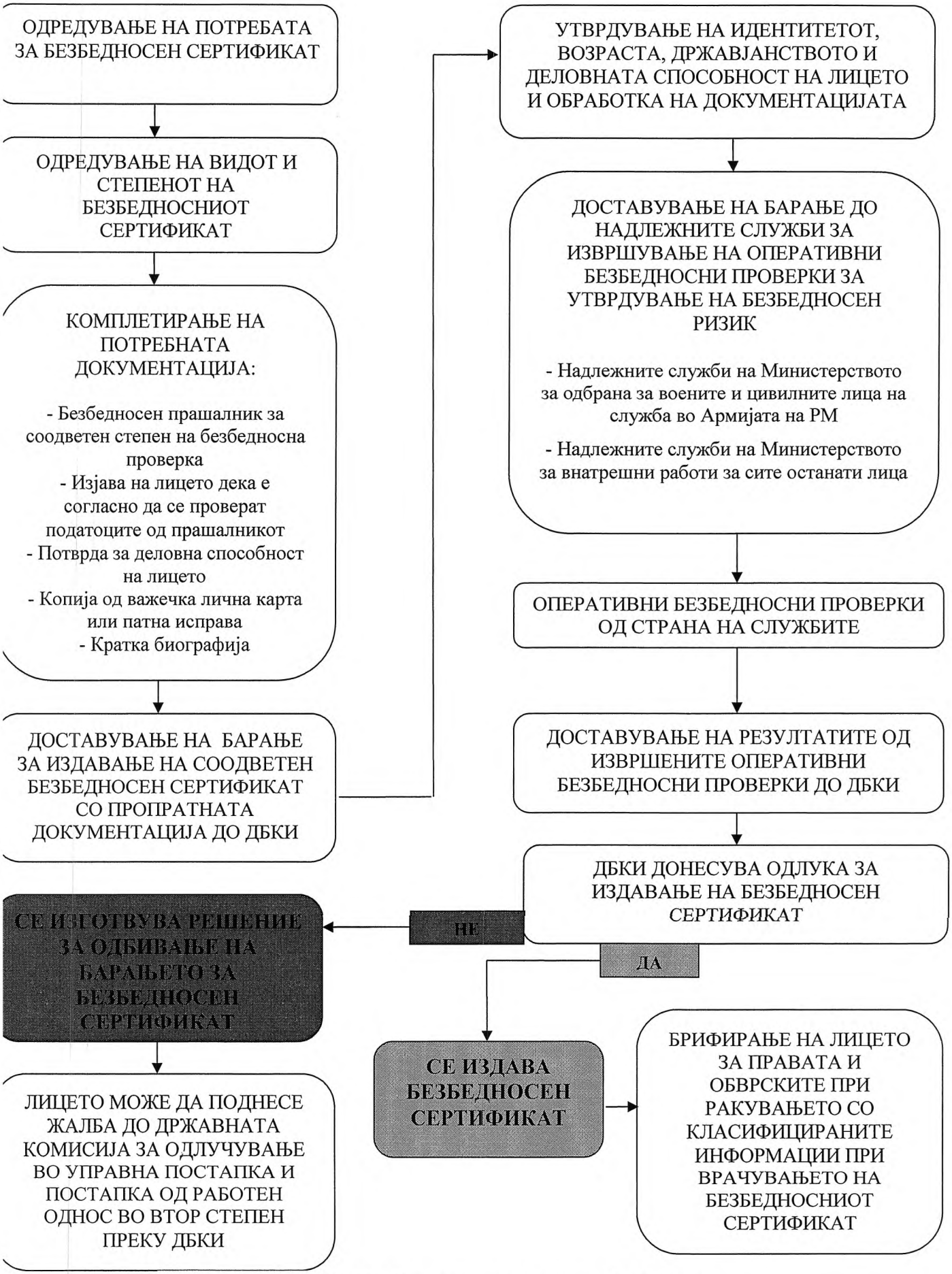
[146] *„Закон за класифицирани информации“*, Службен весник на Република Македонија бр.9/04 од 27.02.2004 година.

ги почитуваат мерките и активностите чија што задача е да го спречат нарушувањето на безбедноста на информациите. За таа цел, како неопходна активност во доменот на персоналната безбедност се прави запознавање на лицето за правата и обврските кои произлегуваат од ракувањето со класифицираните информации (за оваа постапка е прифатен терминот брифирање на лицето) при издавањето на безбедносниот сертификат, бидејќи сите лица кои ракуваат со информации кои се класифицирани потребно е да знаат зошто заштитата на овие информации е важна, кои мерки и активности се должни да ги преземат, како да ракуваат со информациите и како да ги чуваат. Исто така, на одредени периоди се прави и ребрифинг на лицето, со цел негово потсетување на обврските и потребата за одговорно ракување со класифицираните информации.

Потребно е да се разгледа и ситуацијата кога безбедносните проверки укажуваат дека за лицето постои безбедносен ризик и дека не треба да му се овозможи пристап до класифицирани информации. Во тој случај се донесува решение за одбивање на барањето за издавање на безбедносен сертификат, со тоа што во решението не се дава образложение за причините за одбивање[147].

Соодветно со степените на класификација, и безбедносните сертификати имаат степени и различно времетраење. Безбедносниот сертификат со кој се овозможува пристап до информации класифицирани со степените „ДРЖАВНА ТАЈНА" и „СТРОГО ДОВЕРЛИВО" важи пет години, а додека безбедносниот сертификат издаден за пристап до информации класифицирани со степен „ДОВЕРЛИВО" важи десет години. Меѓутоа, ако се утврди дека лицето не постапува со класифицираните информации согласно законските одредби или повеќе не е исполнет некој од условите врз основа на кои е издаден безбедносниот сертификат, се донесува решение за престанок на важење на безбедносниот сертификат и пред истекот на неговата важност.

[147] Против решението од став 1 на овој член лицето чие барање е одбиено може да поднесе жалба до надлежната второстепена комисија на Владата. - *Закон за класифицирани информации*, „Службен весник на Република Македонија бр.9/04" од 27.02.2004 година.



Дијаграм бр.11 - Постапки за издавање безбедносен сертификат

Во решението не се дава образложение за причините за престанокот на важноста на безбедносниот сертификат[148].

Освен кога безбедносниот сертификат му е одземен на лицето, неговата важноста престанува и во следниве ситуации:

- истекот на рокот на неговата важност;
- престанокот на потребата за пристап до класифицирани информации согласно со принципот „потребно е да знае“ и
- настапување на смрт на физичкото лице или престанок на постоење на правното лице.[149]

Обврската за заштита на тајноста на класифицираните информации продолжува и по истекот на важноста на безбедносниот сертификат, а пожелно и да се изврши дебрифинг на лицето, чијашто цел е да го потсети лицето на оваа обврска.

5.7. Мерки и активности за информатичка безбедност на класифицирани информации

Информатичката безбедност претставува примена на безбедносни мерки и активности за заштита на класифицираните информации кои се создаваат, чуваат или пренесуваат во комуникациски, информатички или други електронски системи од случајно или намерно губење на доверливоста, интегритетот или достапноста и превенција од губење на интегритетот и расположливоста на самите системи.

За постигнување на безбедносните цели за одржување на доверливоста, интегритет и достапноста на класифицираните информации се применува балансиран систем од безбедносни мерки и активности за создавање на безбедно опкружување во кое ќе работат комуникациските, информатичките и другите електронски системи. [150]

Генерално кажано, информатичката безбедност е составена од следниве компоненти: компјутерска безбедност, криптографска безбедност, емисиска

---

[148] *Закон за класифицирани информации*, „Службен весник на Република Македонија бр.9/04“ од 27.02.2004 година.

[149] *Ibid.*

[150] North Atlantic Treaty Organization (NATO) – *„C-M(2002)49 - Security Within The North Atlantic Treaty Organisation“*, NATO HQ Brussels, 2002

безбедност и комуникациска безбедност. За да се опфатат сите овие сегменти на информатичката безбедност, потребно е преземање на широк спектар на безбедносни мерки и активности кои ќе се користат во борбата против познатите и очекувани закани, но и за отстранувањето на слабостите и ранливостите кои се воочени.

Дијаграм бр.12 – Компоненти на информатичка безбедност

5.7.1. Компјутерска безбедност

Компјутерската безбедност на комуникациско-информатичките системи (КИС) во кои се процесираат класифицирани информации вклучува мерки и активности кои се насочени кон утврдување на методи и безбедносни процедури за прием, обработка, пренос, чување и архивирање на класифицирани информации во електронска форма.

Некои од нив се:

- идентификација на лицата кои пристапуваат во системот;
- контрола и евиденција на пристап до системот врз основа на дадено право за пристап од дефинирана база на податоци;
- поставување на програмски апликации во системот со кои ќе се оневозможи пристап на корисниците кои го изгубиле тоа право;
- идентификација на корисникот на отпечатениот, преснименият, модифицираниот или копираниот документ;
- сигурна евиденција на модифицирање, копирање, преснимување и бришење на класифицираните документи по корисници и
- заштита на важните технички и програмски елементи, системски можности и функционалност на системот[151].

Компјутерската безбедност ги опфаќа безбедноста на хардверот, безбедноста на софтверот, заштитата од компјутерски вируси и автоматизирано управување со безбедноста и анализирањето на безбедносни записи.

Безбедност на хардвер

Безбедноста на хардверот опфаќа постапки со кои се воспоставува контрола над хардверските елементи во кои се процесираат класифицирани информации. Притоа, задолжително се води евиденција за хардверот која треба да вклучува вид на комуникациско-информатичко средство, хардверски компоненти со сериски броеви и класификација на средството, а исто така и секоја овластена модификација се евидентира во евиденцијата. Безбедноста на хардверот се одржува преку донесувањето и почитувањето на следниве процедури:

- Процедури за заштита на хардвер од негово неовластено манипулирање. Куќиштата на сите комуникациско-информатички средства се запечатуваат со заштитни лепенки потврдени со своерачен потпис на администраторот на безбедност со цел да оневозможи неовластено менување на хардверските конфигурации;

[151] *Уредба за информатичка безбедност на класифицирани информации*, „Службен весник на Република Македонија бр.16/05“ од 11.03.2005 година.

- Процедури за одржување на хардверот, кои вклучуваат редовна контрола на неговата работа, исправност, функционалност и безбедност;
- Процедури кои треба да ги уредат постапките кои се преземаат во случај на дефект на хардверот. Во случај на дефект, хардверот се изолира од неговата мрежа и се исклучува од напојување. Потоа се повикува персонал за одржување и се врши откривање на дефектниот дел и негова замена со резервен дел.

Во делокругот на безбедноста на хардверот спаѓа и употребата на преносни комуникациско-информатички средства. Овие средства можат да се вклучат во КИС само ако се претходно сертифицирани за процесирање на класифицирани информации. Овде е важно да се напомене дека класифицирани информации со степен „ДРЖАВНА ТАЈНА" и „СТРОГО ДОВЕРЛИВО" не смее да се процесираат во преносни комуникациско-информатички средства. Преносните компјутерски средства и мемориски медиуми, кои се користат за процесирање на класифицирани информации, се сметаат како документи кои содржат класифицирани информации.[152]

Безбедност на софтвер

Безбедноста на софтверот претставува воспоставување контрола над инсталациите на оперативниот и апликативниот софтвер кој го користат уредите низ кои се процесираат класифицирани информации. Безбедноста на софтверот ги вклучува механизмите за контрола на пристап, согласно принципот „потребно е да знае". Механизмите кои се користат за остварување контрола на пристап се идентификацијата и автентификацијата на корисниците на КИС. Идентификација на корисниците на КИС се остварува преку креирањето на посебен кориснички акаунт за секој корисник на КИС, и овој акаунт треба да го содржи името и лозинката на корисникот. Автентификација на корисникот се прави со помош на лозинка, која треба да ја познава само корисникот и која треба да обезбеди дека никој друг нема да може да оствари пристап до неговите материјали.

Пред да се процесираат класифицираните информации на одреден КИС, се врши детална контрола на оперативниот систем во однос на присуство на малициозен

---

[152] *„Уредба за информатичка безбедност на класифицирани информации"*, Службен весник на Република Македонија бр.16/05 од 11.03.2005 година.

софтвер. Откако корисникот ќе се увери дека е безбедно, започнува со процесирање на класифицирани информации. Исто така, по завршувањето со процесирање на класифицирани информации, корисникот уште еднаш врши контрола на безбедноста на оперативниот систем и класифицираните информации кои ги процесирал.

Заштита од компјутерски вируси

Корисникот на КИС е должен пред започнување и по завршување на процесирање со класифицирани информации во КИС, да изврши детална контрола на целокупниот софтвер од аспект на присуство на компјутерски вируси и друг штетен софтвер. Во случај да се детектира одреден штетен софтвер, корисникот е должен да го извести администраторот на системот, кој врши откривање и отстранување на штетниот софтвер.

Заштитата се остварува со преземањето на неколку постапки, како на пример инсталација и редовна надградба на софтвери за заштита, проверка на присуство на компјутерски вируси и друг штетен софтвер во оперативни системи и други програмски пакети и нивно отстранување и проверка на присуство на штетен софтвер во компјутерски преносни мемориски медиуми. Сите софтверски апликации, информации и податоци добиени на преносни мемориски медиуми или по пат на електронска размена пред обработка треба да се проверат за присуство на компјутерски вируси и друг штетен софтвер.

Автоматизирано управување со безбедноста и анализирање на безбедносните записи

Анализа и контрола на безбедносните записи се врши за да се овозможи поголема контрола врз функционирањето на комуникациско-информатичкиот систем. Секој настан мора да биде безбедносно запишан со следниве податоци: вид на настан, информација која се однесува на настанот, време на настанот, локација на настанот во КИС. Мерки и активности кои се преземаат во оваа насока се:

- континуиран запис на состојбата на системот, поврзано со безбедноста на системот (безбедносни записи), активноста на системот, измени на параметри и слично;
- навремена реакција на безбедносен инцидент;

- проверки на безбедносните записи;
- одредување период на чување на безбедносните записи;
- постапување по процедури во случај на дефект на системот за анализа на безбедносните записи. Во случај на дефект на системот за анализа на безбедносните записи, потребно е да се врши откривање на дефектот, санирање на системот за анализа на безбедносни записи, согледување на настанатата штета и пишување на вонреден извештај за настанатите последици и преземените мерки.

5.7.2. Комуникациска безбедност

Комуникациската безбедност претставува збир на мерки и активности со кои се заштитуваат електронски пренесувани класифицирани информации од инфилтрирање, неовластен пристап или пресретнување од страна на лица, уреди или апликации. Мерките и активностите за комуникациска безбедност се одговорни за безбедноста на информациите кога тие се движат низ комуникациски медиуми и се дизајнирани да ги заштитат комуникациите од пресретнување и неовластен пристап во текот на нивната електронска трансмисија. Комуникациите во оваа смисла се дефинирани како секоја трансмисија и прием на знаци, сигнали, зборови, слики и звуци кои се остваруваат преку жична врска, радио врска, оптичка врска и други електромагнетни системи.[153] Тие може да бидат компромитирани со директно пресретнување, индукција или специјални ефекти на зрачења.

5.7.3. Криптографска безбедност

Криптографската безбедност е фокусирана на криптографската заштита на комуникациските, информациските и другите електронски системи преку кои се подготвуваат, пренесуваат, обработуваат и архивираат класифицирани информации. Таа

[153] The Combined Communications Electronics Board (CCEB) – „ACP 122(E), Information Assurance For Allied Communications And Information Systems", 2004. p.35

го вклучува дизајнот, имплементацијата, заштитата и употребата на криптографски системи и опрема за криптирање. Системите за криптозаштита мора да се заштитат и од компромитирачко електромагнетно зрачење и да ги исполнат условите за компјутерска и комуникациска безбедност.

Криптографската безбедност опфаќа пропишани мерки и постапки со кои се обезбедува заштита на работните места, содржините и методите на работа, системите за криптозаштита, како и управување со криптографски клучеви. Класифицираните информации со степен „ИНТЕРНО“ и повисоко, при пренос преку КИС надвор од контролираниот простор се штитат со одобрени криптографски методи и средства. Со системите за криптозаштита на класифицирани информации се обезбедува:

- сигурна и заштитена идентификација на корисниците;
- продукција на крипто клучеви;
- потврда на автентичноста на испраќачот и примачот на информацијата кои треба да се извршат пред почнување на пренос на информацијата;
- доверливост, интегритет и достапност на информацијата и
- потврда за прием на информацијата[154].

5.7.4. Емисиска безбедност

Емисиската безбедност го вклучува преземањето на мерки и активности кои треба да спречат неовластен пристап до информациите преку пресретнувањето и анализата на електромагнетни зрачења од КИС во кои се процесираат класифицирани информации.[155]

Сите електронски, електро-оптички или електромеханички уреди, независно од тоа дали се дизајнирани како трансмитери, при својата работа произведуваат електромагнети сигнали, кои се нарекуваат емисии. Кога се во прашање уреди низ кои се процесираат класифицирани информации, овие емисии претставува безбедносен

---

[154] *Уредба за информатичка безбедност на класифицирани информации*, „Службен весник на Република Македонија бр.16/05“ од 11.03.2005 година.

[155] The Combined Communications Electronics Board (CCEB) – „ACP 122(E), Information Assurance For Allied Communications And Information Systems”, 2004. p.38

ризик, на кој мора да му се посвети големо внимание, со цел да се минимизира или комплетно отстрани[156].

Електромагнетните емисии може да се манифестираат преку пропуштање на сигнали кои зрачат од КИС преку видните површини, преку зрачење на сигнали од инсталациските линии на уредите во кои се процесираат класифицирани информации и истекување на класифицирани информации преку инсталациите во просториите.

Нарушување на функционирањето на КИС со електромагнетна емисија може да настане случајно или намерно. Случајно загрозување може да настане со електромагнетна интерференција од внатрешно или надворешно средство, како на пример радар, радио антена, станица за генерирање електрицитет. Намерно загрозување на КИС со зрачење може да настане од човечки фактор кој може да врши насочено зрачење за да ги попречи или преоптовари комуникациите, или да го загрози оперирањето на некој уред. Пример за ова е дисторзија на сигналот на катодната цевка од мониторот, со што се нарушува процесирањето на информациите.

Мерките и активностите за емисиска безбедност се одредуваат со цел да се заштитат КИС и криптографската опрема.[157] Потребно е тие да се имплементираат со цел да го спречат компромитирањето на класифицираните информации преку електромагнетната емисија и да бидат пропорционални со ризикот за нарушување на безбедноста на информациите и нивниот степен на класификација.

Постојат три метода кои се користат за намалување на ризикот од емисијата:

- Емисиите се филтрирани или блокирани со помош на заштитни материјали, најчесто метални површини. Оваа техника може да се употреби за заштита на една просторија, група на простории или цел објект.;
- Компјутерите и другите медиуми во кои се процесираат класифицирани информации се опремени со специјални уреди и технологија, која значајно ја намалува емисијата. Технологијата која е наменета за мониторинг и заштита на

---

[156] Доколку овие емисии се пресретнат и обработат со помош на специјализирани уреди, голема е веројатноста дека ќе се открие нивната содржина. На пример, со помош на специјализирани антени или рисивери, можно е да се прифатат емисии од незаштитени електронски уреди оддалечени до 200-300 метри. Квалитетот на пресретнатата емисија ќе зависи од сигналот, далечината, конструкцијата на објектот во кој е сместен уредот кој зрачи и чувствителноста на рисиверот, но сепак ваквата ситуација претставува очигледен ризик за нарушувањето на безбедноста на класифицираните информации кои се процесираат.

