ЗБОРНИК НА ТРУДОВИ ОД
ЧЕТВРТАТА МЕЃУНАРОДНА НАУЧНА
И СТРУЧНА КОНФЕРЕНЦИЈА

на тема:

ИНТЕГРИРАНА КОРПОРАТИВНА БЕЗБЕДНОСТ И ДИГИТАЛНИТЕ ТРАНСФОРМАЦИИ - ПРЕДИЗВИК ЗА АКАДЕМСКАТА ЗАЕДНИЦА И МОДЕРНИТЕ КОРПОРАЦИИ

СКОПЈЕ, 2018

ЗБОРНИК НА ТРУДОВИ ОД ЧЕТВРТАТА МЕЃУНАРОДНА НАУЧНА И СТРУЧНА КОНФЕРЕНЦИЈА

на тема:

ИНТЕГРИРАНА КОРПОРАТИВНА БЕЗБЕДНОСТ И ДИГИТАЛНИТЕ ТРАНСФОРМАЦИИ- ПРЕДИЗВИК ЗА АКАДЕМСКАТА ЗАЕДНИЦА И МОДЕРНИТЕ КОРПОРАЦИИ

СКОПЈЕ, 2018

СОДРЖИНА:

Проф. д-р Атанас Козарев, Декан на Факултетот за детективи и криминалистика
Д-р Алексеј Сопронов, Скопје
Бујар Дулови, студент на последипломски студии на Факултетот за детективи и криминалистика
Ајрулау Дулови, студент на последипломски студии на Факултетот за детективи и криминалистика

Еколошкиот криминалитет и корпоративната безбедност во Република Македонија

Апстракт:

Заштитата на животната средина е регулирана со Уставот на Република Македонија, вклучително и со закони од општиот правен поредок, но и одделни lex specialis закони. Во овие до-кументи се имплментирани и меѓународни декларации, резолуции, акти од европското aquis со кои се изврши хармони-зација на македонското национално законодавство. Меѓутоа и покрај тоа, нашата држава не е имуна од еколошкиот криминалитет и закани. Современите компании во желбата да остварат профит и да ги задоволат апетитите на нивните сопственици не ги превземаат потребните активности за еколошка заштита. Еколошкиот криминалитет се манифестира со посебна етиологија и феноменологија и претставува предизвик за академската и научна јавност. Полициската дејност се појавува како репресивна и се реализира откога ќе се случи некое еколошко кривично дело или катастрофа. Еколошката безбедност претставува неопход-ност и детерминанта за создавање на здрави генерации и здраво општество. За таа цел од големо значење е развивање на еколошката свест на сите нивоа. Корпоративната безбедност како дел од безбедносни-от систем исто така својот фокус се повеќе треба да го насочува кон елиминирање на потенцијалните еколошки опасности и штети.

Клучни зборови: животна средина, криминалитет, корпоративна безбедност, заштита.

Atanas Kozarev, Ph.D., Dean of the Faculty of Detectives and Criminology
Aleksej Sopronov, Ph.D. Skopje
Bujar Dulovi, a postgraduate student at the Faculty of Detectives and Criminology
Ajrulau Dulovi, a postgraduate student at the Faculty of Detectives and Criminology

Environmental Crime and Corporate Security in the Republic of Macedonia

Abstract:

The protection of the environment is regulated by the Constitution of the Republic of Macedonia, including laws of the general legal principles, as well as separate lex specialis laws. These documents include international declarations, resolutions and

acts of the European aquis which harmonise the Macedonian national legislation. However, in spite of that, our country is not immune to environmental criminality and threats. Modern companies in the desire for profit and satisfaction of the appetites of their owners do not undertake the necessary activities for environmental protection. Environmental crime is manifested by a distinctive etiology and phenomenology and is but a challenge for the academic and scientific public. Police activity appears to be repressive and only takes place after an environmental crime or disaster occurs. Ecological safety is a necessity for the creation of healthy generations and a healthy society. For this purpose, the development of ecological awareness at all levels is of great importance. Corporate security, as a part of the security system, needs to shift its focus on eliminating potential environmental hazards and harm more often.

Key words: environment, criminality, corporate security, protection.

Вовед

Еколошките аспекти поврзани со деловното работење пара-лелно со технолошкиот развиток во последно време добиваат значителна димензија и вредност. Притоа, практиката покажу-ва дека овој актуелен проблем има две димензии: од една страна деловните правни субјекти во настојувањето да ос-тва-рат што поголем профит понекогаш настојуваат да ги зао-биколат законските стандарди и одредби со еколошки пред-знак, а од друга страна во јавноста настојуваат да прикажат дека нивните инвестиции во редуцирањето на еколошките закани придонесуваат за поголема еколошка безбедност. Крајниот резултат од оваа економско-еколошка увертира претставува финалниот резултат кој го покажуваат мерните инструменти за нивото на загаденост на животната средина и рангирањето на нашата држава според овие индикатори на регионално и глобално рамниште. Оваа прашање има своја актуелност како на национално ниво, но и пошироко, како на пример, познатиот пакет за циркуларна економија донесен од Европската унија како основа за подготовка на Закон за управување со отпадот. Поврзано со овој сегмент претставува утврдувањето на зоните од деловниот свет кои имаат влијание односно вршат притисок врз животната средина. Како што е наведено во Стратегијата за животна средина и климатски промени 2014-2020 година[1], четири сектори се посебно значајни: енергетика, транспорт, индустрија и земјоделство: енергетскиот сектор во Република Македонија има најголем придонес кон загадувањето на животната средина, затоа што околу 90% од примарната енергија се генерира од фосилни горива, главно лигнит и мазут; транспортниот сектор има негативни влијанија врз загадувањето на воздухот и климатските промени, преку емисии на одредени загадувачки супстанции од сообраќајот. На ниво на држава, сообраќајот учествува со 24% во емисиите на азотните оксиди, 345 во емисиите на јаглерод моноксид и 16% во емисиите на испарливи органски соединенија; индустријата учествува со околу 28% во вкупните годишни емисии на сулфур диоксид, околу 14% од

[1] Министерство за животна средина и просторно планирање, Стратегија за животна средина и климатски промени 2014-2020 година, Скопје, 2015 година, стр. 22, 23 и 25.

вкупните просечни годишни емисии на азотни оксиди, додека има голем удел (38%) во годишните емисии на испарливи органски соединенија и просечен удел од 60% од годишните емисии на цврсти честички; секторот земјоделство има влијане преку емисиите на амонијак во воздухот и емисии на стаклени гасови. Имено, 99% од вкупнит национални емисии на NH_3 се од секторот земјоделство и истиот е втор по големина извор на емисии на стаклениците гасови: CH_4, N_2O и CO_2. "Накратко, користењето на современите технологии особено кога се отргнуваат од контролата на човекот ја загрозуваат неговата околина и ја нарушуваат еколошката рамнотежа, а последиците можат да бидат толку сериозни што со нив се доведува во прашање и опстанокот не само на сегашните, туку и на идните генерации, односно опстанокот на човековиот род воопшто."[2]

Застапеноста на овие значајни сектори во рамките на кои функционираат бројни деловни субјекти ја потврдува тезата за реалноста од постоење на еколошки закани за безбедноста, но и за потребата од отворање на едно ново поглавје во рамките на корпоративната безбедност во кое фокусот на интерес ќе се насочи пред се јакнење на еколошката свест на сите нивоа во деловното работење. "Паралеллно со ова, мора да се има во вид и фактот дека ризиците и заканите за безбедноста и сигурноста на резидентните компании се зголемени како никогаш досега."[3] Имено, остварувањето на заштитата на животната средина треба да претставува не само гола декларација, туку и конкретна цел преку вложување на значајни финансиски средства во модернизација на производствените капацитети. Меѓутоа, без соодветен надзор и контрола како менамент функција спроведувана од страна на менаџерите за корпоративна безбедност овие цели од стратешко ниво не би се остварале доследно.

1.Кривично – правни аспекти на еколошкиот криминалитет

Материјалното казнено законодавство во нашата држава од осамостојувањето забележува континуиран реформски процес во кој покрај останатото се воведуваат и нови законски инкриминации со кои се опфаќаат кривично правни релевантни поведенија кои пред неколку децении воопшто не биле познати кај нас. Меѓутоа, криминалната практика и криминалните умови во остварувањето на својата цел не бираат средства, а уште помалку не се предомислуваат да "освојуваат" нови пространства од човековото живеење и работење. Во тој контекст посебно место имаат кривичните дела од областа на еколошкиот криминалитет во кои се групираат според исти или слични криминалистички и кривично-правни карактеристики во рамките на систематиката на посебниот дел на кривичното право, кое содржи "класификација на кривичните дела и нивно групирање во посебни групи врз основа на заеднички карактеристики. Со систематизацијата подеднакво за

[2] Сулејманов З., Македонска криминологија, Скопје, 2000 година, стр. 572.

[3] Козарев А., Приватната безбедност во Република Македонија – теоретски и институционален дизајн, Зборник на трудови од Втората меѓународна научна и стручна конференција: Општествени, економски, правни, безбедносни и социјални детерминантни за развој на корпоративната безбедност во Република Македонија, регионот и пошироко, Асоцијација за корпоративна безбедност- Скопје, 2017 година, стр. 10.