[157] Air Force Manual 33-214, Volume 2 - „Communications and Information - Emission Security Countermeasures Reviews", 2011, p.9

уредите кои оддаваат електромагнетни емисии се нарекува ТЕМПЕСТ, и се користи за лимитирање на електромагнетната емисија од електронските уреди (компјутери, принтери, скенери и сл.) низ воздухот и низ сите средства кои имаат кондукторски особини (електрична инсталација, водоводни цевки и сл.).; [158]

- Емисиите можат да бидат значително намалени преку планското поставување и физичката сепарација на електронската опрема и напојувањето. Ова е познато како концепт на ЦРВЕНА/ЦРНА сепарација. Уредите низ кои се процесираат класифицирани информации се сместени во црвената зона, а оние кои служат за работа со некласифицирани информации се наоѓаат во црната зона. Овие зони треба да бидат физички раздвоени една од друга.[159]

5.7.5. Процена за нарушување на безбедноста на комуникациско-информатичките системи

Како резултат на постојаните технолошки достигнувања и развивања во областа на информатичката технологија, се зголемува и појавата на нови безбедносни закани и ризици. Со цел да се зголеми безбедноста на класифицираните информации кои се процесираат во КИС, се врши процена на безбедносен ризик на сите комуникациско-информатички системи.

Проценатa на ризикот претставува процес за определување на безбедносните ризици, т.е. заканите и ранливоста на КИС, утврдување на нивната големина и идентификување на областите каде што е потребна заштита или примена на мерки за заштита. Таа служи за определување на постојните ризици, определување на тековната безбедносна поставеност на КИС во однос на процесирање на информациите и за прибирање информации кои се неопходни за селекција на ефективни безбедносни

[158] Овој термин е прифатен во САД во 60тите години на минатиот век и претставува акроним за кој што има две толкувања. Првото толкување, кое е пошироко прифатено, е дека акронимот е формиран од фразата Telecommunications Electronics Material Protected from Emanating Spurious Transmissions. Некои други извори тврдат дека акронимот всушност води потекло од Transient Electromagnetic Pulse Emanation STandard. – SANS Institute IFOSEC Reading Room - *„An introduction to TEMPEST"*, SANS Institute, 2014, p.2

[159] Air Force Manual 33-214, Volume 2 - *„Communications and Information - Emission Security Countermeasures Reviews"*, 2011, p.38

мерки за заштита. Проценатa на ризикот придонесува кон одлуката за тоа какви мерки за заштита ќе бидат потребни и како може да се постигне соодносот помеѓу техничките и другите мерки за заштита на КИС и дава непристрасна процена на резидуалниот ризик. Користа што произлегува од проценатa на ризикот е зголемена свесност за безбедност која ќе биде очигледна на сите организациски нивоа, почнувајќи од управувачкиот тим па до оперативниот и помошниот персонал.

Заканите по безбедноста на КИС ја претставуваат можноста за случајно или намерно компромитирање на безбедноста на КИС. Заканите за КИС можат да бидат:

- случајни: грешки на опремата, кориснички грешки, софтверски грешки, прекин на електрична енергија и невнимателно ракување;
- намерни: инфилтрирани агенти, техничко прислушување, електромагнетно прислушување, компјутерски криминал, кражби;
- природни: поплави, електрично празнење-гром, пожари, земјотреси и други катастрофи.

Слабостите на безбедноста на КИС можат да овозможат или да потпомогнат во реализацијата на одредена закана. Тие може да бидат:

- погрешно или неавторизирано користење на КИС;
- неконтролиран пристап до КИС;
- неефективни процедурални безбедносни мерки;
- слабости или недостатоци во оперативниот или апликативниот софтвер;
- хардверски грешки;
- грешки во комуникацискиот систем.

Потребно е да се размислува во насока на детектирање на слабостите и пронаоѓање решенија за нив. Менаџирањето на слабостите е постапка која се користи за воочување на техничките и оперативните слабости на техничката инфраструктура каде што се наоѓаат класифицирани информации, и пронаоѓањето решенија како најефикасно да се отстранат тие слабости. Ова треба да биде една проактивна и превентивна набљудувачка активност, со чија помош се испитуваат системите и мрежите за можните технички грешки и слабости, а добиените сознанија се анализираат и приоритизираат и се предложуваат решенија за нив.

Проценатa на ризикот не е задача што се остварува еднаш засекогаш. Таа се изведува периодично, согласно потребите на процесот на безбедносна акредитација, со цел да се биде во тек со промените на заканите и степенот на ранливост, како и со

промените во мисијата на организацијата, нејзините информации, објекти и опрема. Неможноста соодветно и навремено да се согледаат факторите за безбедносниот ризик може да резултира со неефективни и непотребно скапи безбедносни мерки.

5.7.6. Акредитација на комуникациско-информатичките системи и процеси

Акредитација претставува безбедносна авторизација или одобрување на КИС за работа со класифицирани информации. Примарна цел на безбедносната акредитација е да се утврди дали во имплементираниот КИС е постигнато соодветно ниво на заштита на класифицираните информации, како и дека тоа континуирано се одржува во текот на животниот циклус на КИС. Со оваа постапка се:

- потврдува дали соодветно се имплементирани планираните мерки за безбедност на системот, специфицирани во изјавата за безбедносни потреби;
- потврдува дали се имплементирани мерките за безбедност и дека е постигнато бараното ниво на безбедност;
- утврдува нивото за безбедност преку соодветно тестирање;
- документираат резултатите од верификацијата на имплементацијата на безбедноста на системот.[160]

5.8. Мерки и активности кои се преземаат при настанато нарушување на безбедноста на информациите

Нарушувањето на безбедноста на класифицираните информации настанува кога до информацијата е остварен пристап од лице кое нема овластување да ја добие таа информација. Во ваков случај, најчесто лицето нема безбедносен сертификат или не го исполнува принципот „потребно е да знае“. Задолжително е секое нарушување (или основано сомнение за нарушување) на безбедноста на информациите да се пријави и да се истражи колку што е можно побрзо, со цел да се одреди потенцијалната штета од тоа нарушување и да се одредат корективните и дисциплинските мерки кои треба да се

[160] *Уредба за информатичка безбедност на класифицирани информации*, „Службен весник на Република Македонија бр.16/05“ од 11.03.2005 година.

преземат. За нарушување на безбедноста едновремено се известува и создавачот на класифицираната информација.[161] Во првиот извештај за нарушување на безбедноста на класифицираната информација се даваат податоци за:

- видот и формата на информацијата, степенот на нејзината класификација, називот на органот што ја создал информацијата, деловодниот број и датум, ознаката и бројот на копијата, темата на која се однесува и делокругот;
- кус опис на околностите под кои настанало нарушување на безбедноста, датумот на нарушувањето на безбедноста, периодот во кој што информацијата била изложена на откривање и, ако е познато, бројот и/или категоријата на неовластените лица кои имале или можеле да имаат пристап до класифицираната информација;
- дали создавачот е информиран за нарушувањето на безбедноста.[162]

По известувањето, се одлучува за потребата од преземање дејства за утврдување на степенот на нарушување на безбедноста на класифицираната информација. Утврдување на степенот на нарушување на безбедноста на класифицираната информација треба да се спроведува од страна на експерти со професионално безбедносно и истражно искуство, кои се независни од лицата непосредно поврзани со настанатото нарушување на безбедноста на класифицираните информации. Потребно е да се земе предвид степенот на штетата која настанала како последица на неовластеното објавување и дали има компромитирање на некои чувствителни аспекти од класифицирани проекти, извори на податоци или методи за прибирање на податоци, обемот на циркулација на неовластено објавените информации и бројот на лица кои имале пристап до нив и дали истрагата за нарушувањето на безбедноста на информацијата ќе направи дополнителна штета.

Кога ќе се заврши оваа постапка, се прави процена на штетата и се одлучува дали ќе се преземат дополнителни активности за елиминирање на негативните последици од нарушувањето на безбедноста на класифицираните информации.

---

[161] Известувањето на создавачот на класифицираната информација за нејзино неовластено изнесување, објавување и нарушување на безбедноста е целисходно заради овозможување на процена на настанатата штета од негова страна и за преземање на потребни или вообичаени активности за намалување на ефектите од штетата.

[162] *Уредба за административна безбедност на класифицирани информации*, „Службен весник на Република Македонија бр.82/04“ од 19.11.2004 година.

Глава 6

Информациите и информирањето како услов за ефикасно планирање во безбедносниот сектор на Република Македонија

6.1. Информациите и информирањето во безбедносниот сектор на Република Македонија

Последните две децении ги одбележаа радикални и разни промени на глобалниот безбедносен амбиент. Во текот на овој период беа зачнати длабински промени кои сега веќе имаат пресудно влијание врз економската, социјалната, политичката и безбедносната конфигурација на светската заедница, а веќе се чувствуваат и првите последици од тие промени. Помеѓу останатото, изменета и проширена е и листата на безбедносни предизвици, ризици и закани, а паралелно со ова, се менува и нивната природа, содржина, појавните облици и нивниот досег.[163] На сцена стапија и некои нови носители на загрозување на индивидуалната, регионалната и глобалната безбедност, носители на кои не може да остане имуна ниту една држава во светот, вклучувајќи ја и Република Македонија[164]. Во оваа нова безбедносна средина, државните институции треба да одговорат адекватно на променетата природа на внатрешните и на надворешните извори на закани, ризици и предизвици. Промените во светот и зголемувањето на бројот, на содржината и на различноста на безбедносните ризици и закани ја условија потребата за редефинирање на безбедносната политика на земјите од Југоисточна Европа, но наметнаа и усвојување на нови пристапи за дефинирање на националната безбедност. Република Македонија мора да се приспособи на новите околности во регионот и на непосредното опкружување заради заштита на националните стратегиски интереси и воспоставување ефикасни безбедносни институции.[165]

За да можат безбедносните институции како единки и безбедносниот сектор како целина да ја извршуваат својата задача на најдобриот можен начин, потребни им се одредени информации и сознанија врз кои ќе ги темелат своите одлуки и ќе ги насочуваат своите активности. Информациите и информирањето, кои треба да се

---

[163] Hadžić Miroslav & Švarm Filip - *„Priručnik sa pojmovnikom za novinare - bezbednosna pitanja"*, Beograd, 2005, p. 7

[164] Глобалната безбедност претставува безбедност, детерминирана од глобалните интереси и глобалните закани, која ја опфаќа индивидуалната, националната и регионалната безбедност помеѓу кои постои идеалполитичка и/или реалполитичка врска помеѓу секторите (политичко-правен, воен, економски, социјален и еколошки), чија суштина е меѓусебно корегирање, контролирање и моделирање со цел постигнување на мирот и безбедноста на планетата и луѓето. – Котовчевски, Митко – *„Национална безбедност на Република Македонија"*, прв дел, Скопје, 2000, стр.45

[165] Бакрески, Оливер и Милошевиќ, Милан - *„Современи безбедносни системи"*, Скопје, 2010, стр.9

вклучат како незаменлив дел во процесот на донесување одлуки, може многу да им помогнат на донесувачите на одлуки во Република Македонија при нивното одлучување како да се разреши одредена чувствителна ситуација. Навремената и точна информација претставува силен адут при донесувањето на одлуките и изборот на наредните активности – колку е поквалитетна и посодржајна информацијата, толку подобра ќе биде одлуката која се базира на неа. Со цел да се заштитат интересите и вредностите на Република Македонија, како и внатрешната и надворешна безбедност од евентуалните промени на глобално, регионално или локално ниво во периодот кој следи, од огромна важност е државниците и донесувачите на одлуки во Република Македонија да добиваат информации кои се неопходни за успешно водење на сите витални државни функции. Потребно е овие субјекти навреме и објективно да бидат информирани за ситуациите со кои се соочуваат, за можностите кои ги имаат и за импликациите од нивните одлуки.

За да се постигне оваа цел на полето на безбедноста во Република Македонија, потребно е да се преземаат одредени мерки и активности од страна на безбедносниот сектор, кои ќе вклучуваат најразлични начини за доаѓање до потребните податоци кои се поврзани со националната безбедност, и нивна обработка во крајна информација која ќе биде презентирана пред крајните корисници. Бидејќи податоците кои се од интерес за безбедносниот сектор можат да бидат од различен вид, потребно е институциите на безбедносниот сектор да ги земаат предвид сите можности за прибирање, односно мора да вклучуваат широк дијапазон на методи и начини на работа со цел да произведат навремени, точни и релевантни информации. Како заклучок на претходно наведеното, произлегува потребата од успешно менаџирање со податоците и информациите кои се користат во безбедносниот сектор, односно нивно навремено прибирање, нивна обработка и анализа и нивна навремена дисеминација до раководните државни или безбедносни органи на Република Македонија. За да се обезбеди потребната ефикасност во работата, од огромно значење е сите прибрани податоци, континуирано и навремено да се обработуваат со цел да се подготви конечната информација, која ќе се достави до државните раководни органи на Република Македонија, кои врз основа на таа информација ќе донесат одлука како да се одговори на прашањата и дилемите со кои се соочува државата за поддршка на нејзината политика и за целосна заштита на нејзините витални национални цели и интереси. Секоја институција која е дел на безбедносниот сектор на Република Македонија, без разлика на нејзиниот делокруг на работа, поставеност во системот или

големина, мора да е подготвена и да има разбирање за значењето на информациите и информирањето. Безбедносните институции мора да имаат капацитети за ефективно искористување на информациите кои ги подготвуваат, но и за оние информации кои се споделени помеѓу различните компоненти на безбедносниот сектор и да им дадат соодветно толкување на тие информации во рамките на својот домен на работа.

Со цел информирањето да биде колку што е можно пообјективно и попрецизно, на секоја изготвена информација мора да ѝ биде проценета релевантноста и веродостојноста со цел да се одреди колку таа ја објаснува и нуди решение за одредена безбедносна ситуација или појава. Кога ќе се одреди дека таа информација има одредено значење и дека може да се искористи, врз нејзина основа се прават анализи и предлози за одредена безбедносна закана и за менаџирањето на неа. Ова е процес што мора да се прави континуирано со цел да се избегне каков било пропуст или донесување одлука врз основа на непроверена информација, и затоа мора секоја информација да ги исполни ригорозните стандарди на проверка, со цел да се земе предвид и да се вклопи во целосната слика. Како резултат на претходно кажаното, може да се заклучи дека ова е еден многу специфичен и интензивен процес, кој поставува многу високи критериуми пред субјектите кои треба да ги вложат сите свои познавања и аналитички капацитети за да не донесат погрешна одлука за релевантноста и веродостојноста на одредена информација.

Промените во безбедносното опкружување и појавата на нови безбедносни предизвици и закани, наметнуваат нови побарувања пред безбедносниот сектор на Република Македонија, и како резултат ја наметнуваат потребата од што повеќе податоци, кои ќе опфаќаат што поголем дијапазон на области. Безбедносните институции на Република Македонија треба да се фокусираат кон прибирањето податоци кои можат да ги посочат можните актери кои би ја нарушиле националната безбедност на Република Македонија. За таа цел, треба постојано да се работи во насока на унапредување на методите и техниките за доаѓање до нови податоци, донесувањето објективна процена на нивната вредност и релевантност, колку што е можна поквалитетна и побрза анализа на овие податоци, изработка на конечната информацијата и нејзина навремена и прецизна дисеминација до донесувачите на одлуки.

6.2. Потребата за споделување информации во безбедносниот сектор на Република Македонија

Секоја институција која го сочинува безбедносниот сектор на Република Македонија има свое поле на работа, односно свои приоритети и насоченост на своите активности. Споделувањето информации е критично за остварувањето на целите на безбедносниот сектор и успехот во неговата работа зависи од воспоставувањето на ефикасни системи и процеси кои ќе помогнат во споделувањето на информациите, развивањето на стратегија за надминување на сите препреки кои го спречуваат споделувањето информации, и пронаоѓањето начин да се воспостави модел кој ќе овозможи ефективна соработка и доверба помеѓу неговите компоненти. [166]

Успешното споделување информации и координацијата помеѓу безбедносните институции во Република Македонија имаат големо влијание во справувањето со безбедносните закани. Споделувањето треба да биде насочено преку одредени законски рамки и директиви, кои симултано ќе им дадат и овластувања и одредени ограничувања на сите учесници во тој процес, и кои јасно ќе дефинираат за кои типови на информации ќе биде дозволено да се споделуваат, но и кои типови ќе треба да подлежат на дополнителна заштита. Потребно е да се искомбинираат упатствата, процедурите и технологиите кои ќе ги поврзат луѓето, системите и информациите кои ќе бидат дел од процесот на споделувањето. Треба да се делегираат улогите и одговорностите со цел да се воспостават темелите на тој процес и да се дефинираат задачите кои треба да се извршат и целите кои треба да се постигнат со споделувањето информации.

Споделувањето е сеопфатно и многуслојно прашање кое во себе вклучува управни, информатичко-комуникациски, културни и економски фактори. Со цел да се унапреди споделувањето, мора да се идентификуваат и да им биде посветено внимание на критичните прашања кои одредуваат каков е односот на безбедносниот сектор кон сите овие фактори. Овие напори ќе бидат круцијални за воспоставувањето еволуиран модел за споделување информации кој ќе ја засили соработката, ќе внесе унифициран

---

[166] Carter L. David - *„Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies"*, Michigan, 2006, p.1

пристап кон практиките за споделување и ќе ја зголеми достапноста на корисни информации.

Доколку се направи анализа за тоа на кој степен се наоѓа споделувањето информации во безбедносниот сектор на Република Македонија, може да се забележи дека во одредени инстанци постои споделување информации, и тоа прилично успешно споделување, кое се врши на одредени координации помеѓу институциите кои го сочинуваат безбедносниот сектор, како и преку учеството во различни работни групи и заеднички акции. Меѓутоа, треба да се напомене дека има многу простор за унапредување на споделувањето, и ова е всушност констатација која произлегува од видливоста на некои од препреките за споделување. Имено, препреките за споделување информации кои се евидентни во безбедносниот сектор на Република Македонија, се истите оние препреки кои се идентификувани како предизвик при секое споделување информации и во останатите држави и во нивните безбедносни сектори, како и во меѓународните организации кои работат на полето на безбедноста. Постапките во насока на унапредување на споделувањето треба да се концентрираат врз овие категории на препреки и да понудат применливи решенија кои ќе ја опфатат секоја перспектива.

Овде во прв ред се мисли на препреките кои произлегуваат од учесниците во процесот на споделување информации, и кои се веќе добро идентификувани, а тоа се недостатокот на доверба помеѓу учесниците во споделувањето и организациона култура и различните работни практики на институциите. Довербата е многу значаен фактор за споделувањето, бидејќи институцијата која треба да ги сподели информациите може да има одбивност кон споделувањето, бидејќи нема доверба во другата институција на која им ги доставува информациите дека успешно ќе ги заштити. На институционално ниво, различните безбедносни институции во Република Македонија немаат доверба во другите институции кои се дел од безбедносниот сектор, и имаат одредени задршки при споделувањето информации. Тие може да одлучат да не споделуваат информации воопшто или да споделуваат само некорисни информации, бидејќи немаат доверба во другите институции кои се дел од безбедносниот сектор на Република Македонија. Оваа недоверба може да се должи на меѓусебниот натпревар за репутација или за одобрување поголем буџет и други ресурси, и има големо значење за нивната мотивација за споделување, бидејќи тие ги гледаат своите сопствени интереси.

Освен погоре споменатите препреки, мораме да се земат во предвид и препреките кои произлегуваат од карактеристиките на информациите кои се споделуваат, а никако не смеат да се занемарат и препреките од техничка природа, кои произлегуваат од различниот степен на развиеност во поглед на комјутерско-технолошките способности на различните институции кои го сочинуваат безбедносниот сектор на Република Македонија. Исто така, мораат да се земата во предвид и интероперабилноста на системите кои ги поседуваат различните безбедносни институции во Република Македонија, како и постоењето/непостоењето и почитувањето на безбедносни мерки и процедури, како и контролата на системот.

За крај на оваа дискусија околу препреките за споделување информации во безбедносниот сектор на Република Македонија, мора да се предочат и препреките кои произлегуваат од недостатокот на утврдени законски регулативи и процедури за споделување, односно непостоењето на законска регулатива за споделување информации, како и отсуството на централизирано тело во Република Македонија што ќе го управува споделувањето.

Треба да се промовира една култура за споделување информации и да се спроведат обуки кои ќе стават акцент на одговорноста за споделување, и кои ќе придонесат за разбирањето на импликациите за заштита на изворите и методите на работа на безбедносните институции во Република Македонија. Со промовирањето култура за споделување информации, учесниците во процесот самите ќе работат во насока на отстранување на пречките и во изнаоѓањето подобри методи и алатки за споделување, што пак од своја страна ќе придонесе за поуспешна работа на целокупниот безбедносен сектор на Република Македонија. Со цел да заживее споделувањето информации во Република Македонија, мора да се идентификуваат предизвиците и грешките кои ќе се појават, да се унапреди културата во безбедносниот сектор во однос на промоција и препознавање на предностите кои ги нуди споделувањето и да се усвои пристап кој ќе вклучува менаџирање на безбедносните ризици кои го носи споделувањето.

За таа цел, може да се размисли на инкорпорација на предложениот модел погоре во текстот во безбедносниот сектор на Република Македонија. Бидејќи овој модел е составен од неколку стратегиски и оперативни компоненти, секоја од нив се истакнува со свое значење за неговото беспрекорно функционирање. Функционирањетоа на овој модел во Република Македонија може да им ја обезбеди неопходната поддршка на безбедносните институциите при споделувањето

информации. Институциите кои го сочинуваат безбедносниот сектор на Република Македонија мора да имаат обезбедена максимална достапност до сите информации кои се однесуваат на националната безбедност. Токму затоа, неоходно е да се усвојат конзистентни практики и стандарди за пристапување, заштита, како и демонстрација на подготвеност од страна на безбедносните институции да се вклучат во процесот на споделување информации. Веродостојноста на информациите кои се споделуваат, степенот на меѓусебна доверба помеѓу институциите кои споделуваат информации, мерките и активностите за заштита на информациите и начинот на кој ќе бидат употребени информациите се есенцијалните елементи на воспоставувањето на околина на доверба помеѓу безбедносните институции во Република Македонија.

Во денешната сложена безбедносна средина, ризикот од несподелувањето информации може да доведе до пропуштање на важни сознанија кои се однесуваат на одредени антиопштествени дејства, кои може да предизвикаат загуба на човечки животи и да ја загрозат националната безбедност на Република Македонија. Оваа нова средина бара од безбедносниот сектор да работи во насока на создавање една култура која ќе промовира одговорност за споделување, и која треба да осигура дека сите компоненти на безбедносниот сектор имаат волја, можности и инфраструктура за споделување. Новиот принцип ќе придонесе токму во таа насока, притоа функционирајќи како воспоставена практика во донесувањето одлука дали една информација да се сподели.

6.3. Мерки и активности за заштита на информациите во безбедносниот сектор на Република Македонија

Со цел информациите кои се користат во безбедносниот сектор на Република Македонија да бидат искористени со сиот свој капацитет и да ја одиграат својата значајна улога, мора да се заштитат од неовластен пристап или од неовластено објавување во јавност што ќе ја намали (или тотално ќе ја уништи) нивната вредност. За да се спречи ваквата ситуација, најважните, односно најчувствителни информации се класифицираат и за нив се применуваат посебни мерки и активности кои треба да го заштитат нивниот интегритет. Меѓутоа, ова не е така лесна работа, затоа што заканите за безбедноста на информациите и информатичката технологија која се користи за

ракување со нив и нивно чување се постојани и променливи. Заштитата на класифицираните информации во Република Македонија е многу сложен предизвик, бидејќи заканите и ризиците за нарушување на безбедноста на информациите постојано се зголемуваат, и стануваат многу поконкретни и пософистицирани. Доказ за ова се големиот број класифицирани информации кои завршуваат во медиумите во Република Македонија, како и неколкуте афери и судски случаи кои вклучуваа компромитирање и доставување класифицирани информации до трети лица или до други заинтересирани страни. Уште една работа која треба да се земе предвид кога се зборува за заштита на класифицираните информации, е тоа што безбедносните институции на Република Македонија со цел да ги остварат своите обврски се потпираат на користењето најразлични информатичко-комуникациски уреди и компјутерски мрежи, а како резултат на ова се зголемува и бројот на лица кои ракуваат со класифицирани информации. Ваквата ситуација кога има зголемени безбедносни ризици и закани за безбедноста на класифицираните информации, и кога расте бројот на субјектите кои имаат пристап до класифицирани информации значително го зголемува ризикот од безбедносни нарушувања и компромитирања.

Класифицираните информации кои се користат во безбедносниот сектор на Република Македонија мора да се заштитат од голем број безбедносни закани кои доколку се манифестираат ќе резултираат со нарушување на безбедноста на класифицираните информации, најчесто преку неовластен пристап до нив или нивно неовластено објавување. Ваквата ситуација би предизвикала одредена штета (во зависност од чувствителноста на информацијата е и штетата која би настанала) при работата на безбедносната институција. Безбедносните закани можат да се манифестираат преку ненамерни грешки и невнимателност на лицата кои ракуваат со нив, шпионски активности, неовластен упад во информатички систем и сл. Затоа, секоја институција во која се ракува со класифицирани информации треба да презема одредени мерки и активности за заштита на класифицираните информациите, кои ќе имаат за цел да го заштитат интегритетот и чувствителноста на информациите.

Постојната законска регулатива која ја уредува заштитата на класифицираните информации во Република Македонија (Законот за класифицирани информации и пропратните уредби), предвидува одредени мерки и активности кои треба да се преземат со цел да се исполнат минималните безбедносни стандарди за безбедност на класифицирани информации. Со цел да се исполнат овие стандарди, потребно е да се

инкорпорира еден систем, кој ќе вклучува мерки и активности од административната, физичката, персоналната и информатичката безбедност на класифицирани информации. Секоја од овие компоненти кои го сочинуваат системот на заштита на класифицираните информации поставува одредени побарувања пред создавачите и корисниците на класифицираните информации, и само со исполнување на овие побарувања може да се гарантира дека успешноста во работата на безбедносниот сектор нема да се намали, туку напротив ќе се зголеми и интензивира.

Заштитата на класифицираните информации во безбедносниот сектор на Република Македонија е на задоволително ниво, но сепак мора да се нагласи дека има простор за напредок на ова поле. Резултатите од истражувањето покажуваат дека голем број од испитаниците се запознаени со законските одредби и имаат поминато некаков вид на обука за ракување со класифицирани информации. Оние испитаници кои во рамките на своите работни обврски ракуваат со класифицирани информации и поседуваат безбедносен сертификат, детално се запознаени со своите обврски при редовното брифирање кое е задолжително при врачувањето на безбедносниот сертификат од страна на овластеното лице во институцијата. Овде треба да се напомене дека Дирекцијата за безбедност на класифицирани информации, како одговорна институција за заштитата на класифицираните, има своја мрежа на регистри и контролни точки во сите институции во кои се ракува со класифицирани информации (не само во безбедносните институции, туку и во другите органи на државна управа каде што има класифицирани информации) и остварува координација со овластените лица (офицери за безбедност) кои се грижат за почитувањето на мерките и активностите за заштита на класифицираните информации во рамките на своите инситуции.

Бидејќи безбедносниот сектор на Република Македонија е постојано исправен пред безбедносни ризици и закани кога е во прашање безбедноста на класифицираните информации, мора да се оддржи постојана алертност и антиципација во поглед на реалната манифестација на овие ризици и закани. Ситуацијата мора постојано да се следи и да се посветува огромно внимание на оние закани чиешто остварување е најверојатно и кои може најмногу да наштетат на работата на безбедносниот сектор на Република Македонија.

Како централна и најголема закана овде се наметнува внатрешната закана, што всушност е нарушување на безбедноста на класифицираните информации од лица кои

се дел од безбедносниот сектор, односно се вработени во некоја од безбедносните институции на Република Македонија. Внатрешната закана може да се манифестира на два начини, и тоа:

- Внатрешна закана која настанала заради ненамерен пропуст, случајност, невнимателност или неажурност на вработениот. Во овој случај, грешката што ја направил вработениот може да биде лошо чување на класифицирани информации (на работна маса, во незаклучена фиока) во моменти кога е отсутен од своето работно место, оставање отворен кориснички акаунт на компјутерот во ситуација кога не е присутен на своето работно место, водење на разговор за класифицирани теми на необезбедено место (кујна, место за пушење, превозно средство) и сл.;
- Внатрешна закана која настанала заради умисла и намерна акција на вработениот. Ова е ситуацијата која резултира со најголема штета и која е можеби и најтешко да се превенира. Во овој случај, се работи за лица кои детално ги познаваат практиките и процедурите кои се на сила во институцијата и кои можат незабележано да ја извршуваат својата незаконска активност подолго време. Тие имаат непречен пристап до класифицирани информации, уживаат доверба во средината во која работата, и доколку се внимателни и посветени на својата незаконска активност, можат многу лесно да избегнат каков било сомнеж или откривање.

Како еден краток заклучок на досега споменатите побарувања, критериуми и предизвици, може да се заклучи дека е потребно воспоставување на еден сеопфатен пристап во безбедносниот сектор на Република Македонија кој ќе овозможи будност и ефективност во заштитата на класифицираните информациите од неовластен пристап или објавување.

6.4. Информациите како услов за ефикасно планирање во безбедносниот сектор на Република Македонија

Република Македонија треба да биде насочена кон изградување безбедносен сектор што ќе биде погоден, ефикасен и компатибилен до таа мера што секој граѓанин којшто е дел од заедницата ќе се чувствува сигурен, обезбеден и слободен во

остварувањето на своите права и интереси загарантирани со Уставот, законите и голем број на меѓународни документи. Целта на овој сектор е да ја отстрани загрозеноста што му се заканува на општеството и на неговите составни делови и да овозможи остварување на интересите на поединците како и заштитување на нивните основни слободи и права што им се гарантирани со голем број меѓународни документи, преку ефикасно, брзо и навремено реагирање во сложени безбедносни ситуации.

Планирањето на безбедноста претставува специфично подрачје на примена на научни методи за согледување и проценување опасности за безбедноста на земјата, предвидување на идните настани и движења и утврдување мерки и активности за навремено реагирање доколку дојде до загрозување на мирот, независноста и територијалниот интегритет на државата.[167] Тоа претставува конкретизирање на остварувањето на целта на безбедноста и е една од битните функции на секоја држава со конституиран безбедносен сектор. Задачите кои треба да се постигнат со планирањето на безбедноста зависат од многу фактори и влијанија на околината. Процесот на планирање на безбедноста, почнувајќи од дефинирањето на целите, политиката и стратегијата, активности кои се однесуваат на анализа на состојбите и можностите, процена на бројните услови и фактори кои влијаат и кои ќе влијаат на безбедноста во одредени конкретни услови, односи и ситуации. Со помош на планирањето се врши насочување на безбедносните институции, кое се базира врз анализа на развојот и работата во изминатиот период, преку процена на моменталната состојба и очекувањата за иднината. Планирањето е дефинитивно, функција на антиципативно одлучување која определува разновидни цели кои ќе бидат приспособени под влијание на екстерното и интерното окружување.[168]

За планирањето во безбедносниот сектор да биде ефикасно, повеќеслојно, интегрирано, тоа мора да се гради врз основа на квалитетни информации кои го опфаќаат секој моментален и иден аспект од работата на безбедносниот сектор на Република Македонија. Ова планирање треба да се темели на научна и стручна анализа на информациите кои се однесуваат на одредени безбедносни ризици и закани и информирање на сите релевантни фактори и субјекти кои имаат улога во донесувањето и насочувањето на акциите и организацијата на националната безбедност на Република Македонија. Со помош на информациите и информациите се прави едно ефикасно

---

[167] Стаменковски, Алекса – *„Планирање на одбраната“*, НИП Ѓурѓа, Скопје, 1996, стр.11

[168] Шуклев, Бобек – *„Менаџмент“*, Економски Факултет, Скопје, 1998, стр.131

планирање на следните чекори и активности и се овозможува флексибилност во денешната променлива безбедносна околина во која се наоѓа Република Македонија. Ваквото ефикасно планирање им овозможува на институциите да ги насочат своите постапки и да ги спречат изненадувањата, како краткорочно така и долгорочно, и да ја заштитат внатрешната и надворешната безбедност на Република Македонија.

Доколку планирањето во безбедносниот сектор на Република Македонија се врши врз основа на релевантни и веродостојни информации, кои навреме се доставени до донесувачите на одлуки во државата, кои преку тоа информирање ќе се стекнат со витално разбирање на безбедносната состојба и моменталната ситуација, може да се очекува следнава идеална состојба:

- идентификација и анализа на предметот на безбедносната закана;
- анализа на моменталната состојба и веројатните идни промени на безбедносната закана;
- планирање на активности и планирано алоцирање на сопствените ресурси и
- фокусирање на очекуваните ефекти и последици.

При планирањето постојано треба да се разгледуваат и да се ажурираат сите аспекти од работата. За да постои добро планирање, мора да постои добра соработка и координација помеѓу институциите кои го сочинуваат безбедносниот сектор на Република Македонија. Размената на совети и информации помеѓу безбедносните институциите е исто така многу важен дел при планирањето. Преку ефикасното планирањето треба да се постави визијата, насоката и активностите во поглед на тоа што, кога и како треба да се постигне. Она што е неопходно да се истакне е дека планирањето не треба да биде ригидно, туку мора да се приспособува на новонастанатите ситуации и новите информации.

Глава 7

Интерпретација на резултатите од спроведеното истражување

7.1. Интерпретација и анализа на резултатите

За потребите на докторската дисертација беше спроведено истражување кое треба да претставува една добра основа за согледување на состојбата кога е во прашање местото на информациите и информирањето во безбедносниот сектор, и кое докажува дека постои простор и можност за унапредување и надградување на нивното место.

Во основа, ова истражување се фокусира на концептите информација и информирање, и како тие се корисни во работата на институциите кои го сочинуваат безбедносниот сектор, од една инсајдерска перспектива. Истражувањето вклучува теоретска расправа, но и истражување кое се однесува на секојдневните практики и активности во работата на институциите. Со тоа, резултатите од истражувањето ќе придонесат за зголемување на свесноста во поглед на вредноста на информациите, што пак ќе придонесе кон идентификување и имплементирање на решенија од нова перспектива. Исто така, истражувањето дава контрибуција за разбирањето на моменталните и идните фактори, притоа ставајќи ги сите нив во една рамка за која може поконструктивно да се дискутира и да се дебатира јавно, имајќи ги предвид новите технолошки можности и трансформацијата на моменталните општествени и безбедносни парадигми. Поширокатa цел на ова истражување е да даде придонес кон академското и практичното знаење кое се однесува на ефективното искористување на информациите во безбедносниот сектор и да ја унапреди работата на безбедносните институции. Преку прифаќањето на одредени наоди од ова истражување, безбедносните институции ќе можат поефикасно и поекономично да ги насочат своите активности, и преку својата функционалност да ја постигнат нивната примарна цел - навремен и прецизен одговор што ќе резултира со отстранување на сите опасности по здравјето и животите на граѓаните.

За потребите на истражувањето, направена е една кохерентна анализа на истражувачките инструменти, која придонесува кон концептуализација на главните елементи во истражувањето (информациите и информирањето) во тридимензионалната рамка која се истражува: прибирањето на информациите, нивното споделување и нивната заштита. Истражувањето беше извршено комбинирано, квантитативно и квалитативно.

Како техника на прибирање податоци се користеше анкетирањето и идејата беше да се соберат податоци за ставовите и размислувањата на одредена група на лица од интерес (вработени во безбедносниот систем) со помош на структурирани прашања. Преку анкетирањето се собираат податоци за појавата што се истражува врз основа на мислењето на испитаниците, и овој емпириски метод имаше предност пред другите методи затоа што овозможува: собирање податоци од поголем број испитаници за релативно кратко време, анонимноста на анкетата обезбедува поголема искреност на испитаникот, економичноста на овој метод и полесната обработка на податоците. Како истражувачки инструмент, беше користен анонимен анкетен прашалник. Овде треба да се напомене дека прашалникот беше од комбиниран тип, затоа што одреден број од прашањата не содржеа понудени одговори, туку имаа за цел да ги наведат испитаниците да дадат свои сопствени размислувања и образложенија, бидејќи постоеше опасност дека предвидените одговори не го опфаќаат целосно проблемот. На крај, треба да се истакне дека при изготвувањето на прашалникот, се водеше сметка тој да биде приспособен на предметот на истражувањето, на хипотезите, како и на испитаниците (изворите на податоци) и да биде валиден и објективен.

Исто така, за потребите на истражувањето, се примени и нестандардизирано итервју. При водењето на интервјуто, суштината беше да се насочи разговорот кон истражувањето на појавата, и негова огромна предност (за разлика од анкетниот прашалник) е во непосредниот контакт помеѓу испитувачот и испитаникот, како и во можноста испитувачот да се адаптира на физичките и менталните конструкции на испитаникот, како и можноста за дополнителни прашања и објаснувања. Употребата на овие методи придонесе за зголемување на синергијата помеѓу истражувачот и соговорниците, што придонесуваше кон поуспешна дискусија, а мора да се напомене и динамичката природа на интервјуто и групната дискусија која овозможува поголема активност отколку структурираниот анкетен прашалник, како и можноста да се добијат подетални објаснувања за одредени ставови и размислувања.

По прибирањето на резултатите од истражувањето, се пристапи кон анализа и синтеза на добиените одговори на колку што е можно попрецизен начин, со цел заклучоците кои ќе произлезат од истражувањето да бидат објективни и во согласност со добиените резултати. Со цел да се зголеми колку што е можно повеќе веродостојноста на истражувањето и на добиените резултати, и имајќи предвид дека истражувањето е извршено преку интеракција со човечки субјекти, целта на истражувачот беше да осигура дека истражувачкиот инструмент, т.е. анкетниот

прашалник, е колку што е можно порепрезентативен, со цел да се добие поголем вариетет на одговори. Анкетниот прашалник е даден како прилог кон дисертацијата, со цел да се добие слика за начинот на кој беа анкетирани испитаниците.