занимава и законодавството и науката. Основата за групирање на кривичните дела во поедини групи може да биде различна, како што се: објектот на заштита, дејствието на извршување, видот на последиците, својството на сторителот, својството на пасивниот субјект, видот на вина, видот на казна или некое друго заедничко обележје кое ги обединува."[4]

Кривичните дела од областа на еколошкиот криминалитет во нашиот Кривичен законик се систематизирани во Глава XXII и ја опфаќаат следните појавни облици: загадување на животната средина и природата, член 218; производство, трговија или употреба на супстанции кои ја осиромашуваат озонската обвивка, член 218-а; загадување вода за пиење, член 219; производство на штетни средства за лекување добиток или живина, член 220; несовесно укажување ветеринарна помош, член 221; пренесување заразни болести кај животниот и растителниот свет, член 222; загадување на добиточна храна или вода, член 223; уништување насади со употреба на штетна материја, член 224; узурпација на недвижности, член 225; незаконита експлоатација на минерални суровини, член 225-а; пустошење на шума, член 226; предизвикување шумски пожар, член 227; незаконит лов, член 228; неовластено ловење чување и отуѓување диви животни и птици, член 228-а; незаконит риболов, член 229; загрозување на животната средина и природата со отпад, член 230; неовластено прибавување и располагање со нуклеарни материи, член 231; неовластено производство, постапување и промет со опасни материи или штетни организми или семенски или саден материјал, член 232; убивање или уништување на заштитени видови на дива флора или фауна, член 232-а; неовластено воведување на диви видови во природата, член 232-б; неовластено тргување, увезување или превезување дива флора или фауна, член 232-в; мачење животни, член 233 и тешки дела против животната средина и природата, член 234.[5] Со измената и дополнувањето на КЗ во 2015 година[6], се врши измена во членот 231 став (1), кој гласи: Тој што со сила или закана, со извршување кривично дело или на друг начин неовластено прибавува, располага, поседува или му дава на друг нуклеарни и радиоактивни материи, неовластено презема нуклеарни уреди или нуклеарни или радиоактивни материи или уред за активирање, разградување или емитување на радиоактивни материи, ќе се казни со затвор од една до десет години. "Покрај кривичните дела од оваа глава, има и други кривични дела предвидени во други глави на Кривичниот законик, кои може да се третираат како кривични дела од областа на еколошкиот криминалитет."[7] "Еколошкиот криминалитет претставува секое постапување кое директно или индиректно е насочено кон загадување и предизвикување друг вид штета врз еколошките вредности какви што се: атмосферата, почвата, воздухот и водата или со други дејствија кои се насочени кон натрупување на цврсти отпадоци, натрупување отровни материи во храната, појава на бучава, опасноста од радиоактивни материи и сл."[8] Меѓутоа, според поновите истражувања,

[4] Јовановић Љ., и др. Кривично право посебни део, треће измењено и допуњено издање, Београд, 2004 године, стр. 20-21.
[5] Кривичен законик (пречистен текст), База на закони www.pravdiko.mk.
[6] Службен весник на РМ, бр.226 од 25.12.2015 година.
[7] Малиш-Саздовска М., Прирачник за истраги кај еколошки кривични дела, Скопје, 2013 година, стр. 9.
[8] Сулејманов З., цит. труд, стр. 573.

еколошките кривични дела се "сместени во групацијата на кривични дела од економскиот криминалитет од аспект на својствата на нивните сторители кои се од делот на одговорните лица во правните лица поради непревземање на одредени заштитни мерки во поголемите индустриски и стопански капацитети за заштита на човековата околина со одбегнување на вградување заштитни филтри за загадување на воздухот или други предвидени средства за заштита на водата, воздухот, почвата и сл."[9]

Карактеристично за кривичните дела од оваа глава е што имаат бланкетни диспозиции затоа што кај поголем број од нив дејствието на извршување опфаќа повреда на одредби кои се содржани во одделни прописи кои се однесуваат на заштитата на човековата средина и на тој начин потребно е да се знае содржината на овие прописи за да може конкретно да се утврди и содржината на конкретното дело односно забраната или наредбата кои се повредуваат од страна на сторителот.

"Општо опасната природа на овие дела, опасноста и загрозувањето на објектот на заштита во поголем обем, на пошироко подрачје и во поглеми размери, при што во законското битие на некои од кривичните дела се содржани облици на апстрактно и на конкретно загрозување и други тешки последици, како и умисленият или небрежниот облик на вината, се критериуми врз кои се установени, се систематизирани кривичните дела од оваа глава."[10] Опасноста на овие кривични дела се согледува преку нивниот конкретен појавен облик во реалноста, модус операнди системот, локус операнди системот и останатите елементи на структурата на секое конкретно еколошко кривично дело. "Посебна карактеристика на овие кривични дела е и тоа што најчесто се вршат од небрежност, меѓутоа не е исклучено и нивното вршење со умисла (на пример со евентуална умисла)."[11]

Одговорноста за извршување на еколошки кривични дела подразбира индивидуална одговорност, одговорсност на правното лице и на одговорното лице во правното лице. Оттука произлегува и улогата на корпоративната безбедност во редуцирање на условите и причините кои доведуваат до појава на еколошки кривични дела, односно превентивна димензија, но и истражување на конкретни случаи во деловниот субјект, на последиците кои настапуваат од еколошките криминални дејствија односно репресивна димензија.

2. Улогата на корпоративната безбедност во откривање на кривичните дела од областа на еколошкиот криминалитет

Корпоративната безбедност на компаниите подразбира обезбедување нивна заштита во однос на деловното работење, безбедност на човечките ресурси кои го сочинуваат јадрото еден деловен субјект, "воспоставување систем на корпоративна заштита во целната (партнерска) компанија со следните

[9] Џуклески Г., Николоска С., Економска криминалистика, Скопје 2007 година, стр. 72.
[10] Проевски Ј., Коментар на КЗ, Агенција "Академик", Скопје, 1998 година, стр. 510.
[11] Сулејманов З., цит. труд, стр. 574.

содржини: безбедносна проценка на ризикот, проектирање на оптимална организација на корпоративната заштита, проектирање на оптималните потреби на соодветна структура на стручниот безбедносен кадар, нормативно уредување на корпоративната заштита, воспоставување на функционални информациони системи и воспоставување систем на физичко-техничко и инжењерско обезбедување."[12] Имено, преку остварување на мисијата на корпоративната безбедност во суштина се остварува економска безбедност на деловното работење што подразбира и ефикасна превенција против еколошките кривични дела. Тоа се постигнува преку реализација на надлежностите на менаџерите за корпоративна безбедност кои се будно око во една компанија и даваат безбедносни услуги на различни нивоа. Корпоративните безбедносни услуги се разнолики и во нив спаѓаат следните одделни безбедносни задачи: безбедност на човечкиот капитал во деловниот субјект и поврзано со него и на пазарниот капитал, безбедност на менаџментот на деловниот субјект, на сопственичкиот капитал, безбедност на деловните информации, деловните стратегии, информатичка и индустриска безбедност. Кон овој каталог на безбедносни корпоративни надлежности може да се набројат и други кои произлегуваат од секојдневното функционирање на компаниите и безбедносните ризици со кои се соочуваат истите во своето работење.

Кога станува збор за еколошките кривични дела, менаџерите за корпоративна безбедност потребно е да ги насочат своите активности во неколку правци: а) на ниво на спречување и откривање на незаконски и непрофесионални однесувања на вработените кои се вклучени во деловниот процес на различни позиции; б) на ниво на одговорни лица во правното лице кои имаат посебни надлежности и в) на ниво на сопственици на правното лице. Преку овој системски пристап се овозможува остварување на "корпоративната безбедност како стратешка фунција на компаниите, која има за цел остварување безбедност на деловниот успех на корпорациите, што подразбира: елиминација на сите ризици и загрозувања кои може да влијаат на деловната активност и остварување на деловниот успех; доведување на загрозувачките фактори на најмала можна мерка; деловно функционирање во услови на криза (crisis management), совладување на кризи и повторно нормално работење."[13]

Како позначајни аспекти на корпоративната безбедност поврзани со еколошкиот криминалитет би можеле да се наведат следните:

- Заштита од ризици и закани поврани со деловното работење чиешто присуство би можело да доведе до извршување на еколошки кривични дела;
- Помош при донесување на менаџерски одлуки со кои се подигнува нивото на компаниите за вложување во еколошката заштита на деловното работење;

[12]Стојановић М., Павловић Д., Економска безбедност пословања, Београд, 2014 година, стр. 207.
[13] Ivandić Vidović D., Karlović L., Ostojić A., Korporativna sigurnost, Udruga hrvatskih menadžera sigurnosti, UHMS, Zagreb, 2011 godine, str. 66.

- Јакнење на еколошката свест кај вработените и нивната безбедносна култура воопшто;
- Редовно информирање на топ – менаџментот за евентуални слабости во производствениот процес кои би можеле да доведат до загрозување на животната средина од една страна и како последица на тоа опаѓање на интегритетот на компанијата од друга страна;
- Воспоставување на основите за спроведување на сите компоненти на "интегрална безбедност на компаниите"[14].

"Корпоративната безбедност перманентно е вклучена во механизмите на деловното управување на тој начин што го штити нормалното одвивање на деловните процеси, ги отстранува актуелните безбедносни проблеми и на вработените им создава безбедни услови за работа. Конкретно набљудувано, корпоративната безбедност се активира на создавање планови и спроведување на мерки чија што цел е: заштита на корисниците на услугите, заштита на вработените во деловната организација, заштита на имотот во сопственост на длеовната организација, заштита на информациите и репутацијата на деловните организации од материјални штети, криминални дејности итн. На овој начин корпоративната безбедност претставува составендел на процесите кои управуваат со деловните ризици внатре во стопанскиот субјект."[15] Оттука, може да се нотира дека фокусираноста на корпоративната безбедност кон актуелни и идни безбедносни ризици и закани придонесува и кон редуцирање на еколошките предизвици со кои може да се соочи секој деловен субјект или негов вработен.

3.Проценка на ризици во деловното работење како предуслов за спречување и откривање на еколошките кривични дела

Загрозувањето на безбедноста на корпорациите може да доведе до извршување на еколошки кривични дела од најразличен вид. Етиолошки основи за тоа постојат и тие се од субјективна и објективна природа. Така на пример, неефикасната организација на еден производен процес или отсустно на перманентна контрола на длеовното работење може да бидат доволна причина за продуцирање на еколошки катастрофи за животната средина и животот на човекот. На подрачјето на Скопје, како реликт од минатото може да се наведе опасноста од депонијата на фабриката Охис во Скопје, каде пред 40 години се депонирани 13 илјади тони токсичен и канцероген пестицид линдан. Тој е оставен на отворено и ги загадува почвите, подземните води и воздухот. Истовремено, со некоординацијата меѓу институциите, постојаното преклопување со надлежностите и со индиферентноста на оние што треба да похрабро да тргнат со порадикални чекори, како да се занемарува фактот што во дворот на ОХИС се наоѓа токсичен и канцероген отпад, кој бара итен ангажман. Особено што сите досегашни истражувања и студии укажуваат дека на тој потег освен големо количество жива, со години скопјани ги труе линданот, кој бил користен како инсектицид со широк обем на дејствување кај

[14] Milošević M., Pojam i sadržaji korporativne bezbednosti, Zbornik radova, Fakultet za bezbjednost I zaštitu Univerziteta Sinergija, Banja Luka, 2010 godine, str. 59-60.
[15] Trivan D., Korporativna bezbednost, Dosije studio, Beograd, 2012 godine, str. 84.

семенскиот материјал, за третирање на почвата, прскање, заштита на дрвата и дрвената граѓа и против ектопаразити кај животните и луѓето (Слика бр. 1: приказ на депонии во Скопје).

Слика бр. 1

“Исто така, во Македонија има 16 места кои се извор на радиоактивно зрачење. Дури четири од нив се наоѓаат во Скопје. Најопасниот извор е кобалтот 60 кој е сместен на Клиниката за онкологија, велат експертите. Проблем е што државата нема специјален склад каде што ќе се чува радиоактивниот отпад.”[16]

Овие евидентни и опасни случаи кои се јавуваат како извори на загрозување на животната средина и пошироко, ја наметнуваат потребата од благовремена и квалитетна проценка на ризикот во работењето преку детектирање на постоечки проблеми, предвидување на нивниот развој и навремено превземање мерки и активности за нивно отстранување. Тоа подразбира детално истражување на изворите на загрозување, криминогените, виктимогените и патогените жаришта кои може да го дестабилизират длеовниот процес во целина. Активностите со кои се врши безбедносна проценка условно може да се поделат на следниот начин:

1) Проценка на можните извори (носители) на загрозување на безбедноста во корпорациите;
2) Проценка на можните облици (начини) на загрозување на безбедноста во корпорациите;
3) Проценка на можните места на загрозување на безбедноста во корпорациите и
4) Анализа на ризиците.[17]

[16] https://novatv.mk/radioaktiven-kobalt-ke-se-otstrani-vladata-na-gruevski-odbivala/., 13.03.2018 година.
[17] Драгишић З., Безбедносни менаџмент, Службени гласник, Београд, 2007, стр.47-52.

Проценката на ризиците треба да биде содржинска и применлива така што на сопствениците или на надлежните лица ќе им помогне да:

- Ги препознаат опасностите во работењето и да ги проценат ризиците поврзани со тие опасности за да се одредат мерки за заштита на здравјето и безбедноста на вработнеите и другите работници внимавајќи притоа на законските прописи;
- Ги проценат опасностите за да се избере најсоодветна работна опрема од хемиска материја, опременост на работното место и организација на работата;
- Проверат дали постоечките мерки се соодветни;
- Ги превземат оние дејствија кои се неопходни после спроведување на проценката на ризикот со кои ќе покажат на самите себе, на надлежните државни органи, работниците и нивните претставници дека сите фактори во врска со работата биле разгледувани, како и дека е донесена соодветна проценка за присутност на опасност и мерките кои се потребни за зачувување на здравјето и безбедноста;
- Се грижат за превентивните мерки како метод на работа и производство кои се применуваат после спроведена проценка на ризикот, претставуваат подобрување на безбедноста на работниците и подобра заштита на нивното здравје.[18]

4.Заклучок

Еколошките безбедноснии ризици и закани претставуваат реалност во секојдневното деловно работење. “Евидентното постоење на еколошките кривични дела со национален и меѓународен предзнак, односно нивна интернационализација е логична последица на научно-технолошкиот развој и глобализацискиот тренд. Човекот и неговиот ум во овој соврмен моментум ја потврдија тезата дека може многу лесно да ја злоупотребат науката и технологијата за остварување на што поглем и нелегален профит! Но, од друга страна, истовремено и со уште позастрашувачки штетни последици врз животната средина, врз одржливиот развој и човечката безбедност се манифестираат и влијанијата на овие кривични дела.”[19]Корпоративната безбедност како модел на заштита на функционирањето на современите деловни субјекти има свои надлежности во превенцијата на еколошките кривични дела затоа што тие како посебна групација на кривични дела имаат импликација и врз економската безбедност во целина. Точките на поврзување помеѓу потребата од редуцирање на еколошките кривични дела и менаџерите за корпоративна безбедност се видливи и реални. Имено, еколошката безбедност претпоставува и вложувања финансии од страна на топ менаџерите и сопствениците на компаниите во двојна насока: во јакнење на еколошката свест пред се кај вработените и во сопствената свест за континуирано модернизирање на рабонтите и производствените процеси.

[18] Marković S., Osnovi korporativne i industrijske bezbednosti, USEE, Novi Sad, 2007 godine, str. 213-214.
[19] Kozarev A., Harmful Consequences on Economic Development due to Endangering Environmental and Nature with Waste, IDEA – International Journal of Science and Arts, VOl. 1 Skopje, 2017 y., p. 156.

Безбедносните проценки за ризиците кои може да се јават во случај кога овие вложувања се стават на маргините на стратешките цели на компанијата, а кои се подготвуваат од менаџерите за корпоративна безбедност се првото скалило на сигнализирање од страна на системот на корпоративна безбедност. Понатаму, тука се надоврзуваат корпоративните индикатори во областа на човечките ресурси, заштитата на информациите, деловните тајни, конкурентската предност итн. На тој начин може да се заклучи дека корпоративната безбедност како концепт, модел, визија има посебно значење во подигинување на економската безбедност која пак според природата на еколошките кривични дела (со економски предзнак) е од клучно значење за јакнење на деловниот интегритет и доверба.

Литература

1.Сулејманов З., Македонска криминологија, Скопје, 2000 година.
2.Јовановић Љ., и др. Кривично право посебни део, треће измењено и допуњено издање, Београд, 2004 године.
3.Малиш-Саздовска М., Прирачник за истраги кај еколошки кривични дела, Скопје, 2013 година.
4.Џуклески Г., Николоска С., Економска криминалистика, Скопје 2007 година.
5.Проевски Ј., Коментар на КЗ, Агенција "Академик", Скопје, 1998 година.
6.Стојановић М., Павловић Д., Економска безбедност пословања, Београд, 2014 година.
7.Ivandić Vidović D., Karlović L., Ostojić A., Korporativna sigurnost, Udruga hrvatskih menadžera sigurnosti, UHMS, Zagreb, 2011 godine.
8.Milošević M., Pojam i sadržaji korporativne bezbednosti, Zbornik radova, Fakultet za bezbjednost i zaštitu Univerziteta Sinergija, Banja Luka, 2010 godine.
9.Trivan D., Korporativna bezbednost, Dosije studio, Beograd, 2012 godine.
10. Драгишић З., Безбедносни менаџмент, Службени гласник, Београд, 2007.
11.Козарев А., Приватната безбедност во Република Македонија – теоретски и институционален дизајн, Зборник на трудови од Втората меѓународна научна и стручна конференција: Општествени, економски, правни, безбедносни и социјални детерминантни за развој на корпоративната безбедност во Република Македонија, регионот и пошироко, Асоцијација за корпоративна безбедност- Скопје, 2017 година.
12.Kozarev A., Harmful Consequences on Economic Development due to Endangering Environmental and Nature with Waste, IDEA – International Journal of Science and Arts, VOl. 1 Skopje, 2017 y.

Документи:

1.Министерство за животна средина и просторно планирање, Стратегија за животна средина и климатски промени 2014-2020 година, Скопје, 2015 година.
2.Кривичен законик (пречистен текст), База на закони www.pravdiko.mk.
3.Службен весник на РМ, бр.226 од 25.12.2015 година.

Интернет адреси:

https://novatv.mk/radioaktiven-kobalt-ke-se-otstrani-vladata-na-gruevski-odbivala/., 13.03.2018 година.

Проф. д-р Зоран Јолевски
Европски Универзитет Република Македонија
Македонија, Скопје
е-маил: jolevski@gmail.com

КОРПОРАТИВНА БЕЗБЕДНОСТ ВО СОВРЕМЕНАТА УСЛУЖНА ЕКОНОМИЈА И ИНДУСТРИЈАТА 4.0.

Кога станува збор за иднината во развојот во корпоративната безбедност треба да има во превид трансформацијата низ која поминуваат современите корпорации. Како резултат на најновите техничко технолошки достигнувања светската економија, а со тоа и корпорациите се менуваат, односно трансформираат. Ако средствата на компаниите поделиме во две групи: видливи (tangible) и невидливи (intangible) и напрвиме временска анализа тогаш се забележува промена во нивната улога во производствените и услужните процеси на микро ниво. Настануваат промени во нивното учество во креирањето новосозденатa вредност и тоа во насока на експоницијален раст на учеството на т.н. невидливи средства (знаење и умеење, патенти, авторски права, информации, информативни мрежи, софвери, интеграции на оперативните процеси). Значи вредноста на т.н. невидливи средства расте побрзо од вредноста на видливите средства на корпорациите. Ова природно предизвикува промени во потребата и значењето на нивната заштита, а со тоа во концептите и формите на корпоративната безбедност, односно заштитата на т.н. невидливи средства станува се позначајна.

Ако пред повеќе векови земјоделското производство, а потоа традиционалното индустриското производство доминираа во создавањето на бруто националниот доход, денес сме сведоци на доминација на услужниот сектор во создавање на националното богаство. Покрај ова, треба да се земе предвид дека денес индустрискиот сектор минува низ процес на трансформација, кој се нарекува Индустриска револуција 4.0., односно се создава т.н. Индустрија 4.0. Овие два сегменти на националната економија, услужниот сектор и Индустријата 4.0. играат се поголема улога во креирањето додадената вредност, што укажува дека заштитата, односно безбедноста на т.н. невидливи средства ќе има се поголема улога.

Првата индустриска револуција ја користеше парата за покренувањето на машините. Втората индустриска револуција се базира врз употребата на електричната енергија во фабриките, додека пак третата индустриска револуција настана како резултат на употребата на електорниката и информатичката технологија, кои доведоа до висок степан на автоматизација на производствените процеси. Четвртата индустриска револуција која е во тек, односно Индустриска револуција 4.0. може да се опише како создавање „паметни стоки“ со паметни производствени процеси, во „паметни фабрики“. Според Консултантската куќа ***McKinsey***[20] „Индустриската револуција 4.0. се

[20] „Industry 4.0 at McKinsey’s model factories: Get ready for the disruptive wave“, група автори, предводена од Erhard Feige, McKinsey, 2016 г. стр 2

дефинира како следна фаза во дигитализацијата на секторот за производство и се придвижува врз основа на четири нарушувања (промени – забелешка на 3J): неверојатен пораст на обемот на податоци, компјутерската моќ и конективност, особено на новите широкопојасни мрежи со ниска моќност; појавата на аналитички и деловно-разузнавачки капацитети; нови форми на интеракција на човекот со машината како што се интерфејси за допир и системи за зголемена реалност; и подобрувања во пренесувањето на дигитализацијата во физичкиот свет, како што се напредната роботика и 3-Д печатењето.