Во однос на целната група треба да се потенцира дека истражувањето опфати 209 анкетирани лица. Со анкетата беа опфатени лица кои се припадници на Министерството за внатрешни работи, Министерството за надворешни работи, Секторот - Служба за воена безбедност и разузнавање (ССВБиР), Г-2 на Генералштабот на Армијата на Република Македонија, неколку офицери за разузнавање од АРМ, припадници на Дирекцијата за безбедност на класифицирани информации, како и активни и поранешни припадници на Агенцијата за разузнавање и на Управата за безбедност и контраразузнавање. Исто така, истражувањето ги опфати и експертите, но и студентите на II и III циклус студии од Институтот за безбедност, одбрана и мир, Воената Академија, како и од Факултетот за безбедност. Освен домашните колеги и експерти, во истражувањето беа опфатени и испитаници од светски реномирани организации и институции, меѓу кои: Fakultet Bezbednosti, Univerzitet u Beogradu, Beograd, Srbija; The Intelligence & Security Academy, Arlington, Virginia 22203; National Security Studies Institute, The University of Texas at El Paso; International Association for Intelligence Education, Marymount University, Arlington, Virginia; Center for International and Security Studies at Maryland, School of Public Policy RAND Corporation, Santa Monica, California; Institute for Security Studies, Veale St, Pretoria, South Africa; Institute for National Security and Counterterrorism, Syracuse University; The European Union Institute for Security Studies (EUISS), Brussels, Belgium и U.S. Security Institute, Arlington, Texas.

За полесно прикажување на резултатите, испитаниците беа поделени во неколку категории, и тоа:

- претставници на Министерството за одбрана
- претставници на Министерството за внатрешни работи
- претставници на безбедносните и разузнавачките служби
- претставници од екпертската заедница
- претставници од II и III циклус студии на безбедносно едукативните образовни институции (Воена академија, Институт за одбрана, безбедност и мир, Факултет за безбедност).

Во однос на одговорите на прашањата мора да се истакне дека за одредени прашања се добиени целосни одговори, за дел од прашањата имаме симболични одговори заради чувствителноста на прашањата и затворената природа на институциите, а за мал дел и послаби одговори кои се должат на непознавање на материјата која се истражува.

7.1.1. Информации и информирање

Информациите и информирањето се неопходни и конзистентни во многу различни околини и претставуваат една од основните карактеристики на човечкиот род, а тоа е можноста субјективно да се процесираат спознанија и факти и да се генерира одредено знаење. Ефикасноста и ефективноста во работата со информациите полека станува еден од најзначајните фактори за успех во голем број сфери на човечки активности, а во исто време истражувањето на информациите станува сè покомплексно и бара сè поголеми специјализирани знаења и техники. Скоро секоја научна дисциплина денес го користи концептот информација во свој контекст и во однос на свој специфичен феномен.

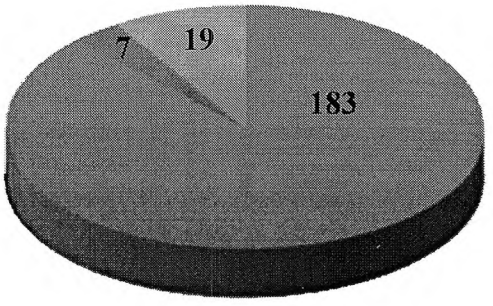
Во однос на информациите и информирањето, за потребите на безбедносниот сектор, на испитниците им беше поставено следното прашање: „*Дали сметате дека информациите и информирањето се доволно истражени во домашната научна теорија?*“

Ова прашање се одликува со голема усогласеност на одговорите. Ставовите на експертите, чиишто одговори беа следени со особено внимание, заради нивното најдобро познавање на достапната литература, се прилично усогласени по однос на ова прашање, и едноставно е зачудувачки фактот дека досега немало некои посериозни обиди за разработка на овие концепти, а со тоа и на самата нивна улога во работата на безбедносниот сектор. Одговорите на испитаниците од другите категории исто така посочуваат дека е потребна дополнителна работа на ова поле. Ваквата појава, заедно со останатите добиени одговори на ова прашање, му ја даваат толку посакуваната научна оправданост на истражувањето на информациите и информирањето и ја зголемуваат неговата вредност. Ова се согледува во продлабочувањето на теоријата која се однесува на работата на безбедносниот сектор и стекнувањето на нови и проширени знаења за улогата и влијанието на информациите во безбедносниот сектор.

7.1.2. Информирањето како важен предуслов за ефикасното функционирање на безбедносните институции

Информирањето има свој придонес во сите области на човечки активности, па така и во работата на безбедносните институции. Тоа претставува наука и уметност за преземање практични постапки кои ќе придонесат за зголемување на ефективноста, етичноста и/или ефикасноста во проширувањето на знаењето и контролата врз реалноста. За да биде корисно при работата на безбедносните институции, информирањето мора да биде ефективно и постојано. Успехот на безбедносниот сектор зависи од комбинација на различни фактори, па за таа цел институциите кои го сочинуваат тој сектор мора да ги разгледуваат безбедносните ризици и закани од колку што е можно повеќе гледни точки, а за да го направат тоа, потребно им е да поседуваат доволно информации кои се однесуваат на нив.

Прашањето *„Дали сметате дека информирањето е важен предуслов за ефикасното функционирање на безбедносните институции?“* предизвика незначителна варијација во одговорите на испитаниците. По анализата на добиените одговори, може да се забележи дека огромен дел од испитаниците одговориле позитивно на прашањето дали информирањето е важен предуслов за ефикасното функционирање на безбедносните институции. Вредноста на информациите и информирањето се огледува во големото давање на признание за неговата ефикасност од страна на анкетираната група.



- **Одговор под а) Информирањето е важен предуслов за ефикасното функционирање на безбедносните институции**
- **Одговор под б) Информирањето не е важен предуслов за ефикасното функционирање на безбедносните институции**
- **Одговор под в) Не знам**

При разговорите со одреден број испитаници од сите категории, беше утврден став дека без точни, навремени и квалитетни информации активностите на безбедносниот сектор може да бидат задоцнети, лошо испланирани, насочени и изведени, и дека делувањето без доволно информации е делување на слепо. Исто така, интересно е да се забележи и една појава која ги карактеризира одговорите на ова прашање, а тоа е што поголемиот дел од испитаниците сфаќаат дека информирањето е неопходно за да се оствари успех во работата во оние професии или области кои се поврзани со користење информации. Во контекст на ова, мора да се истакне дека најобединети размислувања по ова прашање имаат припадниците на безбедносните и разузнавачките служби кои му даваат огромно значење на информирањето.

7.1.3. Планирањето како ефикасна алатка во менаџирањето на работата на безбедносниот сектор

Бидејќи работата на институциите кои го сочинуваат безбедносниот сектор вклучува повеќе логично поврзани постапки во правец на најефективно извршување на своите задачи, планирањето се наметнува како една неопходна и исклучително чувствителна постапка. Основната функција на планирањето во безбедносниот сектор се состои во утврдување на безбедносната политика, планирање безбедносни мерки и активности, планирање на силите и средствата за безбедност. Со планирањето се проценуваат идните настани и влијанија врз земјата, а врз таа основа се планираат безбедносни мерки и активности и постигнување поголем степен на безбедност. Исто така, се планираат повеќе варијанти за сите безбедносни активности со цел во определено време и во конкретни услови да може да се примени најповолната варијанта која ќе обезбеди постигнување на најефикасни резултати.[169]

Во однос на планирањето, на испитаниците им беше поставено следново прашање *„ Дали сметате дека планирањето е ефикасна алатка во менаџирањето на работата на безбедносниот сектор? “*

При анализа на одговорите на испитаниците од сите категории опфатени со истражувањето може да се согледа дека нема значителни отстапувања од вкупната проценка на одговорот што доминира. Анкетираните лица од сите категории преку своите одговори му го даваат заслуженото внимание на планирањето. Имено, веќе

[169] Стаменковски, Алекса – *„Планирање на одбраната“*, НИП Ѓурѓа, Скопје, 1996, стр.126

станува задолжителен дел при секоја активност, па дури и најсекојдневните активности не се извршуваат без него. Затоа, не треба да зачудува фактот што скоро сите анкетирани лица сметаат дека планирањето е една од неопходните фази, а големо совпаѓање на одговорите може да се забележи и ако се разгледуваат одговорите според категориите на испитаници. Припадниците на Министерството за одбрана, Министерството за внатрешни работи и на безбедносните и разузнавачките служби одговориле позитивно во скоро сите одговори. И другите две категории на испитаници, експертите и колегите студенти исто така имаат доминантно позитивни одговори на ова прашање.

7.1.4. Превентивни активности на безбедносниот сектор

Активностите на безбедносниот сектор на државата во прв ред мора да бидат насочени кон антиципација и превенција на сите форми на безбедносни закани или криминалитет, а не кон реакција откако тие го манифестирале своето антиопштествено дејство. Ова значи дека активностите на институциите кои го сочинуваат безбедносниот сектор мора да вклучуваат широк дијапазон на методи и начини на работа со цел да успеат да ги неутрализираат безбедносните закани.

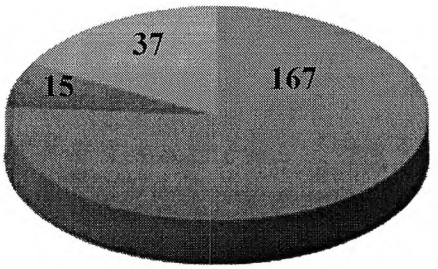
За да се согледа односот кон превенцијата, на испитаниците им беше поставено следното прашање „ *Дали се согласувате дека активностите на безбедносниот сектор треба да бидат насочени кон превенирањето на безбедносните закани, односно справување со нив пред тие да успеат да ги манифестираат своите општествено негативни последици?* “

За голем број од испитаниците нема дилема дека превенцијата е особено важна, па затоа сфатлива е доминацијата на позитивниот одговор по однос на ова прашање, бидејќи анкетираните лица се согласуваат дека само преку превенирањето на одредени антиопштествени појави ќе се спречат несаканите последици кои тие би ги предизвикале.

Она што е интересно во однос на одговорите на ова прашање е доминацијата на потврдниот одговор кај припадниците на МВР и припадниците на безбедносно-разузнавачките служби. Ова се должи на природата на работа на овие институции, чијашто задача е да го спречат остварувањето на безбедносните ризици, односно да

успеат навреме да реагираат за да спречат какви било безбедносни инциденти, конфликти, немири, различни форми на криминал и слично.

Превенцијата на безбедносните закани вклучува активности на различни субјекти кои треба да преземаат превентивни мерки. Квалитетот во работата на полето на превенција ќе има влијание не само врз општата безбедносна состојба во државата, туку и врз безбедносната култура на граѓаните. Но, и покрај фактот што работата на полето на превенција на безбеднисните закани не е инстантно видлива, ниту пак е статистички мерлива во одреден момент или временски период, таа е потребна и неопходна заради поквалитетна иднина на самите нас и на идните генерации.



- **Одговор под а) Активностите на безбедносниот сектор треба да бидат насочени кон превенирањето на безбедносните закани**
- **Одговор под б) Активностите на безбедносниот сектор не треба првенствено да бидат насочени кон превенирањето на безбедносните закани**
- **Одговор под в) Не знам**

7.1.5. Придонесот на информациите во работата на безбедносниот сектор

По првичните неколку прашања, кои беа со веќе понудени одговори, ова е првото од серијата прашања кои немаат понудени одговори и имаат за цел малку поинтерактивно да ги вклучат испитаниците во самото истражување.

Самата формулација на прашањето *„На каков начин сметате дека информациите придонесуваат во работата на безбедносниот сектор?“*, доведува до ситуација во која имаме најразлични понудени одговори, што би било преобемно да се обработуваат поединечно. Меѓутоа, одговорите кои беа дадени на ова прашање се многу блиски еден до друг и отсликуваат слични ставови на испитаниците од сите категории, а тоа е дека информациите имаат големо значење и придонес во работата на безбедносниот сектор.

Ако не се располага со бројни и сигурни информации, не е можно да се спроведе анализа на работењето во претходниот период, да се предвиди иднината, да се оствари процесот на планирање. Информациите и информирањето овозможуваат да се конципираат што поквалитетни плански одлуки. Најмногу одговори на поставеното прашање одат во насока според која информациите се важни затоа што со поголема информираност може да се преземат превентивни дејства, кои ќе спречат какви било безбедносни закани. Навремената реакција на безбедносниот сектор врз основа на потврдени и целосни информации значително ја зголемува вредноста и потребата на информациите. Тие ја претставуваат и основата за насочувањето на активностите на безбедносните институции и ни овозможуваат подобро да ги запознаеме безбедносните закани и ризици и условите кои се потребни за нивно остварување.

7.1.6. Важноста на поседувањето навремени и точни информации

Потребата за навремени и веродостојни информации е од неопходно значење бидејќи безбедносните одлуки се донесуваат со помош на користењето на овие информации. Поседувањето објективна информација во даден момент може да ја направи разликата помеѓу добро донесена одлука и успешно завршена работа и погрешна одлука и катастрофален исход. Во истражувањето, за да се дознаат ставовите на испитаниците во однос на оваа дилема, им беше поставено прашањето *„Според Вас, какви ефекти може да предизвика имањето/немањето на навремени и точни информации врз работата на безбедносниот сектор?“* и им беше оставен простор за подолга дискусија и изнесување на свои сопствени ставови.

Притоа, најпрактичен начин за претставување на тие ставови е да се групираат одговорите во две групи, и тоа едната да се фокусира на ефектите од имањето навремени и точни информации, а другата на немањето на таквите информации.

Имањето, односно располагањето со навремени и точни информации во голема мера ја олеснува работата на безбедносниот сектор и ги има следниве позитивни ефекти:

- ефективност и ефикасност во работата
- насоченост и координација на активностите
- економичност во работата
- неутрализација на заканите

- спречување паника и несигурност кај населението
- задржување на ефектот на изненадување
- остварување на превентивната цел.

Немањето, односно недостатокот на навремени и точни информации при работата на безбедносниот сектор, ги има следниве негативни ефекти:

- пристап базиран врз основа на минати искуства, кој може да се покаже како погрешен
- некоординирана и избрзана реакција
- зголемена можност за грешки при дејствувањето
- ненавремена или задоцнета реакција
- ефектот на изненадување е кај противникот
- дополнителни обврски со цел да се намали паниката кај населението.

7.1.7. Информационен циклус

Во последниве неколку години, забележливо е значително зголемување на истражувања и трудови кои се пишуваат на тема информационен (во некои трудови се употребува терминот разузнавачки) циклус, бидејќи веќе и јасно се дефинирани фазите кои го сочинуваат овој циклус.

Процесот на прибирање, обработка и дистрибуција на точни, навремени и релевантни податоци кои можат да бидат претворени во информација не се случува сам по себе, туку е точно утврден циклус, кој е развиен на начин да претставува своевиден водич за креирањето релевантни и точни информации од брдото на податоци со кое се соочуваме. За да биде ефикасен, овој циклус мора да биде проактивен, да развива уникатни методи и принципи, и да ги доставува финалните информации навремено и конзистентно до соодветните корисници. Целта на овој процес е да им обезбеди на донесувачите на одлуки готови информации кои ќе им помогнат при донесувањето важни политички, безбедносни, економски и други одлуки.

Можеби сè уште постои една дилема дали одредени фази треба да се спојат или се самостојни, дали пак некои треба да се разделат бидејќи се премногу обемни и значајни за да се проучуваат заедно, но сево ова би било предмет на можеби некое друго истражување. Во истражувањето, особено интересно беше да се споредат

ставовите на испитаниците по однос на прашањето *„Дали сметате дека на информациониот циклус му е посветено доволно внимание во безбедносната теорија и практика?“* Одговорите на испитаниците во поглед на ова прашање се условени од неколку работи, како на пример навлезеноста на испитаникот во литературата која се однесува на овој циклус, неговата прилика да можел да учествува во ваков циклус и сл. На пример, одговорите на експертите посочуваат дека треба да се работи дополнително кон пронаоѓање начини за негово усовршување. Одговорите на припадниците на безбедносно-разузнавачките служби кои секојдневно преку својата работа се вклучени во некој дел од овој циклус (или во повеќе делови од него) нагласуваат дека е потребна понатамошно истражување на оваа тема. По однос на ова прашање, имаше и неколку испитаници од различни категории кои не беа доволно запознаени со овој циклус, затоа што не дошле во контакт со него ниту преку својата работа, а немаат ни теоретски познавања за него.

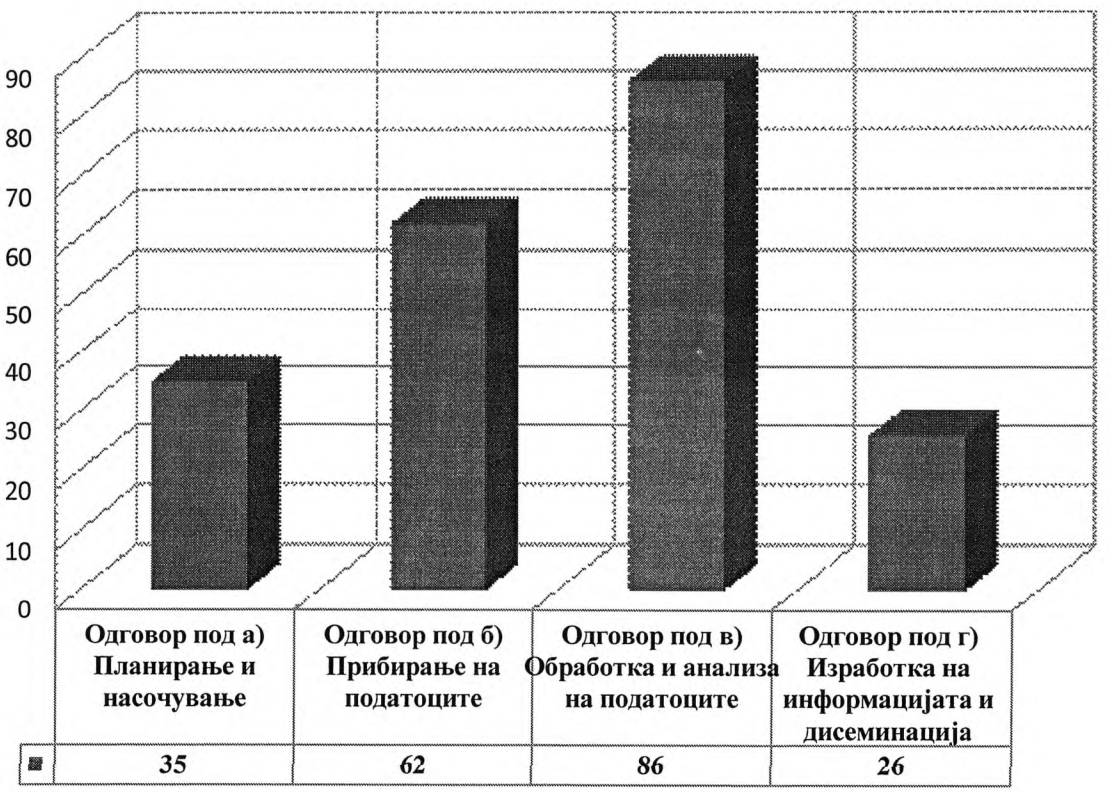
7.1.8. Фази на информациониот циклус

Бидејќи информациониот циклус подразбира повеќе логично поврзани постапки во правец на комплетирање на сликата за еден објект на интерес, тој е една сложена и исклучително чувствителна постапка, која вклучува повеќе значајни и комплицирани фази. Сите постапки во овој циклус имаат карактеристичен и незаобиколен период на траење и претходно замислени и заокружени целини. Всушност, овој процес е мултидимензионален, мултидирекционален, и најважно интерактивен и меѓусебно зависен.[170] Концептуално, овој циклус никогаш не завршува. Низ сиот процес, кој претставува една динамична средина, постојано ќе има побарувања за нови податоци или дадени случувања ќе им дадат нови значења на веќе изготвените информации, што ќе доведе до продолжување на овој циклус. Намената на овој циклус не е да воспостави процедура која мора да се следи, туку само да опише еден процес кој природно се појавува кога ќе се укаже потребата за дополнителна информираност за одреден предмет на интерес за безбедносниот сектор. Информациониот циклус опфаќа неколку зависно поврзани постапки, кои последователно би изгледале вака: планирање и

[170] Dearth, H. Douglas - *"National Intelligence: Profession and Process"*, Joint Military Intelligence Training Center, Washington DC, 1995, p.17

насочување, прибирање на податоците, обработка и анализа на податоците, изработка на информацијата и нејзино доставување (дисеминирање) до крајните корисници.