Индустријата 4.0. ја сочинуваат „паметни фабрики“ во кои производствениот процес е управуван од автоматизирани системи, роботика и преку вештачка интелегенција ги интегрира потребните инфомации за носење на автоматизирани одлуки за производство на „паметни стоки“. Новиот модел на индустрија се базира на интегрирање на машините со компјутерите, а вештачката интелегенција ги управува производствените процеси. Оваа индустриска револуција се движи со експоненцијална брзина и веќе почна сериозно да ја менува формата на средствата на компаниите, а со тоа и концептот за корпоративна безбедност, односно заштита на овие средства.

Во претходните економски системи елементите на производството (земја, машини, хали, пари во форма на метал или хартија) и резултатите од овие процеси (земјоделски или индустриските стоки) беа видливи за човечкото око. Релативна вредност на невидливите средства во новосоздадената вредност, иако секогаш постоела, била многу помала во споредба со онаа денеска. Ако се до втората половина на минатиот век доминантен аспект на корпоративната безбедност беше физичката безбедност на факторите за производство (главно видливи средства), од втората половина на минатиот век потребата за обезбедување на т.н. невидливи средства се зголемува со голема брзина. Појавата на интернетот и неговата поинтезивна употреба која започна во последната деценија на минатиот век донесе до нови квалитативни промени во концептот на корпоративна безбедност, односно до појава на една сосема нова гранка, а тоа е сајбер безбедноста.

Заштитата на корпоративните средства веќе не е доминантна како облик на физичката заштита на средствата во сопственост на корпорацијата, туку позначјна станува заштитата и безедноста на информатичките мрежи, податоците кои се движат низ овие мрежи, податоците кои се чуваат во складишта за податоци, интелектуалната сопственост, know-how, авторските права и сл. Компаниите од услужната дејност заедно со индустриските компаниите од т.н. индустрија 4.0 имаат потреба од еден сосема нов вид на корпоративна безбедност.

До пред половина век, поимот шпиунажа главно се однесуваше на шпиунажа меѓу државите. Имајќи ја предвид структурата на современата економија, треба да се промени името од „индустриска“ во „деловна“ шпиунажа, бидејќи предмет на шпиунажа не се само деловните тајни во индустријата, туку и во услужниот сектор. Денеска деловната шпиунажа е и пораспостранета од

шпиунажата меѓу државите. За разлика од оддавањето на државни тајни кое се санкционира со кривични закони и е кривично дело, корпорациите многу тешко можат да користат законски мерки против неовластеното оддавање на деловни тајни. Ова ја прави заштитата од деловна шпиунажа уште посложена и потешка. Потребата за квалитетна на заштитата кај деловната шпиунажа станува се поголема. Заради ова компаниите се приморани да изнаоѓаат и имплементираат нови креативни солуции кои ќе обезбедат нивна заштита од т.н. индустриска шпионажа. Најранливи за вакви дејствија се истражувачките единици на корпорациите.

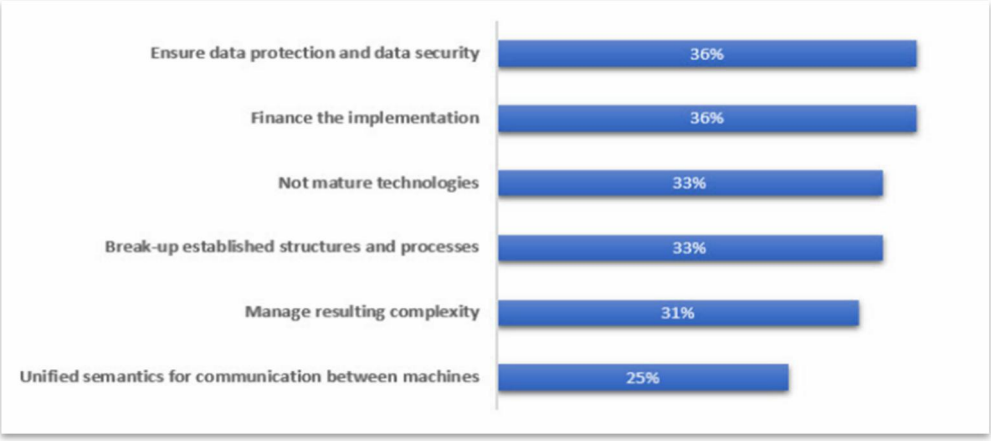
Тука треба да се додаде уште еден многу значен момент за современите компании, но и за корпоративната безбедност, а тоа е обезбедување на континуитет на производството, односно операциите на компанијата, елиминирање или субстантивно намалување на застоите на операциите. Ова е посебно значајно заради поврзаноста на производствените процеси, односно функционирањето на т.н. suplay chains. Со цел да не врзуваат голем капитал во репроматеријали и други компоненти потребни за производство, корпорациите чуваат минимални залихи и очекуваат навремено да бидат снабдени со потребните инпути. Континуитетот на снабдување со репроматеријали и полупроизводи, стоки и давање на услуги во услови кога економијата функционира во модул на just on time suplay chain е особено значајно. Способноста на компанијата навремено и во континуитет да ги снабдува своите клиени е поеднакво важно како и цената и квалитетот на суровините, полупроизводите што се продаваат, односно услугите што се даваат. Заради ова компаниите покрај добрата заштита на видливите и невидливите средства, неопходно е да имаат добро разработени планови за превенција, но и планови за постапување доколку се случи настан кој го нарушува континуитетот на бизнис операциите без оглед дали е резултат на природата или пак на човечки фактор. Нарушување на континуитетот покрај директните финансиски штети, може да ја наруши и репутацијата на компанијата.

Bernard Marr во неговата статија „What Everyone Must Know About Industry 4.0“ објавена во Форбс[21], како прв од предизвиците со кои се соочува Индустријата 4.0. ја наведува сајбер безбедноста, паралелно со заштитата на интелектуланата сопственост врз кои се базираат новите производни и услужни процеси.

Според истражувањето за факторите односно предизвиците кои влијаат на развојот на Индустријата 4.0. во Германија (Germany’s Industrie 4.0 – the challenges in IT-Security Raphael Labaca Castro 3 Nov. 2015) корпоративната безбедност е на прво место (Графикон бр. 1).

[21] https://www.forbes.com/sites/bernardmarr/2016/06/20/what-everyone-must-know-about-industry-4-0/#1f5a00c0795f

Графикон 1
Кои пречки треба да се надминат за да се постигне концептот на Индустрија 4.0.



Извор: Germany's Industry 4.0 – the challenges in IT-Security, Raphael Labaca Castro, 3 Nov 2015 https://www.welivesecurity.com/2015/11/03/what-is-industry-4-0/

Дури 36% од испитаните компании истакнале дека безбедноста на податоците, односно информациите кои се неопходни за функционирање компаниите во Индустијата 4.0. е предизвик, односно ја идентификувале како можна препрека за развојот. Финансиските импликации и немањето доволно развиена технологија се на второто, односно третото место. Значи корпоративната безбедност е поголем предизвик од финансирањето на Индустријата 4.0. Дури и недоволната созреаност на технологиите што треба да се користат во овие комапнии е помал предизвик корпоративната безбедност. Ова произлегува од тоа што вредноста на невидливите средства кои се неопходни за развојот на паметните фабрики се доминантни. Врз основа на овие невидливи средства компанијата има компаративна конкуретска предност во споредба со конкуренцијата. На ова треба да се додаде дека неовластено влегување во корпоративниот информациски систем може да нанесе штата на паметното производство, да ги поремети алгоритмите врз основа на кои се носат децентрализирани оперативни одлуки во паметните производни процеси и со тоа направи материјална и финансиска штета на компанијата.

До слични резултати дојде и студијата на Националната академија за науки и инженерство на Германија „Обезбедување на иднината на германската преработувачка индустрија: Препораки за имплементација на иницијативата ИНДУСТРИЈА 4.0: Краен извештај на Работната група 4.0."[22]. Во оваа студија е истакнато дека корпорацискта безбедност има посебно значење за развојот

[22] Securing the future of German manufacturing industry Recommendations for implementing the strategic initiative INDUSTRIE 4.0: Final report of the Industrie 4.0 Working Group, Acatech – National Academy of Science and Engineering, 2013, Франкфурт

на компаниите од т.н. Индустрија 4.0. Во апстрактот на Извештајот се истакнува дека корпоративната безбедност е значајна, пред се, заради тоа што „производните капацитети и производите, а особено податоците и информациите што ги содржат - треба да бидат заштитени од злоупотреба и неовластен пристап. Ова бара, на пример, распоредување на интегрирани безбедносни и безбедносни архитектури и уникатни идентификатори..."[23]. Безбедносните предизвици можат да бидат во форма на сајбер напади кои нанесуваат штета, но и во форма на деловна шпионажа, преку која се крадат доверливи информаци и тајни од компаниите. Доколку оваа заштита е несоодветна може да предизвика одлив на корпорациски тајни и информации. Во одредени случаи трошоците поврзани со истражувањето и развојот чинат многу повеќе од физичките фактори на производството (хали, машини и сл.), така да кражбата на овие многу вредни информации може да му овозможи ентитетот кој неовластено ги поседува да оствари екстра профит и ја доведе во опасност профитабилноста на компанијата која вложувала во истражувачките активности. Затоа корпорациската безбедност се смета за клучен фактор за успехот на Индустријата 4.0.

Со оваа констатација се согласуваат скоро сите аналитичари,. Тие сметаат дека сајбер безбедноста е најголем предизвик за развојот на Индустријата 4.0. Овој вид на заштита односно безбеднот ќе претставува се поголем трошок кој компаниите треба да го калкулираат и треба да се очекува неговото учество во вкупните трошоци постојано да се зголемува.

Покрај промените во комплексноста, доаѓа до зголемување на трошоците за корпоративна безбедност. Тие станаа толку значајни што Светската банка започна да собира податоци од компаниите колкави се нивните трошоци за оваа намена. Проценка е дека овие трошоци ќе растат во иднина не само во апсолутна, туку и во релативна вредност. Значи корпоративната безбедност не треба да ја гледаме само од аскпет на безбедност на средствата на компанијата (видливи и невидливи), туку и од аспект на можност за намалување на вкупните трошоци, а со тоа зголемување на профитабилноста.

Влегуваме во ера во која корпоративната безбедност, заштитата на мрежите и инфомрациите кои се движат низ нив, станува услов за раст на современите компании. Квалитетот и ефексаноста на корпоративната безбедност станува клучна за растот на компаниите. Развојот на овие сектори на економијата е свразан со огромни вложувања во R&D и имплементација на резултатите од овие истражувања. Загубата на овие информации, односно неовластен пристап на конкуренцијата до нив, ќе резултира во загуба на компаративната предност на компанијата која произлегува од вложувања во развојот. Неовластеното влегување во информатичките мрежи во корпорациите може да придонесе за сериозни нарушувања во процесот на производство, односно давање услуги. Штетите кои настануваат може да имаат влијание врз компанијата и нејзината профитабилност, квалитетот на производот или улогата, како и врз консументот.

[23] Исто стр. 6

Последниве неколку години американското општество беше сериозно потресено од крадењето на персонални информации од неколку компании. Влегувањето во базата на податоци на една од трите кредитни агенции во САД, Equifax, во периодот од мај до јули 2017 година резултираше во кражба на сензитивни лични податоци на повеќе од 143 милиони американци, нешто помлаку од половина од граѓаните на САД. Хакерите украдоа подтаци за адресите, датумот и местото на раѓање, матичните броеви за социјална сигурност (Social Security numbers), еквивалент на Единствениот матичен број во Македонија, а во некои случаи и на броевите на возачките дозволи. Имајќи предвид како функционира американското општество, интензитетот на трансакциите кои се одвиваат преку интернет, постои опасност да се нанесе голема материјална и финансиска штета на лицата чии податоци се украдени. Лице кое неовластено располага вакви податоци може неовластено да направи трансфер на средства, да нанесе штета на кредитниот рејтинг на лицето и многу други работи. Ова влијаеше врз репутацијата на компанијата, резултираше со оставки во Управниот одбор.

Еден од најголемите ланци на супермаркети во САД Таргет во неколку наврати беше предемет на хакирање. Покрај директните оштети што Трагет ги плати на консументите чии лични податоци беа украдени, компанијата претрпе големи штети од намалувањето на обемот на продажба заради недовребата во нејзиниот информатички систем. Една од причините за намалување на вредноста на Yahoo е неможноста овој провајдер на улуги да ги заштити податоците на корисниците на неговите услуги.

Компаниите не секогаш ја информираат јавноста за хакирањето, бидејќи може да влијае врз нивниот раст. Губењето на довербата и репутацијата може да биде погубно дури и за компанија која е добро етаблирана на пазарот. Така на пример во 2012 беше хакиран серверот на компанијта LinkedIn. Оваа информација не беше позната на јавноста до 2016 година. Доколку се појавеше во јавноста во 2012 година прашање е дали LinkedIn ќе го постигнеше денешното ниво на развој, па дури прашање е дали ќе беше на пазарот денеска, а да не зборуваме колку ќе изгубеше од вредноста на компанијата.

Кога говориме за трансформацијата која настанува во облиците на корпоративната безбедност треба да се има во превид и промената која настанува на пазаарот, како место на кое се врши продажба на стоките и услугите. Интернетот се повеќе станува место на кое се разменуваат стоките и услугите. Продавачот преку интернет ги пласира своите стоки и услуки, а консументот ги нарачува и ги плаќа електронски. Интернет трговијата експоницијално расте. САД е најнапред во оваа свера. Слободна проценка е дека тоа што се случува на интернет пазарот во САД, со закаснување од неколку години доаѓа и другите делови на светот. Интернетот придонесува до промена на тоа како некои бизниси егзистираат и се развиваат. Општо познато е дека во САД печатените дневни весници и магазини постепено исчезнуваат, а консумнетите наместо хартиени промероци се повеќе ги читаат

нивните електронски изданија. Тој тренд станува поприсутен и во останатиот дел од светот. Авио билтетите, резервациите на хотели, крстарења, пакет туристички патувања, во САД, скоро и да не се купуваат во туристички агенции, туку исклучиво преку интернет. Бројот на туристички аганеции, како физичко место каде се продаваат овие услуги е драстично намален. Плаќањето на сметките се повеќе се реализира на интеренет, а експозитурите на банките се помалку се посетуваат за давање на налози за овие плаќања. Апаратите за домашна употреба и електорниката доминантно се набавуваат преку интернет. Џеф Безос, сопственикот на Амазон, компанија специјализирана за електронска трговија, стана најбогат човек на светот во 2017 г.. Ова е најмаркантен доказ за големината на трговијата која се одвива преку интеренет.

Како што продавниците, шопинг моловите треба да се заштат, така треба да се заштити и интерентот како место на кое се одвива трговијата. Жртви на сјабер крминалот се и компаниите и консументите. Така, последниот Извештај за криминалот преку интернет[24] на ФБИ оценува дека во 2017 година губитокот на корпорациите и консументите е над 1,7 милијарди долари, и тоа во следниве категории: крадење преку неовласен влез во приватните и бизнис е-маил адреси – 676 мил. $, кражби преку кредитни картички 57 мил. $, преку неовластено користење на лични податоци 77 мил. $, на корпорациски податоци 61 мил. $, кражби преку неовластен влез во електронски податоци на недвижности и нивно изнајмување 56 мил. $, електронска каражба на инвестициони вложувања 97 мил. $, на авансни плаќања 57 мил. $, електронска кражба преку неовластено корестење на идентитетот на физички правни лица 66,8 мил $, неиспорачани и неплатени стоки 141 мил. $ и преку штети направени со губење на довербата 211 мил. $. Сајбер криминалците потекнувале од странство, но и од САД.

Доколку компанијата не успее да го заштити своето тргување преку интеренет, може да се соочи со губење на репутација и порај тоа што нејзините производи и услуги се квалитетни. Оваа заштита се однесува и на личните податоци на клиентите. Несоодветната безбедност на базите на податоци, како лични, така и корпорациски може сериозно да нанесе штета на компанијата. Репутацијата на компаниите отсекогаш била значајна за нивната позиција на пазарот. Тука треба да се додаде дека со интернетот, социјалните мрежи, информацијата за репутацијата на компанијата брз се шири. Затоа корпорациите мора да обезбедат соодветна заштита на опреациите кои ги реализираат на интернет. Загубата, како што претходно кажавме, нема е само во финансиски и физички облик, туку загубата може да биде во облик на губење и на репутација, што може мошне сериозно да го загрози опстанокот на компанијата. Сајбер безбедноста станува еднакво важна како и квалитетот и цената на производот.

Заради промените во безбедносните закани кои настанаа особено последниве 20-тина години, активности поврзани со корпоративната безбедност стануваат

[24] 2017 Internet Crime Report, FBI, Вашингтон, 2017 г.

се посложени и покомплексни. Се зголеми потребата од интердисцилинарен пристап кон корпоративната безбедност и интегрирање на разни системи од различни дејности, но и различен карактер, како што се кадровски, техничко-технолошки, информатички и други. Заради комплексноста и значењето на овој сегмент на функционирањето, компаниите се повеќе се одлучуваат за outsourcing на дел или пак целокупниот сегмент на корпоративна безбедност. Заради комплексноста пазарот се сегментира, односно се јавуваат специјализирани компании, кои даваат услуги на физичкото обезбедување, компании кои продаваат опрема потребна за обезбедување, компании кои обезбедуваат услуги од областа на сајбер безбедноста и др.

Ова пак од своја страна ја наметнива потребата за интеграција на овие различни безбедносни подсистеми, како и за зголемување на ефикасноста на корпоративната безбедност, а истовремено намалување на трошоците. Затоа последнава деценија се јавуваат компании кои обезбедуваат стратегиски совети за интегрирање на различните елементи на корпоративната безбедност, т.е. компании кои даваат стратегиски консалтинг за корпоративна безбедност. Како експерти во овие компании се јавуваат лица кои долги години работеле за државни инситуции чија цел била одбраната и безбедноста на државата и заштита на критичната инфраструктура. Овие лица располагаат со најсофистицарана експетиза која го зголемува квалитетот на копрацискатa безбедност, а истовремено овозможува поефикасно користење на ресурстите за оваа намена. Ова најдобро може да се опише преку цитатот на Sussman Corporate Security **(**SCS) компанија која има канцеларии во Вашингтон, Торонто, Тел Авив и Хонг Конг:
„SCS обезбедува трошковно ефикасни, специјално дизајнирани солуции за обезбедување кој ја зголемуваат профитабилноста преку:

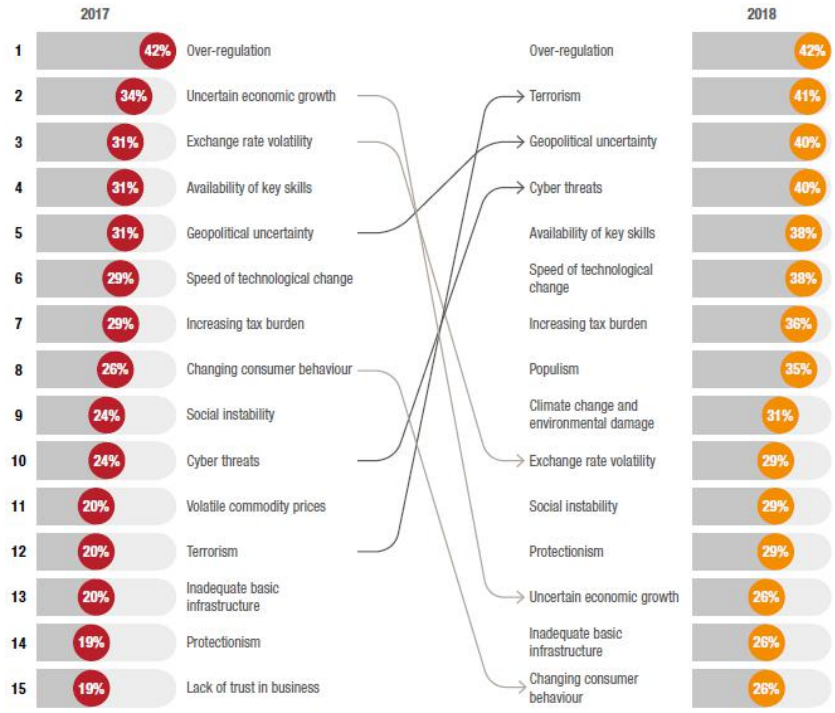
- зголемена и поефикасна безбедност со пониски трошоци;
- обезбедување на континуитет и флексибилност во бизнис операциите, преку минимизрање на застоите и неефиканостите;
- зајакнување на репутација на пазарот како безбеден и сигурен снабдувач на стоки и/или услуги“

На ова треба да се додаде дека во последниве децении настанува промена на пазарот за услоги од областа на безбедност. Имено државните институции, од провајдери, преку outsourcing стануваат консументи на вакви услуги. Американската влада има отидено најмногу напред во ова. Значи може да се очекува и останатиот дел од развиените земји поинтезивно да користат приватни компании за дејствија кои порано беа исклучува надлежност на армиите и полициите.