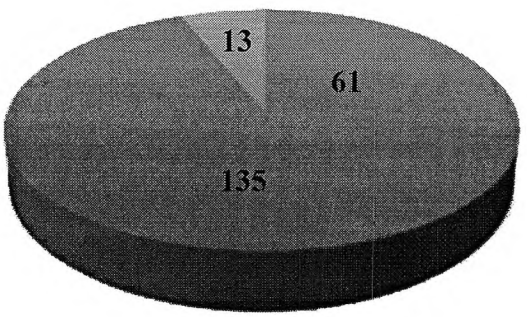
Во рамките на истражувањето, на анкетираните им беше поставено прашањето *„Според Вас, која од фазите на информациониот циклус има најголемо значење?“* во кое требаше да се одлучат која од фазите на информациониот циклус за нив има најголемо значење. Испитаниците кои беа анкетирани беа поделени во неколку категории. Преку анализа на нивните одговори може да се забележи дека нивните ставови се поделени по однос на ова прашање, но сепак на фазата на обработката и анализата на податоците ѝ се дава најмногу предност.



7.1.2. Извори за добивање податоци

Изворите на податоците се во директна корелација со релевантноста и веродостојноста на крајната информација, односно на нејзиниот квалитет. Податокот, основниот градбен блок на информацијата, се добива од извори кои генерално се класифицирани во две групи, отворени извори и затворени извори.

Внимателниот избор на изворите на податоците е една деликатна работа која бара многу внимание и објективна процена. Примери за отворени извори се домашните и странските средства за јавно информирање, печатените и електронските медиуми, интернет порталите, разни списанија, книги и научни истражувања, бази на податоци достапни за јавноста, владини извештаи и документи и сл. Затворените извори вклучуваат чувствителни или класифицирани документи и предмети, криптирани комуникации, тајни државни програми, заштитени објекти кои имаат важно значење за државата и сл. Врз основа на ова, има широко распространето мислење во јавноста дека податоците добиени од затворени извори се оние вистинските, што во некои случаи е точно, меѓутоа мора да се напомене дека во најголемиот број од случаите податоците се добиваат од отворените извори. И покрај тоа што во последно време огромен број податоци се прибираат од отворени извори и во литературата сè повеќе се валоризира нивната улога, одговорите на испитаниците на прашањето „ *Според Вас, кој од понудените (отворени или затворени извори на податоци) е порелевантниот извор за добивање на податоци?*“сепак посочуваат дека затворените извори не ја изгубиле својата вредност во работата на безбедносните органи.



Поголемиот дел од испитаниците сè уште имаат повеќе доверба во ваквиот тип на извори на податоци. Доколку ги разгледуваме одговорите според категоријата на испитаници, може да се забележи дека припадниците на безбедносните и разузнавачките служби, кои најмногу од сите категории на испитаници се среќаваат со изворите на податоци, ќе забележиме дека затворените извори значително предничат во релевантност пред отворените извори на податоци, односно огромен дел од

испитаниците од оваа целна група сметаат дека затворените извори даваат порелевантни податоци. При разговорот со неколку од испитаниците, тие истакнаа дека ова се должи на големата употреба на дезинформациите и пропагандата која е вплеткана во отворените извори, и за чие остстранување и изолирање на објективноста во еден податок е потребен огромен ангажман и губење ресурси.

7.1.9. Методи на прибирање податоци

При прибирањето на податоци, субјектите кои го вршат тоа прибирање (конституенсите на безбедносниот сектор) имаат на располагање најразлични начини и методи за стигнување до нови податоци. За успешно да се исполни потребата од одреден тип на податоци кои се безбедносно интересни, исклучително важно е планирањето на начинот на кој може да се дојде до тие податоци, односно како може тие податоци да се приберат. Во зависност од тоа дали податоците се прибираат од отворени или од затворени извори, се избираат и методите кои ќе се користат за прибирање на тие податоци. Нормално, методите кои се користат за прибирање податоци од затворени извори имаат поспецифична природа и соодветно на своите карактеристики поставуваат многу поголеми побарувања пред институциите од безбедносниот сектор кои ги користат ваквите методи.

Во спроведеното емпириско истражување, со замисла да им се даде на испитаниците повеќе простор да ги искажат своите ставови, им беше поставено прашњето „ *Кои методи на прибирање податоци Ви се најпознати?*“. Ова е едно од прашањата на кои не беа понудени структурирани одговори, па затоа не треба да зачудува широчината на одговорите кои беа добиени. Варијациите на одговорите во голема мера зависи од професионалната насоченост на испитаникот, па така категоријата на испитаници кои работат или порано работеле во оперативните сектори на безбедносните и разузнавачките служби и испитаниците кои работат во Министерството за внатрешни работи беа во можност да дадат многу подетални одговори на ова прашања за разлика од другите категории на испитаници. Меѓутоа, како општ заклучок при прегледувањето на одговорите, може да се каже дека голем број испитаници прават дистинкција и им се јасни разликите помеѓу техничките начини/методи за прибирање податоци и класичните конспиративни методи кои вклучуваат користење на човечки извори. Исто така, најголемиот број од испитаниците

го идентификуваат и методот на прибирање на податоци од отворени извори, со кој се добро запознаени, заради огромните можности кои ги дава денешницата во поглед на неговото користење.

7.1.10. Можноста за прибирање податоци преку дипломатско-конзуларните претставништва

Разузнавачката компонента во составот на функцијата на дипломатскиот претставник отсекогаш имала значајна улога, а една од основните цели е оперативно покривање и разузнавачко истражување на државата, регионот и важните стратегиски области. Основната задача на разузнавачката дејност и на дипломатијата е да се залагаат да ја заштитат својата држава од изненадувања, при што собираат прецизни и точни податоци за постојниот или потенцијалниот противник, како и за остварување услови за инфилтрација на домашниот капитал во странските држави. Тие собираат, анализираат и испраќаат назад во својата држава податоци од политичка, економска, воена, културолошка и од друга природа за животот во државата во која се распоредени. Но, бидејќи најважните податоци се по правило добро чувани и заштитени, дипломатијата е во тесна врска со разузнавачката дејност. Официјалните активности на дипломатско-конзуларните претставништва на државата, кои со оглед на поголемиот степен на безбедност, привилегии и имунитет, како и сигурната комуникација со централата во својата матична земја, несомнено даваат многу поволни можности за прибирање корисни податоци за државата на прием.

На поставеното прашање „*Дали сметате дека дипломатско-конзуларните претставништва даваат добри можности за прибирање на податоци кои се важни за безбедносниот сектор?* “, испитаниците дадоа мошне интересни одговори.

Од извршената анализа, може да се забележи дека мислењата по ова прашање беа поделени. Од голема помош при елаборацијата на ова прашање беа испитаниците кои во текот на кариерата имале можност да работат во дипломатско-конзуларните претставништва на Република Македонија во други држави, како и ставовите на оние испитаници од разузнавачките и безбедносните органи за Република Македонија кои работеле на полето на спротивставување на разузнавачката дејност на дипломатско-конзуларните претставништва на други држави акредитирани во Република Македонија. И покрај тоа што некои од испитаниците се согласуваа со погоре

наведените тврдења дека имунитетот и комуникацијата значат многу и дека преку персонални контакти може да се добијат многу податоци, сепак одреден број испитаници сметаат дека во денешнава разузузнавачка и контраразузнавачка практика, токму странските амбасади и конзулати се првите мети за набљудување на домашните безбедносни и контраразузнавачки органи.

7.1.11. Техничките дисциплини за прибирање податоци наспроти класичните конспиративни методи за прибирање податоци

Методот на прибирање податоци со користење технички средства подразбира користење различни технички направи со чија помош може да се дојде до посакуваните податоци. Постои широк дијапазон на технички направи кои може да се користат при примената на овој метод. Тоа можат да бидат различни модели на направи за аудио и видео снимање, разни видови камери и фотоапарати, направи за привлекување и снимање на електромагнетни зрачења, разни видови радари и радарски апарати, направи за аерофото и сателитско снимање, компјутерски програми за пробивање на заштита на компјутерски системи и сл. Во денешниве услови на унапредување на техниката и информациско-комуникациското поле, експоненцијално се зголемуваат и можностите за користење на технички средства за прибирање податоци.

По еден подолг период на интензивна употреба на техничките средства за прибирање податоци, во последните години може да се забележи едно постојано доближување и поинтензивна примена на тајното користење на човечки извори за *доаѓање до корисни информации на сметка на употребата на техничките средства за* прибирање на информации.

Прашањето кое беше поставено во овој контекст беше *„Дали сметате дека техничките дисциплини за прибирање податоци во целост ќе ги заменат класичните конспиративни методи за прибирање, како на пример прибирањето податоци со користење на човечки извори?“*. Ова прашање е горлива и постојано обработувана тема во светските академски и практични разузнавачки кругови, и претставува една точка на судир помеѓу постарите и поновите поимања за прибирање разузнавачки податоци, ги подели и испитаниците на ова истражување. Помеѓу нив има испитаници кои цврсто тврдат дека не постои замена за човекот како извор на најчувствителните

податоци и дека само со човечко толкување и интеракција може да се дознаат потребните податоци. Од друга страна, еден дел од испитаниците тврдеа дека техничките дисциплини за прибирање податоци се унапредени до толкава мера што можат сами по себе да ги доловат потребните податоци. По однос на ова прашање, треба да се напомене и дека еден дел од испитаниците, нешто повеќе од 20 испитаници се изјаснија дека не знаат да дадат одговор на ова прашање.

7.1.12. Потребата од заштита на изворите на податоци и на методите на работа на безбедносните служби

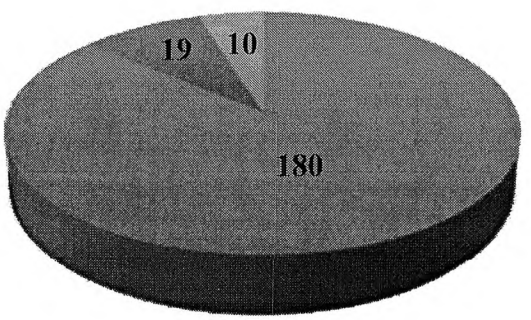
Заштитата на изворите на податоците и методите на прибирање на тие податоци е една многу неопходна активност, со цел да се заштити непречено функционирање и понатамошно успешно информирање. Впрочем, ако се земе предвид дека дури и одредени професии кои не се занимаваат со безбедност (на пример, новинарството) внимаваат да не ги компромитираат своите извори, дури и повеќе од јасно е дека при својата работа безбедносните служби ќе направат сè што е во нивна можност да ги заштитат своите извори и да осигураат дека не постои никаков ризик од нивно компромитирање. Компромитирањето на одреден извор на податоци, на пример инфилтриран припадник на служба во криминална или терористичка група, или врбуван агент на противничка служба, може да има и кобни последици за изворот. Компромитирањето пак на методите преку кои безбедносната служба доаѓа до одредени податоци може да значи моментално оневозможување на понатамошен пристап (на пример следење на комуникации), или пак уште полошо, пласирање на лажни и фиктивни информации.

Во однос на тоа како се размслува на оваа тема, на испитаниците им бепе поставен следното прашање *„Дали сметате дека заштитата на изворите на податоци и на методите на работа на безбедносните служби е значаен фактор?“*. Одговорите на ова прашање во извршеното истражување демонстрираат цврста убеденост кај испитаниците дека заштитата на изворите на податоците е неопходно и е еден од најзначајните фактори за континуираната информираност. Ова особено е изразено кај оние испитаници кои користат најразлични методи при својата работа, како припадниците на МВР и на разузнавачките и безбедносните служби, а со оваа констатација се согласува и експертската заедница.

7.1.13. Евалуација на веродостојноста на прибраните податоци

На прибраните податоци мора да им се направи евалуација со цел да се одреди нивната релевантност, веродостојноста на изворот и точноста на информацијата. Ваквата евалуација вклучува низа на различни постапки за валидирање на нивната вредност. Мора да се одреди дали податоците се релевантни во однос на предметот на интерес, дали има потреба од такви податоци и дали имаат одредена вредност во моментот. Објективното и совесно приоѓање при оценувањето на податоците е неопходно, бидејќи секоја лоша процена во оваа фаза ќе има негативни импликации врз точната интерпретација на конечната информација[171]. По успешната верификација на податоците, потоа следува нивно подредување и поврзување со претходно добиените податоци кои се однесуваат на конкретен предмет.

Околу прашањето *„Дали сметате дека е потребно да се направи евалуација на веродостојноста на прибраните податоци?“* не постои никаква поделеност помеѓу размислувањата на анкетираните лица, бидејќи евалуацијата на прибраните податоци се наметнува сама по себе како природна активност, бидејќи дури и во најсекојдневните ситуации со кои се среќаваме сакаме да дејствуваме врз основа на претходно проверени податоци (избор на маркет, избор на возило и сл.).



Одговор под а) Потребно е да се направи евалуација
Одговор под б) Не е потребно е да се направи евалуација
Одговор под в) Не знам

[171] Баткоски, Томе – *„Разузнавачка и безбедносно-контраразузнавачка тактика“,Скопје, 2008,* стр.129

Ако ја земеме во фокус специфичната средина во која дејствуваат безбедносните институции, и во која најчесто лажните информации, пропагандата и различните интереси се секојдневие, евалуацијата на прибраните податоци се чини дека е понеопходна од кога било во историјата. Со оваа констатација се согласуваат најголем дел од испитаниците, а значително за одговорите е што имаат висок процент на позитивен одговор низ сите категории на испитаници.

7.1.14. Аналитичката обработка на прибраните податоци

Анализата на податоците е процесот кој треба да даде комплетен опис за предметот кој се истражува, притоа земајќи ги предвид сите релевантни варијабли и преку интерпретација на значењето и ефектите на неговите засебни елементи. Ова е процес кој не ветува непогрешливост, меѓутоа врши пополнување на голем број празнини во знаењето за одреден предмет на интерес и ја намалува несигурноста при донесувањето одлуки поврзани со тој предмет. Целта на анализата е да им помогне на крајните корисници во проширувањето на нивните знаења за одреден предмет на интерес и неговите карактеристики. Правилниот начин да се карактеризира анализата е како еден тип на прогноза, поткрепена со експлицитни факти и веројатни претпоставки, која ќе ги претставува оформените ставови и убедувања на аналитичарот кој ја изработил.

Бидејќи прашањето *„До кој степен сметате дека е важна аналитичката обработка на прибраните податоци за квалитетот на конечната информација?“* во истражувањето е формулирано на начин што им дава на испитаниците да даваат одговор според своја сопствена процена, токму затоа и ширината на добиените одговори е прилично голема. Меѓутоа, на втор поглед може да се забележи дека одговорите на испитаниците одат во една слична насока, а тоа е дека анализата на прибраните податоци има голема улога за квалитетот на конечната информација. Степенот на важност што ѝ се придава на аналитичката обработка зависи од профилот на испитаникот, односно од извршените разговори со неколку испитаници кои имаат работно искуство токму во аналитичките сектори на безбедносно-разузнавачките служби, може да се забележат нивните ставови дека анализата има круцијална важност, додека некои други испитаници не ѝ даваат толку големо значење. Како и да е,

заклучок е дека испитаниците ја сметаат аналитичката обработка за многу важен дел и дека таа дефинитивно има влијание врз квалитетот на конечната информација.

7.1.15. Дисеминација на информациите

За да може една информација да го достигне својот полн капацитет, неопходно е да се изврши нејзина ефективна дисеминација. Дисеминацијата претставува одлучување за тоа на кого ќе му се достави одредена информација. Без соодветна дисеминација, голем дел од вредноста на информацијата се губи. Потребно е да се направи прецизна процена за тоа на кого ќе му биде доставена одредена информација и да се осигура дека одредена информација ќе стигне кај оние лица кои имаат вистинска потреба и овластувања да ја добијат таа информација, и да донесуваат одлуки врз основа на неа.

Тука се наметнува прашањето *„Дали се согласувате со тврдењето дека без правилна дисеминација на конечната информација, голем дел од нејзината вредност може да се изгуби?“*. Она што може да се забележи од добиените одговори на прашањето за дисеминацијата во истражувањето, е дека поголемиот број испитаници сметаат дека неправилната дисеминација на конечната информација може да придонесе кон губењето на вредноста на информацијата. Од извршените неколку разговори со лица кои работат токму на работни места каде што се врши дисеминацијата, беа добиени мислења дека правилната дисеминација всушност треба да осигура дека информацијата ќе се достави навреме во вистинските раце, односно до оние лица кои најефективно ќе ја искористат таа информација за да ја донесат вистинската одлука (ова може да бидат донесувачите на одлуки во државата, но може да биде и оперативецот кој се наоѓа на терен подготвен да преземе одредена акција).

7.1.16. Важноста на повратната врска (фидбекот)

Донесувачите на одлуки мора да ги знаат приоритетите кои бараат континуирано унапредување, и токму затоа е потребен регуларен и константен дијалог со безбедносниот сектор. Тие мора активно да се вклучат во процесот и да имаат

реални очекувања за тоа колку една информација може да придонесе во нивната работа. Многу е важно да се избалансира односот помеѓу изготвувачите на информацијата и крајниот корисник. И двете страни мора да ги разберат комплексните параметри на оваа врска и да го пронајдат вистинскиот начин за изградба на конструктивна соработка.

Фазата на доставување на информацијата на крајните корисници треба да биде проследена со дијалог помеѓу изготвувачот на информацијата и крајниот корисник. Изготвувачите на информацијата имаат потреба од добивање повратна врска од крајните корисници, со цел да дознаат дали информацијата им била од корист и дали се задоволни од начинот на кој е презентирана таа информација. Ова се прави за да можат изготвувачите да ја унапредат својата работа во иднина и да подготвуваат информации кои во целост ќе ги задоволат потребите на крајните корисници. Повратната врска помеѓу корисникот и изготвувачот треба да даде одговор на прашањата за употребливоста, релевантноста и навременоста на доставената информација. Добрата комуникација во поглед на овие прашања ќе придонесе кон порефинирани информации, нивна поголема употреба од страна на корисниците и унапредување и зајакнување на повратната врска.

За да се согледа каков е ставот на испитаниците за фидбекот, им беше поставено следното прашање *„Дали сметате дека повратната врска (фидбекот) и дијалогот помеѓу крајните корисници на информацијата и оние кои ја изготвуваат информацијата е важен елемент за ефикасното искористување на информацијата?“*. Резултатите покажуваат дека три четвртини од испитаниците сметаа дека фид-бекот, односно постоењето добра комуникација помеѓу создавачот на информацијата и крајниот корисник придонесува кон поефикасно искористување на таа информација. Создавачите треба да знаат да ги приспособат своите анализи и предлози според очекувањата на крајните корисници, а такво нешто е многу тешко изводливо без добивањето повратна реакција од корисниците. Добриот дијалог помеѓу двете страни може само да придонесе кон поефективна соработка и непогрешливи одлуки. Ваквите тврдења беа особено забележливи во одговорите на оние институции кои имаат аналитички компоненти, значи испитаниците кои доаѓаа од Министертвото за одбрана, од Министерството за внатрешни работи и од разузнавачко-безбедносните служби.

7.1.17. Споделување информации во безбедносниот сектор

Споделувањето информации и координацијата помеѓу институциите се од големо значење за формирањето на сеопфатни и практични пристапи и решенија за справување со безбедносни закани, и е од голема помош за вработените во безбедносните институции при проучувањето на овие закани, како и развивањето соодветни технички и организациони решенија за нивна превенција и справување со нив. На пример, поседувањето информации за одредена закана или настан со кој веќе била соочена друга институција од безбедносниот сектор овозможува да се идентификуваат нејзините појавни облици, да се разбере ризикот што го претставува таа закана и да се одредат превентивните мерки кои ќе се применат.

Несомнено е дека споделувањето информации помеѓу институциите кои го сочинуваат безбедносниот сектор ќе придонесе кон зголемувањето на ефективноста, како на секоја институција посебно, така и на целиот безбедносен фактор како целина. Во истражувањето, особено интересни беа ставовите по прашањето „ *Дали сметате дека споделувањето информации помеѓу институциите кои се дел од безбедносниот сектор ќе придонесе за зголемување на ефикасноста во нивната работа?*“. Како што може да се забележи од одговорите на испитаниците, нивните ставови се поделени во однос на ова прашање, што претставува изненадувачки резултат, имајќи предвид дека во светски рамки многу се работи за унапредување на полето на споделување информации (како на национално, така и на билатерално и на мултилатерално ниво), па некои држави имаат дури и донесени стратегии за споделување информации. Она што можеби може да ги објасни ваквите одговори, се присутните препреки за споделување кои претходно беа обработени, како и недостатокот на дефинитивна платформа (модел) за споделување. Она што охрабрува е што поголем дел од експертската јавност смета дека споделувањето ќе придонесе кон поефикасна работа на безбедносниот сектор, па тоа дава надеж дека со подлабоко проучување на оваа тема ќе се зголеми и свесноста кај безбедносните институции.

7.1.18. Придобивки и ризици од споделувањето информации

Споделените информации може да имаат одлучувачко влијание врз перспективите на донесувачите на одлуки во поглед на проблемите со кои се соочуваат

и одлуките кои ги донесуваат. Можеби најголемата придобивка од споделувањето за оној што ги прима информациите е здобивањето со ново знаење кое е од големо значење за него, а тоа знаење не можело да се добие на друг начин по прифатлива цена. Од друга страна, стојат ризиците кои ги носи споделувањето информации. Неовластеното објавување на споделените информации, споделувањето со трета страна, споделувањето нерелевантни или лажни информации, се само дел од ризиците при споделувањето информации.

Токму затоа, интересно беше да се споредат одговорите на испитаниците на прашањето *„Дали сметате дека придобивките од споделувањето информации ги надминуваат ризиците кои произлегуваат од овој тип на соработка?“*. Слично како и по прашањето за ефикасноста на споделувањето информации, ставовите на испитаниците се разликуваат и во поглед на судирот помеѓу придобивките и ризиците од споделувањето. Од структурата на одговорите се гледа дека размислувањата на испитаниците се поделени и спротивни едни на други При разговорот со неколку испитаници, беа презентирани силни аргументи и искуства кои одат во прилог како на придобивките, така и во однос на ризиците. Одговорите на ова прашање се индикатор дека треба внимателно да му се пристапи на ова прашање, и да се работи во насока на намалување на безбедносните ризици кои произлегуваат од споделување информации, со што би се зголемиле придобивките од споделувањето.

7.1.19. Препреки за споделување информации

И покрај напорите да се воспостави успешно споделување информации, се чини дека овие напори се соочуваат со тешкотии и препреки. Идентификација на тие препреки и нивното проучување и разбирање е првиот чекор кој ќе придонесе кон формирањето на стратегија и преземањето на постапки за нивното надминување. Овие препреки имаат влијание врз споделувањето и индивидуално и колективно, и секоја категорија има посебни карактеристики.

Прашањето *„Што според Вас ја претставува најголемата бариера за споделувањето информации?“*, е често пати поставувано и се водени бројни дискусии. По однос на ова прашање кај анкетираните лица имаше одредена дилема. Но, сепак треба да се констатира дека доминантен (околу 2/3 од анкетираните лица се одлучиле

за оваа опција) е одговорот дека недостатокот на доверба помеѓу страните кои треба да разменат информации се наметнува како главна препрека за споделување.

При анализата на резултатите треба да се напомене дека имаше дилема при изборот на одговор, па затоа можноста за кратка дискусија и давање на свое сопствено мислење беше добродојдено. Имено, претставници од сите категории испитаници истакнаа дека комбинацијата од сите овие препреки можеби е вистинскиот одговор на ова прашање.

Неколку експерти нагласија дека не би било на одмет да почне да се размислува за пронаоѓање законски или подзаконски решенија како да се регулира споделувањето, и да се направи една компаративна анализа како тоа е решено во земјите во регионот и во светот. Дел од испитаниците од министерствата и од безбедносно-разузнавачките служби главно ја посочија компетитивноста помеѓу институциите кои работат на исти или слични полиња на интерес, потоа цврстите ставови за несподелување информации на раководните лица во институциите, а еден одговор ги посочи и нарушените персонални односи помеѓу колегите од разни институции.

7.1.20. Споделување информации помеѓу безбедносниот сектор и приватниот сектор

Споделувањето информации помеѓу државните органи и приватниот сектор е многу моќен механизам за подобро разбирање на константно променливата безбедносна средина и разбирање на сериозните ризици, ранливости и закани, како и пронаоѓањето решенија за нив. Ова партнерство функционира преку споделувањето информации за сајбер напади, справување со природни катастрофи и физички закани. Поттик за ова споделување треба да претставуваат предностите со кои ќе се стекнат учесниците преку соработката во однос на заедничките проблеми.

Она што одговорите на прашањето *„Дали сметате дека треба да се споделуваат информации помеѓу безбедносниот сектор и приватниот сектор?“* во истражувањето недвосмислено го потврдуваат е дека е застапен ставот за партнерство, односно соработка на полето на споделување информации помеѓу приватниот и безбедносниот сектор и е многу задоволителен ако се има предвид дека и практичарите и експертите се согласуваат дека партнерство мора да постои, а имаше и голем број неодлучни одговори. Дискусијата главно се однесуваше на потребата за заеднички

одговор кон кога заканите кои постојано се зголемуваат и се приспособуваат на условите, потоа на неопходноста на заштитата на критичната инфраструктура, која во најголем дел се наоѓа во сопственост на приватниот сектор, како и постојаната потреба на двете страни да располагаат со информациите кои им се потребни, со цел да бидат поефективни и поекономични во извршувањето на своите активности. Критичната структура беше спомената во неколку дискусии и добро е што во отсуство на законска регулатива која ја регулира критичната инфраструктура, сепак таа се смета за една од областите за која е неопходна заштита од безбедносен аспект. Во дискусијата беше напоменато и дека е потребен еден отворен пристап кон оваа активност и дека ваквата практика на споделување информации треба да зачести и да се применува постојано кога за тоа има потреба.

7.1.21. Споделување информации со други држави

Успешното споделување информации на национално ниво треба да води кон поширока соработка и развивање на процесот на споделување информации на билатерално и на мултилатерално ниво. Ова партнерство треба да се развива на тактичко и стратегиско ниво преку споделувањето информации кои се однесуваат на безбедносни инциденти, слабости и ранливости на системот, безбедносни закани и мерки и активности кои треба да се преземат. Слично како и во процесот на споделување информации внатре во безбедносниот сектор на една држава, и во споделувањето информации со други држави се појавуваат неколку препреки или опасности кои имаат одлучувачко влијание врз исходот на споделувањето.

По однос на споделувањето информации со други држави во истражувањето, испитаниците дадоа скоро изедначени одговори на прашањето *„Која е најголемата опасност при споделувањето информации со други држави?“*, бидејќи секој од понудените одговори се чини како вистинскиот. Дискусијата која следеше при изборот на отворената опција исто така не смее да се занемари. Во дискусијата имаше тврдење дека секоја од понудените опции е опасност сама по себе, но најчесто сите овие опасности се испреплетуваат и можат да се пронајдат заедно. Споделувањето со други држави е секогаш чувствителна работа, и изборот дали да се сподели или не, треба внимателно да се направи. Имаше и коментари дека ако има ситуација во која се надзира комбинација од сите три ризици, тогаш да се „игра на сигурно“ и да се донесе

одлука да не се споделат информациите. Меѓутоа, имаше и такви испитаници кои во својата кариера работеле на позиции каде што биле надлежни за остварување на меѓународна соработка со други држави (дипломати, офицери за врска и сл.), и во чијшто делокруг на работа, меѓу другото, било вклучено и споделувањето информации, и кои се изјаснија дека споделувањето со други држави е исклучително корисна работа и во неколку случаи се покажало како незаменливо.

7.1.22. Споделување информации во безбедносните институциите

Безбедносниот сектор мора да им обезбеди максимална достапност и пристап на своите компоненти до сите информации кои се однесуваат на националната безбедност. За да се оствари тој пристап до што повеќе информации, потребно е да се усвојат конзистентни практики за пристап, да се воспостават унифицирани стандарди за безбедност на информациите и различните институции да бидат подготвени да се вклучат во процесот на споделување. Веродостојноста на информациите кои се споделуваат, степенот на меѓусебна доверба помеѓу институциите кои споделуваат информации, мерките и активностите за заштита на информациите и начинот на кој ќе бидат употребени информациите се есенцијалните елементи на воспоставувањето на околина на доверба.

Прашањето во истражувањето кое се однесуваше на споделувањето информации во безбедносните институции, можеше да биде одговорено само од оние лица што се запознаени со процесот на споделување во институциите од кои доаѓаат, и мора да се напомене дека заради полесна илустрација, пресметани се само одговорите на испитаниците кои работат во институции во кои има воспоставено процедури за споделување. Начинот на кој беше поставено прашањето „*Како ја оценувате моменталната ситуација во однос на споделувањето информации во Вашата институција?*“, се однесуваше само за оние испитаници кои се вработени во институции во кои има воспоставени практики за споделување. Не треба да се заборави и дека во овие одговори може да постои некој промил на грешка, затоа што според принципот „потребно е да знае“, вработените во една институција немаат целосен преглед во однос на тоа дали нивната институција споделува информации и до кој степен е тоа споделување. Сепак, од анализа на одговорите може да се види дека проценатa е дека постои некое средно ниво на споделување, а низ разговорот со

испитаниците вработени во Министерството за одбрана, во Министерството за внатрешни работи и во разузнавачките и безбедносните служби беше истакнато дека постои меѓуресорска координација и дека се организираат редовни средби на кои се споделуваат информации.

7.1.23. Ограничување одредени информации од слободна циркулација во јавност

Ограничувањето на најчувствителните информации од слободна циркулација во јавноста го овозможува поефективното искористување на тие информации и ја намалува можноста тие информации да завршат во погрешни раце или да станат јавно достапни во момент што може да ја наруши или да предизвика штета на работата на безбедносниот сектор или општеството како целина. Ваквото ограничување најчесто се врши со класифицирање на информацијата со одреден степен на класификација. Имплементацијата на конзистентни методи за класификација на информациите овозможува нивно безбедно користење, како и примена на одредени мерки и активности кои треба да ја заштитат таа информација од неовластен пристап или неовластено објавување во јавност. Степенот на класификација го означува релативното значење што го има таа информација во однос на националната безбедност и ги одредува специфичните безбедносни побарувања за нејзина заштита. Во принцип, информациите се заштитуваат пропорционално со нивната вредност и чувствителност.

Ако се земат предвид горенаведените критериуми, ќе се дојде до заклучок дека донесувањето одлука за класифицирање на една информација не е воопшто лесна работа. Со цел да се согледаат предностите и недостатоците на клсифицирање на одредени информации, беше поставено прашањето *„Дали сметате дека е потребно одредени информации да се ограничат од слободна циркулација во јавноста?“*. Бидејќи ова не е една егзактна постапка за која има прецизни и унифицирани насоки кои се применуваат автоматски, таа бара донесување субјективни одлуки од оние што ја одредуваат класификацијата. Со ова тврдење се согласуваат и поголемиот број од анкетираните лица, а некои од нив се изјаснија дека не само што таквото ограничување е потребно, туку во одредени случаи треба да биде и задолжително. Интересно е што во направените разговори со лица кои припаѓаат на различни категории на испитаници со кои беше направено истражувањето, неколку пати беше напоменато дека

ограничувањето/класификацијата мора да биде објективна, и дека ова ограничување не смее да се однесува на информации кои покажуваат злоупотреба, криминални дејства или други противзаконски активности. Неколку испитаници укажаа дека во денешно време, мало пребарување може да резултира со пристап до компромитирани класифицирани информации по медиумите кои ѝ се достапни на целокупната јавност.

7.1.24. Евалуација на потребата за задржување на степенот на класификација

Кога се врши класификацијата на информацијата, доколку е возможно, создавачот треба да одреди временски период за кој таа информација ќе биде класифицирана, и кој треба да биде одреден врз основа на проценатa за времетраењето на чувствителноста на информацијата. Ова носи со себе и одреден ризик, бидејќи доколку времетраењето на класификацијата се покаже како прекратко, со нејзиното предвремено објавување во јавност може да се уништат сите придобивки кои се постигнале со нејзиното класифицирање, и да дојде до настанување на првично одредената штета. Токму затоа, создавачот мора да биде внимателен при одредувањето на рокот за декласификација и да земе предвид многу фактори. Можеби како најпрактична опција е на одредени временски интервали да се прави одредена ре-евалуација на потребата за задржување на степенот на класификација, која може да резултира со непроменливост на степенот, рекласификација (намалување или зголемување на степенот на класификација) или декласификација на информацијата (симнување на степенот на класификација).

Преку систематизацијата на одговорите на поставеното прашање *„Дали сметате дека е потребно на одредени периоди да се направи евалуација на потребата за задржување на степенот на класификација на одредена информација?“* целта е да се согледаат ставовите на испитаниците. Со ставот дека има потреба на одредени периоди да се направи реевалуација на степенот на класификација на информацијата се согласуваат поголемиот дел од испитаниците, кое се од различни категории на испитаници. Имено, имаше и неколку тврдења од испитаниците кои не се согласуваа дека треба се прави реевалуација дека ако еднаш се класифицирала, таа треба да остане класифицирана сè додека не помине првичниот временски рок кој е одреден за нејзина класификација и создавачот не одлучи да ги извести сите корисници дека таа веќе не е класифицирана. Но, аргументите кои беа изнесени во корист на потребата за

реевалуација беа дека такво нешто е потребно, бидејќи може веќе настанот заради кој е класифицирана информацијата одамна да завршил или веќе не е чувствителен, па да продолжи да се држи во тајност, или дека создавачот веќе не може да се пронајде (нема правен наследник), или дека едноставно она на што се однесува информацијата веќе станало општо познат факт во јавноста преку други извори. Исто така, неколку од испитаниците кои доаѓаат од експертската јавност посочија дека на светско, а и на локално ниво се донесуваат законски регулативи кои им гарантираат на граѓаните пристап до информации кои тие треба да ги знаат.

7.1.25. Важноста на безбедносниот сертификат

За да не настанат одредени нарушувања на безбедноста на класифицираните информации, се преземаат одредени мерки и активности од доменот на персоналната безбедност кои за своја примарна цел имаат да обезбедат дека само лица кои се безбедносно проверени и за кои не постои сомневање дека можат да ја нарушат безбедноста на информациите имаат пристап до нив. За да се исполни оваа цел и за да се намали ризикот од неовластено објавување мора да се преземат сите разумни и соодветни активности, кои ќе осигураат дека само лица кои ги исполнуваат условите за добивање безбедносен сертификат ќе имаат пристап до класифицирани информации.

За да се одреди односот на испитаниците кон безбедносниот сертификат, беше поставено следното прашање *„Дали сметате дека безбедносните сертификати имаат улога во однос на безбедното и одговорното ракување со класифицираните информации?“*. Бидејќи потребата од безбедносен сертификат во последниве неколку години е постојано истакнувана и веќе станува секојдневие во работата на безбедносниот сектор и правосудните органи, не треба да изненадува фактот што добар дел од испитаниците сметаат дека тој има улога во однос на безбедносното и одговорното ракување со класифицираните информации. Ова тврдење особено се потврди при разговорите што беа водени со неколку припадници на безбедносни институции во кои безбедносниот сертификат е еден од основните услови при самото вработување (на пример Дирекцијата за безбедност на класифицирани информации). Убедливиот потврден одговор за улогата на безбедносниот сертификат кај оваа категорија само го потврдува неговото значење, а големо значење на безбедносниот сертификат му даваат и испитаниците кои доаѓаат од министерствата и од експертската

јавност, како и колегите студенти на II и III циклус студии (од кои добар дел и се вработени по безбедносните институции).

7.1.26. Влијанието на сајбер-заканите врз безбедноста на класифицираните информации

Со развојот на информатичката технологија и нејзината сè поголема употреба во активностите наменети за заштита на националната безбедност, мора да се воспостават процедури и насоки како нивното користење да биде безбедно и практично. Прашањето *„Дали сметате дека со развојот на информатичката технологија се зголемуваат сајбер заканите за безбедноста на класифицираните информации?“* е често апстрахирано во последниот период во безбедносните кругови.

Ставовите на испитаниците по однос на ова прашање беа прилично воедначени, затоа што денешниот свет ја диктира потребата сите безбедносни институции голем дел од својата работа да ја извршуваат и да ја насочуваат кон полето на сајберот. Најголемиот дел од нив сметаат дека постојаниот развој на информатичката технологија ги зголемува безбедносните закани и постојано се отвораат нови фронтови во сајбер просторот, што ги вклучува и заканите кон безбедноста на класифицираните информации. По однос на ова прашање имаше и многу неодлучни одговори, бидејќи испитаниците веројатно немале доволно познавање на оваа материја.

Особено интересни видици понудија испитаниците кои се вработени во секторите во кои најмногу внимание се посветува на сајбер просторот, компјутерскиот криминал, информатичката безбедност и сл., кои со стопроцентна сигурност даваа позитивен одговор на поставеното прашање. Некои од нив дури и посочија на постојните законски и подзаконски директиви според кои процесирањето на класифицирани информации на компјутерско-информатички системи кои се поврзани на Интернет е забрането.

7.1.27. Уништување класифицирани информации

Класифицираните информации кои се одредени за уништување треба да се уништат на начин што ќе оневозможи нивна реконструкција и повторно користење. Методите и опремата кои најчесто се користат за уништување класифицирани информации вклучуваат: палење, сечење или хемиска декомпозиција.

Токму овие најчесто користени методи беа понудени како алтернативни одговори на прашањето *„Кој е најсоодветниот начин за уништување на класифицирани информации кој ќе оневозможи нивно понатамошно користење?“.*

Поголемиот дел од испитаниците го застапуваат тврдењето дека палењето на документите е најбезбедниот начин за уништување на класифицираните информации и дека на тој начин е невозможна нивна повторна репродукција. Корисно за истражувањето е што беше направен разговор со лица кои биле директно вклучени во процесот на уништување на класифицирани информации, како претставници на комисиите за уништување. Во дискусијата некои од нив посочија дека за палење најдобри се индустриските печки кои се наоѓаат во некои од поголемите компании од металната индустрија или од компаниите кои работат со уништување ѓубре. Еден дел од испитаниците и сечењето (шредирањето) го сметаат за прифатлив метод, но притоа имаше коментари дека мора да се користат шредери со одредени спецификации, кои ги сечат документите на толку мали парчиња што е скоро невозможно да се состават. Хемиската декомпозиција ја избраа како опција многу мал број испитаници, а интересно е што како дискусија имаше предлози дека комбинација од сечење и палење е најсигурен метод.