PwC направи анкетаво последното тромесечие во 2017 на 1293 CEO од 80 држави со цел да го анализира оптимизот за економски раст во 2018 година. Истата ја објави во публикацијата „21st CEO Survey“[25]. Меѓу другото ги анализира и факторите кои негативно влијаат врз растот на компаниите. Ако се споредат одговорите на глобално ниво со анкетата од претходната година

[25] 21st CEO Survey: The Anxious Optimist in the Corner Office, 2018 Survey, PwC

може да се забележи дека за 2017 година се зголемени стравувањата од сабер заканите, геополитичката несигурност и тероризмот. Другите фактори бележат намалување[26]. Понатаму во документот се анализираат заканите по корпорацискиот раст и може да се забележи дека на Сверноамериканскито континет на прво место е сајбер безбедноста, на трето место е глобалната несигурност, а на четврто тероризмот. И кај компаниите во Западна Европа ситуацијата е слична, со тоа што геополитичката несигурност е на трето, сајбер заканите на четврто и тероризмот на петто место.



Извор: 21st CEO Survey: The Anxious Optimist in the Corner Office, 2018 Survey, PwC, стр.14

Од овие три закани по растот, државните инсититуции се надлежни да се справат со геополитичката несигурност и тероризмот. Но тоа не значи дека корпорациите не ги имаат во предвид овие закани при носењето на одлуки. Имено реакцијата на корпорациите кон овие надворешни фактори се состои во нивните одлуки за географска алокација на идните директни инвестиции. Притоа тие ги анализираат и носат одлуки кои се однесуваат на обезбедување на деверзификација на ризикот на пазарите на кои ги продаваат нивните производи, односно услуги, како и деверзификација на резиците кои произлегуваат од снабдувањето на репроматеријали и компоненти. Ризокот на овие две безбедносни закани влијае и врз висината на

[26] Исто стр. 14

очекуваниот профит. Имено компаниите во приницип очекуваат многу повисоки профити од поризичите инвестиции, односно пазари.

Сабер безбедноста е во надлежност на самите корпорации. Сајбер безбедноста е закана како на микро ниво (корпорациско ниво), така и на макро ниво (закана по национлната безбедност. Државите носат национални стратегиии за сајбер заканите. Но за ефикасна национална сајбер одбрана потребна е и соработка меѓу државните инситутции и компаниите.

Како заклучок може да се истакне дека корпративната безбедност во иднина ќе станува се познајна и трошоците за неа се очекува постојано да се зголемуваат. Промените во работењето на совеременитe компании, промените во корпоративните процеси, појавата на Индустријата 4.0. како и промените во структурата на средствата на компаниите, оснобено со експоненцијалниот раст на невидливите средства, доаѓа до промени во корпорацискатa безбедност, методите со кои тие ја обезбедуваат услугата на корпорациска безбедност. Паралено се менуваат вештините потребни што ги имаат лицата кои се задожени за корпоративната безбедност. Современтите компании се повеќе ќе прават outsourcing на безбедноста, а пак заради сложеноста на оваа дејност ќе дојде до сегментација, специјализација на ентитетите кои ќе даваат услуги од областа на корпоративна безбедност.

Akademik, prof. dr. Ibrahim Jusufranić
Internacionalni univerzitet Travnik u Travniku
Bosna i Hercegovina

ZNAČAJ I ULOGA KORPORATIVNE SIGURNOSTI U POSLOVANJU PREDUZEĆA

Sažetak
U cilju poboljšanja poslovanja i zaštite svojih interesa korporativna sigurnost je posvećenost privrednog subjekta da doprinese održivosti svoga poslovanja i privrednog razvoja, sarađujući sa partnerima, zaposlenicima i društvom uopšte. Korporativna sigurnost je koncept po kojem privredni subjekti koji ga usvajaju svjesno i dobrovoljno nadilaze svoju primarnu funkciju sticanja i raspodjele profita a posebno sa aspekta zaštite svoje imovine, kupaca, dobavljača, zaposlenih i vlasnika te pozitivno ostvaruju uticaj na radno, društveno i prirodno okruženje. Model upravljanja i implementacije standarda korporativne sigurnosti treba biti u samom vrhu menadžerskog razmišljanja, jer taj pristup omogućava organizacijima da se pripreme za iznenadne nepovoljne situacije i brz oporavak, osiguravajući kontinuitet i kvalitet poslovanja. Akteri koji su uključeni u ovaj proces moraju biti spremni da bih adekvatno odgovorili svim izazovima da bih zaštitili privredni subjekat, poslovanje i resurse.

Ključne riječi: Korporativna sigurnost, privredni subjekti, poslovni procesi, privredni razvoj, poslovanje.

SIGNIFICANCE AND ROLE OF CORPORATE SECURITY IN COMPANY BUSINESS

Abstract
In order to improve business and protect its interests, corporate security is the commitment of an entity to contribute to the sustainability of its business and economic development, working with partners, employees and society in general. Corporate security is the concept by which company business that adopt it consciously and voluntarily overstep their primary function of acquiring and distributing profits, and especially from the aspect of protecting their property, customers, suppliers, employees and owners, and positively affecting the working, social and natural environment. The corporate governance and implementation model of corporate security standards should be at the very top of managerial thinking, as this approach enables organizations to prepare for sudden adverse situations and rapid recovery, ensuring continuity and quality of business. The actors involved in this process must be ready to adequately respond to all challenges in order to protect the company business, business and resources.

Keywords: Corporate security, business entities, business processes, economic development, business.

Uvod

Korporativna sigurnost predstavlja posvećenost preduzeća da doprinese održivosti svoga poslovanja i privrednog razvoja, sarađujući sa poslovnim partnerima, zaposlenicima, vlasnicima i društvom uopšte, u cilju poboljšanja poslovanja i zaštite svojih interesa. Institucionalizacija korporativne sigurnosti kao jedne vrlo specifične oblasti u kompanijama traje i do nekoliko godina, ali u tom razdoblju korporativna sigurnost vrlo se rijetko iskazuje s nekom jasno vidljivom korisnošću za kompaniju, a iziskuje značajna ulaganja. Tada se Upravama kompanija i najčešće postavljaju pitanja poput: treba li njima uopšte takav trošak, da li je to isplativa investicija? Kada će se povratiti uložena sredstva? Iz tog razloga jedan broj kompanija korporativne sigurnosti odustaje i od uređenja i ugradnje u organizacionu shemu službe korporativne sigurnosti ili ipak pozicioniranja menadžera korporativne sigurnosti u upravu kompanije. Sigurnost treba da postane sve prisutnija, kako bi se smanjili gubici u poslovanju i to je potrebno vezati unutra sa svim nivoima odgovornosti u samom preduzeću. Zadovoljavaju se nekim oblicima službe sigurnosti koja se klasično bavi tehničkom i fizičkom zaštitom imovine i objekata kompanije, a koja je ipak isključivo skoncentrisana na modalitete rada usmjerene na sprečavanje klasičnih oblika uništavnja imovine činjenjem protuzakonitih djela, dok apsolutno najvažniji segment korporativne sigurnosti, a to je sigurnost odvijanja poslovnih procesa i zaštita poslovnih interesa kompanije, ostaje u potpunosti nepokrivena. Iako je ekonomska i finansijska kriza uzela svoj danak, pa pojedine zaštitarske firme imaju i porast prihoda, kompanije ulažu manje u ovaj sektor. Uprkos tome, unazad nekoliko godina Bosna i Hercegovina je napravila par iskoraka naprijed po ovom pitanju. Svijest je, što je najvažnije na znatno većem nivou, jer je sve više korporacija koje daju važnost tom jako bitnom segmentu poslovanja, zbog sigurnosti proizvoda klijenata, a posebno vlasnika i zaposlenika. Dobrim dijelom zasluga je to i nauke i prakse iz oblasti korporativne sigurnosti i organizacija niza naučnih skupova. Kroz aktivnosti prakse, poslovna javnost se postepeno senzibilirala na ovu temu u pravcu priznanja potrebe za uvođenjem funkcije korporativne sigurnosti, kao jedne od funkcija podrške koja firmama omogućava nesmetan rad i razvoj što je evidentno u posljednje vrijeme kod nas i u svijetu.

1. Koncept korporativne sigurnosti

Korporativna sigurnost je u savremenoj poslovnoj praksi često korišten koncept, obzirom na to da kompanije u značajnoj mjeri snose odgovornost u svom poslovanju za dešavanja i aktivnosti iz oblasti korporativne sigurnosti. U cilju da doprinese rješavanju problema korupcije preduzeća, društvene zajednice u kojoj obavljaju svoju poslovnu aktivnost kompanije sprovode različite oblike sigurnosti iz oblasti zaštite svoje imovine, poslovnih procesa, informacione sigurnosti, pa sve do sigurnosti svojih kupaca, dobavljača i zaposlenih. Kako bi što uspješnije koristile mnogobrojne prednosti njegovanja društveno odgovornog ponašanja, komapanije moraju da afirmišu svoje ideje i osjećanja, brige za svoje probleme. Izuzetno je važno da obezbijede potpunu transparentnost posvećenosti svojim kompanijama i društvenim interesima. Koncept korporativne sigurnosti preduzeća može se definisati na više načina, ali u širem smislu, to je koncept u kojem poslovni subjekt

odlučuje na dobrovoljnoj osnovi, da doprinosi sigurnijem poslovanju sebi, svojim kupcima i dobavljačima, zaposlenima i vlasnicima, boljem, sigurnijem i čistijem okolišu u interakciji sa ostalim preduzećima, odnosno interesnim grupama i društvom u cjelini. U zemljama u tranziciji, promovisanje korporativne sigurnosti preduzeća postaje efikasno sredstvo i za jačanje društva, putem podsticanja lokalne zajednice i na taj način osiguravanja održivih resursa svog poslovanja u svim segmentima rada i poslovanja svoje kompanije. Korporativna sigurnost predstavlja koncept po kojem privredni subjekti koji ga usvajaju svjesno i dobrovoljno nadilaze svoju primarnu funkciju sticanja i raspodjele profita i ostvaruju pozitivan uticaj na svoje radno, društveno i prirodno okruženje. Korporativna sigurnost u suštini predstavlja svijest o novom položaju i značaju koje kompanije imaju u savremenom, globalnom društvu i odgovornosti koja iz njih proizilazi. To je zapravo proces u kome mogu, mada i ne moraju, imati uticaja na njihovo poslovanje. Praksa korporativne sigurnosti se odnosi na cjelokupnu sferu uticaja i raspona djelovanja jednog preduzeća, kao i na odnose koje ono prema tome uspostavlja: šta proizvodi, kako kupuje i prodaje, da li se pridržava zakona, na koji način zapošljava, osposobljava i utiče na razvoj ljudskih resursa, koliko ulaže u lokalnu zajednicu i poštovanje ljudskih i radnih prava, na koji način doprinosi očuvanju životne sredine.

1. Poslovna strategija preduzeća

Proces globalizacije, tehnološke inovacije, jaka konkurencija i brze društvene promjene neke su od glavnih karakteristika današnjice. Zbog njih se mnogi poduzetnici odlučuju na neetično ponašanje prema konkurentima. Kako bi se spriječilo takvo ponašanje svako poduzeće trebalo bi jasno definirati viziju svog razvoja, ciljeve ali prije svega i strategiju. Kao što i mnogi autori navode: “Poslovna strategija poduzeća – ključ poslovne uspješnosti“.

Danas se poslovanje preduzeća odvija u promjenljivim i nestabilnim oklonostima, zbog čega je potrebno formulisati i implementirati strategiju preduzeća s takvom okolinom i prolagoditi joj se.

Pod pojmom strateškog upravljanja podrazumijeva se uspostavljanje dugoročnih ciljeva, određivanje pristupa za njihovo ostvarivanje, te implementacija, kontrola i vrednovanje ciljeva. Strategiju možemo definisati i sagledati na tri nivoa kao i:

- Korporativna;

- Poslovna;

- Funkcionalna.

Unutar strateškog upravljanja odvijaju se tri poslovna procesa: strateško planiranje, implementacija strategije, kontrola i vrednovanje strategije. Pojam strateškog planiranja obuhvata analizu okruženja i preduzeća u kojem se trenutno nalazi kao i definisanje detaljnog strateškog plana s jasno definisanim ciljevima. Implementacija strategije najvažniji je segment strateškog upravljanja.

3. Upravljanje poslovnim procesima

Osnovni cilj svakog preduzeća je stvaranje vrijednosti. Korporativna sigurnost se svrstava u logističke procese. Poslovni sistemi današnjice moraju identifikovati, kategorizirati, modelirati, pratiti i mjeriti poslovne procese prema kritičnim faktorima uspješnosti. Zbog toga svaka poslovna organizacija razvija vlastiti sistem upravljanja poslovnim procesima, koji omogućava kontinuirano upravljanje i nadzor poslovnih procesa. Dobivene rezultate menadžment koristi za poređenje s konkurencijom i praćenje uspješnosti provođenja strategije. Proces se može definisati kao skup aktivnosti koji koriste jedan ili više inputa i kreiraju rezultat vrijednosti za kupca. Opšta podjela procesa prema vrsti posla koje obavlja neko preduzeće je na:

- Upravljačke;
- Osnovne;
- Logističke poslovne procese.

Sa sigurnosnog aspekta, prije su bile tek neznatne štete koje bi prouzrokovali nezadovoljni pojedinci, dok je situacija danas mnogo gora. Susrećemo se s napadima organizovanih grupa, čiji je cilj ugrožavanje poslovanja preduzeća ili uništavanje cijele organizacije.

Kako bi se ovakavi događaji spriječili, organizacije moraju zaštiti svoje upravljačke, osnovne i logističke poslovne procese. Kako bi se to postiglo, važno je da je sigurnosna strategija usklađena s poslovnom strategijom preduzeća kao i ostalim funkcijskim strategijama.

Opšta podjela procesa prema vrsti posla koje obavlja neko preduzeće je na:

- Upravljačke;
- Temeljne;
- Potporne poslovne procese.

U današnjici se susrećemo s napadima organiziranih skupina čiji je cilj ugrožavanje poslovanja poduzeća ili uništavanje cijele organizacije. Kako bi se ovakav događaj spriječio organizacije moraju zaštititi svoje upravljačke, temeljne i potporne poslovne procese. Kako bi se to postiglo važno je da je sigurnosna strategija usklađna s poslovnom strategijom poduzeća i ostalim funkcijskim strategijama.

Faze upravljanja polovnim procesima korporativne sigurnosti su:

- Dizajn;
- Implementacija;
- Kontrola procesa korporativne sigurnosti.

Korporativna sigurnosti u preduzeću ima važnu ulogu u ostvarivanju postavljenih strateških ciljeva.

Iz tog razloga potrebno je osnovati organizacijsku jedinicu korporativne sigurnosti s jasnim odgovornostima i ovlaštenjima u ispunjavanju svojih temeljnih zadataka. Kod preduzeća s manjim brojem zaposlenih potrebno je usnovati odbor za sigurnost ili imenovati menadžera sigurnosti koji će direktno odgovarati vrhovnom menadžmentu. U velikim preduzećima za to se koristi organizacijska jedinica integralne sigurnosti, koja se dalje raščlanjuje na poslove sigurnosti i zaštite.

Menadžer sigurnosti je direktno odgovoran za upravljanje poslovnim procesima korporativne sigurnosti. U današnje vrijeme postoji sve veća potreba za kompetentnim osobama za upravljanje sigurnosnim procesima u preduzeću.

Kompetencije koje mora posjedovati i znati demonstrirati su znanja, vještine, sposobnosti i osobne karakteristike. Uz sve navedeno važno je i da posjeduje menadžerske vještine (motivacija, karizma, emocionalna inteligencija, upornost, poštenje, razvijene komunikacijske vještine, visoka razina odgovornosti, prepoznavanje i rješavanje problema, profesionalno znanje, inovativnost u radu, praćenje i komunikacija s okolinom poduzeća (vanjskom i unutarnjom), organiziran i ambiciozan).

5. Pravni oblik korporativne sigurnosti

Poslovnu informaciju predstavlja svaka informacija koja je potrebna za obavljanje poslovnih aktivnosti, te za ostvarivanje poslovnih interesa i ciljeva poslovnog subjekta. Poslovne informacije su osnovni resurs svakog poslovnog sistema, te posjedovanje informacija daje prednost u odnosu na konkurente. Informacije omogućavaju prepoznavanje i iskorištavanje poslovnih prilika, donošenje kvalitetnih odluka, poboljšanje produktivnosti te uočavanje tržišnih trendova i prilagođavanje na njih, što na kraju dovodi do ostvarenja poslovnog uspjeha i boljeg pozicioniranja u odnosu na konkurente. Iz tog razloga svako preduzeće stvara i razvija vlastito područje poslovnih podataka i informacija. Informacijska sigurnost je stanje povjerljivosti, cjelovitosti i raspoloživosti podataka, koji se postiže primjenom propisanih mjera i standarda, informacijske sigurnosti, te organizacijskom podrškom za poslove planiranja, provjere i dorade mjera i standarda. Povjerljivost informacija znači da je informacija dostupna samo licima koje imaju ovlaštenja za njeno korištenje. Integritet je zaštita podataka od namjernog ili slučajnog neovlaštenog mijenjanja, a dostupnost je garancija ovlaštenim korisnicima sistema da će im sistem biti raspoloživ u svakom trenutku. Informacijska i informatička sigurnost su dva različita pojma. Informacijska sigurnost obuhvata zaštitu svih informacija, bez obzira u kakvom obliku one bile. Zakon o informacijskoj sigurnosti utvrđuje pojam informacijske sigurnosti, mjere i standarde informacijske sigurnosti, područje informacijske sigurnosti te tijela nadležna za donošenje, provođenje i nadzor mjera i standarda informacijske sigurnosti. Zakon se primjenjuje na državna tijela, tijela jedinica lokalne i regionalne samouprave, te na sve pravne i fizičke osobe koje u svom djelovanju koriste ili imaju pristup klasifikovanim i neklasifikovanim podacima. Zakon o sigurnosnim provjerama utvrđuje sistem sigurnosne provjere osoba koje ostvaruju pristup klasifikovanim podacima. Uredba o načinu pohranjivanja i posebnim mjerama tehničke zaštite poslovnih kategorija ličnih podataka propisuje mjere održavanja i provjere ispravnosti rada računarske, telekomunikacijske i

programske opreme, te sistema za vođenje zbirki posebnih kategorija ličnih podataka i osiguranje radnih prostorija u kojima je smještena oprema. Uredba o mjerama informacijske sigurnosti propisuje mjere informacijske sigurnosti za postupanje s klasifikovanim i neklasifikovanim podacima. Uredba o sigurnosnoj provjeri za pristup klasifikovanim podacima propisuje lice za koje se provodi sigurnosna provjera, vrste i postupci sigurnosne provjere.

6. Informaciona sigurnost

Jedan od temelja za djelovanje i funkcionisanje ljudskog društva su informacije. Važno je napomenuti da podatak i informacija nisu sinonimi. Podatak je činjenica za koju se zna da se dogodila, da postoji ili da je istinita odnosno činjenica koja se navodi da se njome nesto dokaže, dok je informacija obavijest o činjenicama, izvještaj o nečemu, odnosno podaci u bilo kojem stepenu obrade podataka. Znači informacija je obrađeni podatak. Poslovnu informaciju predstavlja svaka informacija potrebna za obavljanje poslovnih aktivnosti, te za ostvarivanje poslovnih aktivnosti i ciljeva poslovnog subjekta. Poslovne informacije su temeljni resurs svakog poslovnog sistema, te mu posjedovanje informacija daje prednost u odnosu na konkurente. Informacije omogućuju prepoznavanje i iskorištavanje poslovnih prilika, donošenje kvalitetnih odluka, poboljšanje produktivnosti te uočavanje tržišnih trendova i prilagođavanje na njih, što dovodi do ostvarenja poslovnog uspjeha i boljeg pozicioniranja u odnosu na konkurente. Iz tog razloga svako preduzeće stvara i razvija vlastito područje poslovnih podataka i infomacija. Informacijska sigurnost je stanje povjerljivosti, cjelovitosti i raspoloživosti podataka, koje se postižu primjenom propisanih mjera i standarda informacijske sigurnosti, te organizacijskom podrškom za poslove planiranja, provođenje i dorade mjesta i standarda. Povjerljivost informacija znači da je informacija dostupna samo licima koje imaju ovlaštenje za njeno korištenje. Integritet je zaštita podataka od namjernog ili slučajnog neovlaštenog mijenjanja, a dostupnost je garancija ovlaštenim korisnicima sistema da će im sistem biti raspoloživ u svakom trenutku.