7.1.28. Нарушување на безбедноста на класифицирана информација

Нарушувањето на безбедноста на класифицираните информации настанува кога до информацијата е остварен пристап од лице кое нема овластување да ја добие таа информација. Во ваков случај, најчесто лицето нема безбедносен сертификат или не го исполнува принципот „потребно е да знае“. Задолжително е секое нарушување (или основано сомнение за нарушување) на безбедноста на информациите да се пријави и да се истражи колку што е можно побрзо, со цел да се одреди потенцијалната штета од тоа нарушување и да се одредат корективните и дисциплинските мерки кои треба да се

преземат. По утврденото нарушување, се одлучува за потребата од преземање дејства за утврдување на степенот на нарушување на безбедноста на класифицираната информација. Утврдување на степенот на нарушување на безбедноста на класифицираната информација треба да се спроведува од страна на експерти со професионално безбедносно и истражно искуство, кои се независни од лицата непосредно поврзани со настанатото нарушување на безбедноста на класифицираните информации.

При анализата на одговорите на ова прашање во истражувањето мора да се напомене дека и покрај изедначеноста на одговорите, ова прашање предизвика многу диксусија од страна на испитаниците. Бидејќи форматот на прашањето „*Според вас, по настанатото нарушување на безбедноста на класифицираната информација, која од наведените активности треба најпрво да се преземе со цел да се минимизира степенот на евентуалната штета?*“ им овозможуваше да испитаниците да изберат од неколку понудени одговори. И покрај тоа што секој даде свое мислење за тоа која постапка ја смета за приоритетна, постоеше една усогласеност во однос на ставот дека сите овие постапки се исклучително важни при справувањето со безбедносните нарушувања и дека можеби најдобар пристап би бил тие да се преземат истовремено и координирано. При разговорите со неколку испитаници кои доаѓаат од институции кои имале искуство со нарушена безбедност на класифицирани информации (поради професионалност и непристрасност, овде нема да биде напоменато кои се тие институции), тие потврдија дека ваквата ситуација е многу непријатна, но дека веднаш се пристапило кон преземање на активности кои ќе ја намалат штетата од тоа нарушување, кои ги вклучуваат сите погоре наведени постапки кои се понудени како можен одговор.

7.1.29. Заштита на класифицираните информации во безбедносните институции

Заштитата на класифицираните информации е многу сложен предизвик, бидејќи заканите и ризиците за нивно компромитирање продолжуваат да се зголемуваат, и стануваат многу поконкретни и пософистицирани.

Информациите мора да се заштитат од голем број закани кои доколку се манифестираат ќе резултираат со губење, неовластен пристап, неовластено објавување или промена на содржината на информациите. Заканите за кои зборуваме можат да се манифестираат преку ненамерни грешки и невнимателност на лицата кои ракуваат со нив, шпионски активности, неовластен упад во информатички систем и сл. Сите мерки и активности кои се преземаат за заштита на информациите имаат за цел да го заштитат интегритетот и чувствителноста на информациите.

Бидејќи прашањето *„Како ја оценувате моменталната ситуација во однос на заштитата на класифицираните информации во Вашата институција?“* се однесува само на испитаниците кои работат во институции каде што се ракува со класифицирани информации, при анализата на одговорите се пресметани само тие категории на испитаници. Ставот на секој испитаник по ова прашање е субјективен и е од негова лична перспектива, но сепак како ориентир при проценатa треба да биде земена важечката законска регулатива која се однесува на заштитата на класифицираните информации. Ова е земено како ориентир, бидејќи потребно е сите корисници при добивањето на безбедносниот сертификат и пред добивањето на каква било класифицирана информација, да се брифираат за нивните обврски и должности кои треба да придонесат за заштитата на таа информација. Токму заради ова, одговорите на поставеното прашање треба да се прифатат со доверба и треба да се валоризираат, затоа што испитаниците се доволно компетентни да го проценат нивото на заштита. Анализата на одговорите укажува дека на класифицираните информации им се пристапува со големо внимание, особено во оние институции каде што тие се секојдневен дел од работата, и нивото на нивна заштита се движи во рамките од напредно до целосна заштита на класифицираните информации.

ЗАКЛУЧОК

Со помош на теоретската дескрипција на информациите и информирањето, како и со емпириското истражување, беше потврдена општата хипотеза дека информациите кои се користат во безбедносниот сектор и нивната ефективна обработка и анализа имаат директно влијание врз планирањето на активностите кои се преземаат со цел одржување на внатрешната и на надворешната безбедност на Република Македонија. Покрај општата, беа потврдени и помошните хипотези кои тврдеа дека:

- безбедносниот сектор на Република Македонија има постојана потреба од прилив на нови информации кои се однесуваат на неговиот делокруг на работа.;
- поседувањето на потребните информации ќе има директно влијание врз адекватните постапки кои ги преземаат припадниците на безбедносниот сектор и раководните органи кои донесуваат одлуки врз основа на тие информации.;
- со постојаното усовршување на методите за прибирање на нови информации се зголемува и приливот на информации кои можат да бидат корисни за безбедносниот сектор на Република Македонија.;
- успешната заштита на безбедносните информации е во директна корелација со нивното ефективно искористување.;
- со зголемувањето на безбедносната култура на лицата кои ракуваат со информациите од безбедносен карактер, се зголемува и шансата за оптимално искористување на тие информации.

Со потврдувањето на општата и помошните хипотези, како е преку научно-стручната анализа што произлезе од емпириското истражување, на крај може да се направи и едно целосно сублимирање кое ќе ги претставува и генералните заклучоци од истражувањето, кои ги опфаќаат сите сегменти кои беа истражувани со оваа докторска дисертација.

Со сигурност можеме да тврдиме дека брзиот општествен, научен, културен и технички развој доведува до нови побарувања кои ја наметнуваат потребата од што повеќе податоци, кои ќе опфаќаат што поголем дијапазон на области. Фокусот на безбедносниот сектор треба да се насочи кон прибирањето податоци кои можат да ни

ги откријат плановите, намерите и можностите на потенцијалните нарушувачи на националната безбедноста на Република Македонија и кои ќе ја претставуваат основата за одлучување и преземање одредени акции.

Бидејќи информацијата го претставува знаењето со коешто сме се стекнале преку логичката интеграција и интерпретација на прибраните податоци и врз основа на неа може да се донесуваат одлуки базирани на нејзините постулати и тврдења, како заклучок може да се каже дека информирањето претставува процесирање на информации помеѓу две страни, при што едната страна пренесува одредено знаење, а другата страна се здобива со проширување на своите знаења за одреден предмет или состојба. Информирањето е неопходно за да се оствари успех во работата во оние професии или области кои се поврзани со користење информации.

Со цел да се заштитат интересите и вредностите на Република Македонија, како и нејзината внатрешна и надворешна безбедност од можните рапидни промени на светско, регионално или локално рамниште во иднина, раководните и безбедносните органи на државата мора постојано да добиваат благовремени и соодветни информации кои се неопходни за успешно водење на сите витални државни функции. Република Македонија треба да биде насочена кон изградување безбедносен сектор што ќе биде погоден, ефикасен и компатибилен до таа мера што секој граѓанин којшто е дел од заедницата ќе се чувствува сигурен, обезбеден и слободен во остварувањето на своите права и интереси загарантирани со Уставот, законите и голем број меѓународни документи. Целта на овој сектор е да ја отстрани загрозеноста што му се заканува на општеството и на неговите составни делови и да овозможи остварување на интересите на поединците како и заштитување на нивните основни слободи и права што им се гарантирани со голем број меѓународни документи, преку ефикасно, брзо и навремено реагирање во сложени безбедносни ситуации.

Пред конституентите на безбедносниот сектор постојано се поставуваат нови очекувања и одговорности со цел заштита на националната безбедност на Република Македонија од сите видови внатрешни и надворешни закани. Како последица на овој тренд од круцијално значење е постојаното унапредување на безбедносниот сектор преку воведување нови иницијативи, усовршување и осовременување на веќе воспоставените методи и практики, воведување нови методи на работа, постојано следење на начините на функционирање на безбедносните сектори на другите држави, како на регионално така и на глобално ниво, а секако и преземање искуства кои се докажале како ефективни.

Резултатите од истражувањето појаснуваат дека планирањето на работата во безбедносниот сектор мора да врши ефикасно и објективно, и треба треба да ги земе предвид брзите промени во развојот, нестабилноста и динамичноста на настаните во околината (односно окружувањето, како сложен и комплексен услов за дејствување), да тежнее кон поефективно искористување на расположливите ресурси и да ги избере најпогодните постапки и методи со кои треба да се остварат целите во неизвесната иднина. Планирањето успешно се остварува само ако се заснова на соодветни информации. Ако не се располага со бројни и сигурни информации, не е можно да се спроведе анализа на работењето во претходниот период, да се предвиди иднината, да се оствари процесот на планирање. Информациите и информирањето овозможуваат да се конципираат што поквалитетни плански одлуки.

Истражувањето покажа дека процесот на прибирање, обработка и дистрибуција на точни, навремени и релевантни податоци кои можат да бидат претворени во информација не се случува сам по себе, туку е точно утврден циклус, кој е развиен на начин да претставува своевиден водич за креирањето релевантни и точни информации од брдото на податоци со кое се соочуваме. За да биде ефикасен, овој циклус мора да биде проактивен, да развива уникатни методи и принципи, и да ги доставува финалните информации навремено и конзистентно до соодветните корисници.

Анализата од одговорите од истражувањето упатува на заклучокот дека за да се одржи максимална будност, флексибилност и оперативна агресивност со цел успешно спротивставување на константната еволуција и зголемувањето на безбедносните закани и предизвици, што пак значи дека за успешно остварување на своите цели и задачи, конституентите на безбедносниот сектор на Република Македонија мора да прибираат, да оценуваат и да анализираат информации кои се поврзани со националната безбедност. Секој конституент на безбедносниот сектор на Република Македонија, без разлика на неговата големина, мора да поседува капацитет за да ги разбере детално импликациите кои се однесуваат на прибирањето податоци, нивната анализа и споделувањето на конечната информација, како и мерките и активностите за нивна заштита од неовластено објавување.

За да се обезбедат потребната ефикасност, економичност и навремена адаптација на променливите потреби, неопходно е сите прибрани податоци, континуирано и навремено да се обработуваат со цел да се подготви информација која ќе се достави до државните раководни органи, кои врз основа на таа информација ќе најдат начин да се одговори на современите барања на државата за поддршка на нејзината политика и за

целосна заштита на нејзините витални национални цели и интереси. На секоја информација мора да ѝ биде проценета релевантноста и веродостојноста со цел да се одреди колку може да придонесе кон разбирањето и наоѓањето начини за превенирање или сузбивање одредена безбедносна закана. Кога ќе се одреди колку е значајна таа информација, врз основа на нејзината релевантност и материјалност, треба да се направи процена за нејзиниот придонес кон процесот на менаџирање со безбедносната закана.

Оваа научно-стручна анализа супстанцијално посочува дека безбедносниот сектор на Република Македонија мора да работи во насока на развивање на своите капацитети за користење отворени извори. Слично како и за другите методи на прибирање податоци, потребно е да се вложи многу работа и ресурси за да се формира една компетентна структура за прибирање податоци од отворени извори, бидејќи тие претставуваат значаен ресурс кој мора да биде инкорпориран во работата на безбедносниот сектор. Соработката и координацијата помеѓу институциите во безбедносниот сектор се од големо значење за формирањето сеопфатни и практични пристапи и решенија за справување со безбедносни закани, и е од голема помош за вработените во безбедносните институции при проучувањето на овие закани, како и развивањето на соодветни технички и организациони решенија за нивна превенција и справување со нив. Споделувањето информации е критично за остварувањето на целите на безбедносниот сектор на Република Македонија и успехот во неговата работа зависи од воспоставувањето на ефикасни системи и процеси кои ќе помогнат во споделувањето на информациите, развивањето на стратегија за надминување на сите бариери кои го спречуваат споделувањето информации, и пронаоѓањето начин да се воспостави модел кој ќе овозможи ефективна соработка и доверба помеѓу неговите компоненти. Споделувањето информации помеѓу државните органи и приватниот сектор е многу моќен механизам за подобро разбирање на константно променливата безбедносна средина и разбирање на сериозните ризици, ранливости и закани, како и пронаоѓањето решенија за нив. Ова партнерство функционира преку споделувањето информации за сајбер напади, справување со природни катастрофи и физички закани.

Мора да се обрати поголемо внимание и на обуката на припадниците на безбедносните институции, со цел формирање квалитетен кадар што ќе поседува капацитет да се справува ефикасно и квалитетно со работните задачи кои ќе се постават пред него (особено во делот на јазичната обука, безбедносната култура, проактивноста и сл.). Вработените во безбедносните институции треба да бидат

професионалци кои се одлично обучени и имаат детални и сеопфатни познавања за полето кое го работат и да поседуваат висок степен на аналитичка подготвеност, индивидуални квалитети, висок степен на образование и широки познавања од различни области.

Интересна и индикативно позитивна линеарност беше најдена во односот помеѓу заштитата на информациите и нивната употребливост во безбедносниот сектор. Информациите мора да се заштитат од голем број закани кои доколку се манифестираат ќе резултираат со губење, неовластен пристап, неовластено објавување или промена на содржината на информациите. Заштитата на класифицираните информации е многу сложен предизвик, бидејќи заканите и ризиците за нивно компромитирање продолжуваат да се зголемуваат и стануваат многу поконкретни и пософистицирани. Информациите се заштитуваат пропорционално со нивната вредност и чувствителност. Сите мерки и активности кои се преземаат за да се заштити една информација се одредуваат врз основа на нејзиниот степен на класификација, кој го диктира изборот и имплементацијата на адекватните безбедносни мерки и активности. Степенот на класификација го означува релативното значење што го има една информација во однос на националната безбедност и ги одредува специфичните безбедносни побарувања за нејзина заштита. Институциите од безбедносниот сектор мора постојано да ги разгледуваат, да ги оценуваат и да ги модификуваат стратегиите за заштита на информациите како одговор на променливата природа на ризиците со кои се соочени. Тие треба да дојдат до решенија со кои ефективно ќе ги спречат заканите, како и да изработат планови како да ги заштитат своите најслаби точки. Притоа, секоја од институциите мора да ги земе предвид сопствените уникатни потреби, организационата култура, своите интереси и приоритети, како и своите буџетски ограничувања.

Градењето безбедносна свест и подигнувањето на безбедносната култура кај вработените во институциите на безбедносниот сектор во иднина мора да се сфати многу посериозно. Институциите мора да бидат свесни и да ја разберат потребата за заштита на информациите со кои работат. Сите вработени мора да бидат свесни за ризиците кои можат да ја нарушат безбедноста на информацијата и да ги познаваат процедурите и стратегиите за заштита на тие информации, соодветно на нивните работни места и одговорности.

Прилог бр.1 - Анкетен прашалник

Имајќи го во предвид фактот дека ниту едно научно истражување не може да биде комплетно или пак сеопфатно без примената на истражувачките техники, овој анкетен прашалник го претставува истражувачкиот инструмент за доаѓањето на сознанија за улогата на информациите и информирањето во работата на припадниците на безбедносниот сектор. Целта на овој прашалник е да се оствари еден краток увид во ставовите на експертите и на вработените во областа на безбедноста и разузнавањето, кои претставуваат луѓе кои се доволно практично и теоретски потковани за да дадат одговор на клучните прашања од оваа тематика.

Заради специфичноста на полето на истражувањето, а со тоа и на природата на прашањата од кои е составен овој анкетен прашалник, анкетирањето ќе се спроведе анонимно. На почетокот на прашалникот се наоѓаат неколку прашања кои се однесуваат на општиот профил на испитаниците, со цел да им се даде кредибилитет на прашањата од главниот дел на прашалникот и да се има претстава каков кадар се анкетира. Се надевам дека прашањата ќе ги задоволат очекувањата на испитаниците, бидејќи ги опфаќаат есенцијалните елементи кои се однесуваат на информациите кои се користат во работата на безбедносниот сектор.

Општи прашања за испитаникот:	
Ве молам, наведете ја Вашата возраст: **а)** од 20 до 30 години **б)** од 31 до 40 години **в)** од 41 до 50 години **г)** над 50 години	**Ве молам, наведете го Вашиот степен на образование:** **а)** средно образование **б)** високо образование **в)** магистер **г)** доктор на науки
Колку време сте (или сте биле) вработени во институција од безбедносен карактер? **а)** до 5 години **б)** од 5 до 10 години **в)** повеќе од 10 години **г)** немам работено во безбедносна институција	

Дел 1: Информациите и безбедносниот сектор		
	Прашање:	**Одговор:**
1.1	Дали сметате дека информациите и информирањето се доволно истражени во домашната научна теорија?	**а)** ДА **б)** НЕ **в)** НЕ ЗНАМ
1.2	Дали сметате дека информирањето е важен предуслов за ефикасното функционирање на безбедносните институции?	**а)** ДА **б)** НЕ **в)** НЕ ЗНАМ
1.3	Дали сметате дека планирањето е ефикасна алатка во менаџирањето на работата на безбедносниот сектор?	**а)** ДА **б)** НЕ **в)** НЕ ЗНАМ
1.4	Дали се согласувате дека активностите на безбедносниот сектор треба да бидат насочени кон превенирањето на безбедносните закани, односно справување со нив пред тие да успеат да ги манифестираат своите општествено негативни последици?	**а)** ДА **б)** НЕ **в)** НЕ ЗНАМ

1.5	На каков начин сметате дека информациите придонесуваат во работата на безбедносниот сектор? *Ве замолувам за кратка дискусија во поглед на Вашето мислење.*	
1.6	Според Вас, какви ефекти може да предизвика имањето/немањето на навремени и точни информации врз работата на безбедносниот сектор? *Ве замолувам за кратка дискусија во поглед на Вашето мислење.*	
1.7	Дали сметате дека на информациониот циклус му е посветено доволно внимание во безбедносната теорија и практика?	**а)** ДА **б)** НЕ **в)** НЕ ЗНАМ

1.8	Според Вас, која од фазите на информациониот циклус има најголемо значење? *Ве замолувам за кратка дискусија во поглед на Вашиот избор.*	**а)** планирање и насочување **б)** прибирање на податоците **в)** обработка и анализа на податоците **г)** изработка на информацијата и дисеминација до крајните корисници
1.9	Според Вас, кој од понудените е порелевантниот извор за добивање на податоци?	**а)** Отворен извор **б)** Затворен извор **в)** НЕ ЗНАМ
1.10	Кои методи на прибирање податоци Ви се најпознати? *Ве замолувам за кратка дискусија во поглед на Вашето мислење.*	
1.11	Дали сметате дека дипломатско-конзуларните претставништва даваат добри можности за прибирање на податоци кои се важни за безбедносниот сектор?	**а)** ДА **б)** НЕ **в)** НЕ ЗНАМ
1.12	Дали сметате дека техничките дисциплини за прибирање податоци во целост ќе ги заменат класичните конспиративни методи за прибирање, како на пример прибирањето податоци со користење на човечки извори?	**а)** ДА **б)** НЕ **в)** НЕ ЗНАМ
1.13	Дали сметате дека заштитата на изворите на податоци и на методите на работа на безбедносните служби е значаен фактор?	**а)** ДА **б)** НЕ **в)** НЕ ЗНАМ

1.14	Дали сметате дека е потребно да се направи евалуација на веродостојноста на прибраните податоци?	**а)** ДА **б)** НЕ **в)** НЕ ЗНАМ
1.15	До кој степен сметате дека е важна аналитичката обработка на прибраните податоци за квалитетот на конечната информација?	**а)** Нема никаква важност **б)** Има мала важност **в)** Има средна важност **г)** Има голема важност **д)** Има круцијална важност
1.16	Дали се согласувате со тврдењето дека без правилна дисеминација на конечната информација, голем дел од нејзината вредност може да се изгуби.	**а)** ДА **б)** НЕ **в)** НЕ ЗНАМ
1.17	Дали сметате дека повратната врска (фидбекот) и дијалогот помеѓу крајните корисници на информацијата и оние кои ја изготвуваат информацијата е важен елемент за ефикасното искористување на информацијата?	**а)** ДА **б)** НЕ **в)** НЕ ЗНАМ

Дел 2: Споделување на информациите

	Прашање:	**Одговор:**
2.1	Дали сметате дека споделувањето информации помеѓу институциите кои се дел од безбедносниот сектор ќе придонесе за зголемување на ефикасноста во нивната работа?	**а)** ДА **б)** НЕ **в)** НЕ ЗНАМ

2.2	Дали сметате дека придобивките од споделувањето информации ги надминуваат ризиците кои произлегуваат од овој тип на соработка?	**а)** ДА **б)** НЕ **в)** НЕ ЗНАМ
2.3	Што според Вас ја претставува најголемата бариера за споделувањето информации? *(Доколку Вашиот одговор го нема во понудените опции, наведете го во продолжение, под г))*	**а)** Недовербата помеѓу учесниците во споделувањето **б)** Недостатокот на технички решенија кои ќе го овозможат споделувањето **в)** Непостоењето на законска регулатива за споделување информации **г)**
2.4	Дали сметате дека треба да се споделуваат информации помеѓу безбедносниот сектор и приватниот сектор? *Ве замолувам за кратка дискусија во поглед на Вашиот избор.*	**а)** ДА **б)** НЕ **в)** НЕ ЗНАМ

2.5	Која е најголемата опасност при споделувањето информации со други држави? *(Доколку Вашиот одговор го нема во понудените опции, наведете го во продолжение, под г))*	**а)** Споделување на добиените информации со трета страна. **б)** Споделување на неквалитетни, неточни или фабрикувани информации **в)** Нарушување на безбедноста на споделените информации **г)**
2.6	Како ја оценувате моменталната ситуација во однос на споделувањето информации во Вашата институција? *(ова прашање важи само за оние испитаници кои се вработени во институции во кои има воспоставени практики за споделување)*	**а)** Нема никакво споделување **б)** Почетно ниво на споделување **в)** Средно ниво на споделување **г)** Напредно ниво на споделување

Дел 3 – Заштита на информациите

	Прашање:	**Одговор:**
3.1	Дали сметате дека е потребно одредени информации да се ограничат од слободна циркулација во јавноста?	**а)** ДА **б)** НЕ **в)** НЕ ЗНАМ

3.2	Дали сметате дека е потребно на одредени периоди да се направи евалуација на потребата за задржување на степенот на класификација на одредена информација?	**а)** ДА **б)** НЕ **в)** НЕ ЗНАМ
3.3	Дали сметате дека безбедносните сертификати имаат улога во однос на безбедното и одговорното ракување со класифицираните информации?	**а)** ДА **б)** НЕ **в)** НЕ ЗНАМ
3.4	Дали сметате дека со развојот на информатичката технологија се зголемуваат сајбер заканите за безбедноста на класифицираните информации?	**а)** ДА **б)** НЕ **в)** НЕ ЗНАМ
3.5	Кој е најсоодветниот начин за уништување на класифицирани информации кој ќе оневозможи нивно понатамошно користење? *(доколку Вашиот одговор го нема во понудените опции, наведете го во продолжение, под г))*	**а)** Палење **б)** Сечење **в)** Хемиска декомпозиција **г)**

3.6	Според вас, по настанатото нарушување на безбедноста на класифицираната информација, која од наведените активности треба најпрво да се преземе со цел да се минимизира степенот на евентуалната штета?	**а)** Известување на создавачот за настанатото нарушување **б)** Изработка на процена на штета **в)** Преиспитување на потребата за понатамошна класификација на компромитираната информација **г)** Процена дали истрагата за нарушувањето ќе направи дополнителна штета
3.7	Како ја оценувате моменталната ситуација во однос на заштитата на класифицираните информации во Вашата институција? *(ова прашање важи само за оние испитаници кои се вработени во институции во кои се ракува со класифицирани информации)*	**а)** Нема никаква заштита **б)** Почетно ниво на заштита **в)** Средно ниво на заштита **г)** Напредно ниво на заштита **д)** Целосна заштита

БИБЛИОГРАФИЈА

1. *„ACP 122(E), Information Assurance For Allied Communications And Information Systems"* - The Combined Communications Electronics Board (CCEB), 2004
2. *„Analyst Toolbox – A Toolbox for the Intelligence Analyst"* – U.S. Department of Justice's Global Justice Information Sharing Initiative Intelligence Working Group, 2006
3. *„An introduction to TEMPEST"* - SANS Institute IFOSEC Reading Room, SANS Institute, 2014
4. Бакрески Оливер - *„Координација на безбедносната заедница во Република Македонија"*, Скопје, 2005
5. Бакрески, Оливер – *„Планирањето како функција на безбедносниот менаџмент"*, Научна Конференција MILCON' 12, Скопје, 2012, стр.51-56
6. Бакрески Оливер и Милошевиќ Милан - *„Современи безбедносни системи"*, Скопје, 2010
7. Barrett Michael – *„The Need for Intelligence-Led Policing"*, DomPrep Journal Online Edition, 2006
8. Best A. Richard Jr. – *„Intelligence Information: Need-to-Know vs. Need-to-Share"*, Congressional Research Service (CRS) Report for Congress, US, 2011
9. Bolz Frank Jr, Dudonis J. Kenneth and Schulz P. David - *„The Counterterrorism Handbook – Tactics, Procedures and Techniques"*, Boca Raton, 2002
10. *„Bringing Intelligence About: Practitioners Reflect on Best Practitioners,,* – Center for Strategic Intelligence Research, Joint Military Intelligence College, 2003
11. Буџаковски, Стефан – *„Разузнавање - контраразузнавање, деловно бизнис разузнавање, безбедносни системи"* , Охрид, 2005
12. Carter L. David - *„Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies"*, Michigan, 2006
13. *„Communications and Information - Emission Security Countermeasures Reviews"*, Air Force Manual 33-214, Volume 2, 2011
14. *„C-M(2002)49 - Security Within The North Atlantic Treaty Organisation" - North Atlantic Treaty Organization (NATO) – NATO HQ Brussels, 2002*
15. *„Contemporary Challenges for the Intelligence Community"* - Geneva Center for the Democratic Control of Armed Forces (DCAF), Geneva, Switzerland, 2006
16. Cooper R. Jeffrey - *„Curing Analytic Pathologies: Pathways to Improved Intelligence Analysis"*, Center for the Study of Intelligence, Washington DC, 2005
17. *„Criminal Intelligence File Guidelines"* – Law Enforcement Intelligence Unit, http://www.leiuhomepage.org [03.12.2013]
18. Dacey F. Robert and Hite C. Randolph - *„Homeland Security:Information Sharing Responsibilities, Challenges, and Key Management Issues"*, Testimony Before the Committee on Government Reform, House of Representatives, Washington, 2003
19. Davis G. B. and Olson, M. H. - *„Management Information Systems:Conceptual Foundations, Structure, and Development*", McGraw-Hill, New York, 1985
20. Dearth H. Douglas - *„National Intelligence: Profession and Process"*, Joint Military Intelligence Training Center, Washington DC, 1995

21. European Network and Information Security Agency (ENISA) – *„Incentives and Challenges for Information Sharing in the Context of Network and Information Security"*, Heraklion, Greece, 2010
22. Faibisoff G. Sylvia and Ely P. Donald - *„Information and Information Needs"*, Commissioned Papers Project, Teachers College, Columbia University, US
23. Floridi Luciano - *„Is Semantic Information Meaningful Data?"*, Philosophy and Phenomenological Research Vol. LXX, No. 2,Wolfson College, 2005
24. *„FMI 2-22.9 - Open Source Intelligence"* - Headquarters Department of the Army, Washington DC, 2006
25. Ford A. Christopher - *„Relations between Intelligence Analysts and Policymakers: Lessons of Iraq"*, Hudson Institute, Washington, 2005
26. Gackowski J. Zbigniew - *„Subjectivity Dispelled: Physical Views of Information and Informing"*, Informing Science: the International Journal of an Emerging Transdiscipline Vol.13, California, 2010
27. Gackowski J. Zbigniew - *„Subjectivity Dispelled: Physical Views of Information and Informing"*, Informing Science: the International Journal of an Emerging Transdiscipline Vol.13, California, 2010
28. Gackowski J. Zbigniew - *„Informing for operations – The first Principia"*, Issues in Informing Science and Information Technology, Vol.5, California, 2008
29. Gackowski J. Zbigniew - *„Quality of Informing – Bias and Disinformation Philosophical Background and Roots"*, Issues in Informing Science and Information Technology, Vol.3, California, 2006
30. Gackowski J. Zbigniew - *„Informing as a discipline – An initial proposal"*, Issues in Informing Science and Information Technology, Vol.13, California, 2010
31. Gackowski J. Zbigniew - *„Focus and Perspectivism in viewing Information, Data and Informing: Fundamental Distinctions"*, Issues in Informing Science and Information Technology, Vol.15, California, 2012
32. Gackowski J. Zbigniew - *„Subjectivity Dispelled: Physical Views of Information and Informing"*, Informing Science: the International Journal of an Emerging Transdiscipline Vol.13, California, 2010
33. Garst D. Ronald - *„Components of Intelligence"*, A Handbook of Intelligence Analysis, Defense Intelligence College, Washington DC,1989
34. *„Good Practice Guide – Network Security Information Exchanges"* - European Network and Information Security Agency (ENISA), Heraklion, Greece, 2009
35. Гоцевски, Трајан – *„Основите на одбранбено-заштитниот систем на Република Македонија"*, Кочани, 1995
36. Hadžić Miroslav & Švarm Filip - *„Priručnik sa pojmovnikom za novinare - bezbednosna pitanja"*, Beograd, 2005
37. Heuer J. Richards Jr. - *„Psychology of Intelligence Analysis"* – Center for the Study of Intelligence, Central Intelligence Agency, 1999
38. Horić Andrea - *„Informacija – Povijest jednog pojma - O Capurrovom razumijevanju pojma informacije"*, Zagreb, 2007
39. *„Intelligence products and dissemination"*- Standing Operating Procedure, Ohio Military Reserve Headquarters, Ohio, 1998
40. *„Information Sharing Strategy"* - United States Intelligence Community , Office of the Director of National Intelligence, Washington DC, 2008
41. *„Information Sharing - The Federal Government Needs to Establish Policies and Processes for Sharing Terrorism-Related and Sensitive but Unclassified Information"* - United States Government Accountability Office (GAO), Report to Congressional Requesters, Washington DC, 2006

42. Israel David and Perry John - *„What is Information?"*, Information, Language and Cognition, Vancouver, 1990
43. Knox T. Karl - *„The various and conflicting notions of Information"*, Issues in Informing Science and Information Technology, Vol.4, California, 2007
44. Котовчевски Митко – „Национална безбедност на Република Македонија", Скопје, 2000
45. Krizan Lisa - *„Intelligence essentials for everyone"*, Joint Military Intelligence College, Washington DC, 1999
46. Lahneman J. William - *„The Future of Intelligence Analysis"*, Center for International and Security Studies at Maryland, Maryland, 2006
47. Lerner, K. Lee and Lerner Wilmoth Brenda – *„Encyclopedia of Espionage, Intelligence and Security"*, Farmington Hills MI, 2004
48. Losee M. Robert - *„A Discipline Independent Definition of Information"* – Journal of the American Society for Information Science 48, Chappel Hill, 1998
49. Margolis Gabriel – *„ The Lack of HUMINT: A Recurring Intelligence Problem"*, Global Security Studies 2013, Volume 4, Wilmington NC, 2013
50. McDowell Don - *„Stretegic Intelligence & Analysis – Guidelines on Methodology & Application"*, The Intelligence Study Centre, 1997
51. Metscher Robert and Gilbride Brion - *„Intelligence as an Investigative Function"*, International Foundation for Protection Officers, 2005
52. Moore T. David - *„Critical Thinking and Intelligence Analysis"* – Center for Strategic Intelligence Research, National Defense Intelligence College, Washington DC, 2007
53. Нацев Александар – *„Безбедносните аспекти од развојот на општеството"*, Четврта Меѓународна Научна Конференција, Европски Универзитет на РМ, 2014
54. Нацев Александар – *„Непосреден контакт со агентот"*, Годишник на Факултетот за безбедност, Скопје, 2010
55. *„National Criminal Intelligence Sharing Plan - Solutions and approaches for a cohesive plan to improve our nation's ability to develop and share criminal intelligence"* - U.S. Department of Justice's Global Justice Information Sharing Initiative, Washington DC, 2003
56. *„National Information Sharing Strategy"* – The Federal Bureau Of Investigation, 2011
57. Nemfakos Charles, Rostker D. Bernard *et all- „Workforce Planning in the Intelligence Community - A Retrospective"* – RAND National Security Research Division, Santa Monica, 2013
58. *„Open Source Intelligence Handbook"*- North Atlantic Treaty Organization, Brussels, 2001
59. *„Operations Security – Intelligence Threat Handbook"* – The Interagency OPSEC Support Staff, Greenbelt MD, 1996
60. Pallaris Chris – *„OpenSource Intelligence: A Strategic Enabler of National Security"*, CSS Analyses in Security Policy, Zurich, 2008
61. Pfeifer W. Joseph – *„Network Fusion: Information and Intelligence Sharing for a Networked World"*, Homeland Security Affairs, Vol.8, US, 2012
62. *„Protecting against terrorism"* – Centre for the Protection of National Infrastrucutre (CPNI), London, 2010
63. Quist S. Arwin – *„Security Classification of Information, Volume 2. Principles for Classification of Information"*,Oak Ridge K-25 Site, Oak Ridge National Laboratory, Tennessee, 1993

64. Randol A. Mark - *„Homeland Security Intelligence: Perceptions, Statutory Definitions and Approaches"*, Congressional Research Service, 2009
65. Sales Alexander, Nathan – *„Share and Share Alike: Intelligence Agencies and Information Sharing"*, The George Washington Law Review, Vol.7, 2010
66. Спасески Јордан – *„Безбедносни Ситеми - Прилог кон учењето за безбедносните системи"*, Скопје, 2010
67. Стаменковски Алекса - *„Основи на разузнавањето"*, Скопје, 1999
68. Стаменковски Алекса - *„Планирање на одбраната"*, НИП Ѓурѓа, Скопје, 1996
69. *„Strategic Intent for Information Sharing 2011-2015"* - United States Intelligence Community, Office of the Director of National Intelligence, Washington DC
70. *„The Federal Bureau of Investigation's Efforts to Improve the Sharing of Intelligence and Other Information* U.S. Department of Justice Office of the Inspector General Audit Division", Audit Report 04-10, 2003
71. *„The Need to Share: The U.S. Intelligence Community and Law Enforcement"*, AFCEA Intelligence Committee White Paper, US, 2007
72. Treglia, Joseph – *„Three Essays on Law Enforcement and Emergency Response Information Sharing and Collaboration: An Insider Perspective"*, Dissertation, Syracuse University Surface, New York, 2013
73. Treverton F. Gregory, Gabbard C. Bryan - *„Assessing the Tradecraft of Intelligence Analysis"* – RAND National Security Research Division, Santa Monica, 2008
74. Treverton Gregory – *„Reshaping National Intelligence for an Age of Information"*, Cambridge, Cambridge University Press, 2001
75. Walsh Igoe James – *„Defection and Hierarchy in International Intelligence Sharing"*, Cambridge University Press, UK, 2007
76. Walsh Igoe James – *„Intelligence Sharing in the European Union – Institutions are not enough"*, JCMS, Vol.44, No.3, 2006
77. Цуклески Гоце - *„Прирачник за соработничка мрежа"*, Скопје, 2005
78. Шуклев, Бобек – *„Менаџмент"*, Економски Факултет, Скопје, 1998

НОРМАТИВНИ АКТИ И ДРУГИ МАТЕРИЈАЛИ

1. Закон за класифицирани информации, „Службен весник на Република Македонија бр.9/04„ од 27.02.2004 година
2. Law of the People's Republic of China on Guarding State Secrets – „14th Session of the Standing Committee of the 11th National People's Congress“, 29.04.2010
3. Security of Information Act Consolidation, Canadian Ministry of Justice, 24.03.2011
4. „Executive Order 13526 - Classified National Security Information“, Memorandum of December 29, 2009, White House
5. 2001/264/EC – Security Regulations Of The Council Of The European Union, EU Council Decision of 19 March 2001
6. Уредба за безбедност на лица корисници на класифицирани информации, „Службен весник на Република Македонија бр.82/04“ од 19.11.2004 година
7. Уредба за административна безбедност на класифицирани информации, „Службен весник на Република Македонија бр.82/04“ од 19.11.2004 година
8. Уредба за физичка безбедност на класифицирани информации, „Службен весник на Република Македонија бр.82/04“ од 19.11.2004 година
9. Уредба за информатичка безбедност на класифицирани информации, „Службен весник на Република Македонија бр.16/05“ од 11.03.2005 година
10. AC/35-D/2001-REV2 - NATO Security Committee Directive on Physical Security, 07.01.2008
11. AC/35-D/2000-REV6 - NATO Security Committee Directive on Personnel Security, 08.09.2009
12. AC/35-D/2002-REV3 - NATO Security Committee Directive on the Security of Information, 06.12.2006
13. AC/35-D/2004-REV2 - NATO Security Committee Primary Directive on INFOSEC, 06.12.2006
14. „5210.50 - Directive on Unauthorized Disclosure of Classified Information to the Public“, US Department of Defense, 22.07.2005
15. „Government Security Classifications – Version 1.0“, UK Cabinet Office, October 2013
16. „Information Security Management Guidelines - Protectively marking and handling sensitive and security classified information“ – Australian Government, 21.06.2011

ИНТЕРНЕТ СТРАНИЦИ

1. www.afio.com
2. www.bbc.co.uk
3. www.bmi.bund.de
4. www.cia.gov
5. www.crs.gov
6. www.dbki.gov.mk
7. www.dni.gov
8. www.domesticpreparedness.com
9. www.enisa.europa.eu
10. www.fas.org
11. www.fbi.gov
12. www.foreignaffairs.org
13. www.ftp.fas.org/irp
14. www.gcsp.ch
15. www.gov.uk
16. www.hudson.org
17. www.humanrights.ucdavis.edu
18. www.iar-gwu.org
19. www.insaonline.org
20. www.ippr.org
21. www.justice.gov.uk
22. www.leiuhomepage.org
23. www.ncs.gov
24. www.nsa.gov
25. www.rand.org
26. www.scholarcommons.usf.edu
27. www.stimson.org
28. www.timesonline.co.uk
29. www.washingtonpost.com