7. Pojam „busssines intelligence“

Pojam „bussines intelligence“ prvi put se pojavio 1989. godine, kao pojam koji označava proces prikupljanja informacija, odnosno poslovno obavještajnu djelatnost u poslovnom svijetu. „Bussines Intelligence“ je poslovno-obavještajna aktivnost u poslovnom svijetu koja je usmjerena na prikupljanje podataka i informacija potrebnih za donošenje što kvalitetnijih poslovnih odluka u cilju očuvanja pozicije u poslovnom okruženju i postizanju poslovnog uspjeha. Važno je napomenuti da su “busssines intelligence“ i poslovna špijunaža dva različita pojma. „Bussines Intelligence“ je legalna i javna aktivnost poslovnih subjekata koje obuhvata legalna i dopuštena sredstva i metode u prikupljanju javnih i svima dostupnih informacija i podataka sa ciljem postizanja poslovnog uspjeha, dok je poslovna špijunaža nelegalna aktivnost koja obuhvata korištenje nezakonitih i neetičnih metoda i aktivnosti sa ciljem dolaska do osjetljivih i zaštićenih informacija. Informacije pružaju podršku u donošenju kvalitetnih odluka u skladu s osnovnom politikom i okruženjem u području djelovanja preduzeća, zbog toga je nemoguće zamisliti bilo kakav poslovni proces bez upravljanja poslovnim informacijama.

„Bussines intelligence“ i poslovne informacije u uslovima današnjice predstavljaju strateški menadžerski resurs bez kojeg je gotovo nemoguće poslovanje firme. Činjenica je da korporativna sigurnost podrazumijeva ukupnu sigurnost firme s ciljem postizanja sigurnosti poslovnog uspjeha preduzeća. Iz toga proizilazi da je „bussines intelligence“ sastavni dio korporativne sigurnosti.

U savremenim uslovima otvorene su tržišne utakmice, tako da mnoge kompanije ne biraju sredstva da dođu do svog cilja jer svaki poslovni subjekat ima priliku za poslovni uspjeh. S druge strane, svaki poslovni uspjeh istovremeno je izložen najrazličitijim prijetnjama u poslovanju. Zbog toga je sasvim razumljivo da danas menadžeri moraju predvidjeti buduće događaje i prijetnje u poslovanju te pripremiti adekvatne mjere i odgovore na buduće poslovne izazove. Poslovanje u nemirnoj i složenoj poslovnoj okolini nametnulo je potrebu traženja primjerenih instrumenata koji će strateškom menadžmentu pomoći da odgovori na buduće poslovne izazove i prijetnje. Upravo se sistem „bussines intelligence“ pokazuje kao prikladan instrument za ostvarenje tog cilja.

Zaključak

Korporativna sigurnost predstavlja koncept po kojem privredni subjekti koji ga usvajaju svjesno i dobrovoljno nadilaze svoju primarnu funkciju sticanja i raspodjele profita i ostvaruju pozitivan uticaj na svoje radno, društveno i prirodno okruženje. Korporativna sigurnost u suštini predstavlja svijest o novom položaju i značaju koje kompanije imaju u savremenom, globalnom društvu i odgovornosti koja iz njih proizilazi. To je zapravo proces u kome mogu, mada i ne moraju, imati uticaja na njihovo poslovanje. Praksa korporativne sigurnosti se odnosi na cjelokupnu sferu uticaja i raspona djelovanja jednog preduzeća, kao i na odnose koje ono prema tome uspostavlja: šta proizvodi, kako kupuje i prodaje, da li se pridržava zakona, na koji način zapošljava, osposobljava i utiče na razvoj ljudskih resursa, koliko ulaže u lokalnu zajednicu i poštovanje ljudskih i radnih prava, na koji način doprinosi očuvanju životne sredine. Polazeći od postojećeg stanja i izražene problematike u oblasti korporativne sigurnosti, potrebno se posvetiti sve većoj sigurnosti u poslovanju kompanije, zbog čega je neophodno preduzeti sljedeće mjere:

1. Menadžment kompanija preduzeća, mora imati jasnu prognozu očekivanih stanja i biti spreman za donošenje kvalitetnih poslovnih odluka na planu prevencije svih oblika sigurnosti u poslovanju preduzeća.

2. Zaposleni u službama korporativne sigurnosti, treba da budu kompetentna lica koja će upravljati u procesima sigurnosti.

3. Korporativna sigurnost mora postati dio poslovne kulture svih zaposlenih sa ciljem objedinjavanja zahtjeva, potreba i očekivanja kako menadžmenta, tako i poslovanja preduzeća unutar vlastite svekupnosti.

4. Za korporativnu sigurnost je važno da se kvalitetno upravlja procesima sigurnosti, kao i da bez toga nema uspješnog poslovanja kompanije.

5. Sve više razvijati partnerske odnose, javnog i privatnog sektora, da se poslovanje/znanje korporacija javnog i privatnog sektora što više približe Vladinom sektoru sigurnosti, te međusobnu saradnju u cilju sveukupne sigurnosti društva.

6. U mjerama za korporativnu sigurnost treba da se podrazumijeva fizička i tehnička zaštita, zaštita biznisa, zaštita informacionog sistema, zaštita inteligentnog vlasništva, robnih marki i slično. Kroz provođenje strateških mjera i postupaka treba da se ostvari smanjenje sigurnosnih rizika, i unaprijedi planiranje za slučaj opasnosti od štete a da se u okviru mjera sigurnosti planiraju i pravne zaštite korisnika, vlasnika, radnika i imovine firme, poslovnih informacija kao i položaja preduzeća na tržištu.
Realizacijom ovih mjera došlo bi do poboljšanja korporativne sigurnosti u našim preduzećima, a to bi dovelo do sigurnijeg poslovanja preduzeća čime bi se stvorili preduslovi za donošenje kvalitetnih poslovnih odluka, a time jasnije i vidljivije istakle koristi od korporativne sigurnosti bez iziskivanja značajnijih investicionih ulaganja, čime se postiže efikasnija zaštita najvažnijih segmenata poslovne sigurnosti u odvijanju poslovnih procesa.

LITERATURA

[1] Bilandžić M. (2008.), Poslovno-obavještajno djelovanje: Business intelligence u praksi, Zagreb, AGM
[2] Hammer M., Champy J., (2004.), Reinžinjering tvrtke, Zagreb, MATE
[3] Ivandić Vidović D., Karlović L., Ostojić A., (2011.), Korporativna sigurnost, Zagreb, UHMS
[4] Javorović B., Bilandžić M., (2007.), Poslovne informacije i business intelligence, Zagreb, Golden marketing -Tehnička knjiga
[5] Mintas Hodak Lj., (2010.), Pravno okruženje poslovanja, Zagreb, MATE
[6] Puljić N., (2009.), Sigurnost i zaštita zdravlja na radu, Zagreb, Poslovni zbornik
[7] Zlatović D., (2010.), Intelektualno vlasništvo i marketing, Zagreb, INMAG
[8] Zdravka Krakara i suradnika, Korporativna informacijska sigurnost, Fakultet organizacije i informatike, Varaždin i Zavod za informatiku Hrvatske, 2014.
[9] Heid, Ulrich. Corpus linguistics and lexicography. U: Corpus Linguistics, an international handbook, vol. 1 (ur. Ludeling A. I Kyto M.) De Gruyter, Berlin, 2008.
[10] Ivandić Vidović, Karlović, Ostojić: Korporativna sigurnost, UHMS, Zagreb, 2011.
[11] Nikolić, M, Sinkovski, S: Korporativna bezbednost, osnove zaštite biznisa i preduzetništva, Beograd, 2013

Д-р Милан Милошевиќ
Факултет за пословне студије и право
Белград, Република Србија

М-р Бранислав Милосављевиќ
Институт за стратегиски истражувања
Белград, Република Србија

ИНФОРМАЦИОНО ВОЈУВАЊЕ ВО УКРАИНСКИОТ КОНФЛИКТ

Апстракт: и во современо време спорните прашања помеѓу државите, општествените групи и другите организирани човечки заедници, покрај бојното поле, се пренесуваат и (раз)решаваат во политичката, медиумската, научната, културната, спортската, информативната, информатичката, економската и меѓународната правна област. И покрај тоа што крајните цели и облици на конфликтите останале непроменети, забележливо е проширување на сферата и примена на нови методи и средства на вооружените судири. Една од основните крактеристики на современата војна е и диспропорцијата на конфликтните страни, во многу сегменти кои војната како општествена појава ја каректеризираат, како што се: цели, сили, средства, простор, време, начин на водење операции и слично. Актуелниот конфликт во Украина помеѓу останатото покажал нова димензија на вооружените конфликти во кои информационото војување има посебно место. Иако големите сили интензивно го користат информатичкото војување, во овој конфликт Русија покажала дека ја научила лекцијата од минатото и не си дозволила повторување на грешките. Покрај тоа, посебно е значаен високиот степен на координација и спроведување на различни активности со цел парализирање на противникот и рушење на неговите капацитети за давање успешен отпор.

Клучни зборови: украински конфликт, информациона војна, асиметрија, хибридни конфликти, медиуми, пропаганда.

INFORMATION WAR IN UKRAINE CONFLICT

Abstract: And at the same time, controversial issues between the state, social groups and other organized human communities, in the battlefield,are transferred and resolved in the political, media, scientific, cultural, sports, information, information, economic and international legal fields.Despite the fact that the ultimate goals and forms of conflict remained unchanged, it is noticeable the expansion of the sphere and the application of new methods and means of armed conflict. One of the basic features of the modern war is the disproportion of the conflicting sidesin many segments characterized by war as a social phenomenon, such as: goals, forces, resources, space, time, way of conducting operations.The current conflict in Ukraine has shown, among other things, a new dimension of armed conflicts in which information warfare has a special place. Although great forces are intensively using information warfareIn this conflict, Russia has shown that it has learned lessons from the past and did not allow itself to repeat the mistakes. In addition, there is a particularly high level of coordination and implementation of various

activities in order to paralyze the opponents and to undermine its capacity to provide a successful resistance.

Keywords: Ukrainian conflict, information war, asymmetry, hybrid conflicts, media, propaganda.

ПОЈАМ ИНФОРМАЦИОНИ РАТ

Информациони рат је нови облик рата у коме се информације користе као циљеви и средства ратовања, при чему се издвајају два основна значења овог појма. Првенствено се под информационим ратом подразумева битка за добијање поузданих, потпуних и благовремених информација али и спречавање да непријатељ дође до њих. Благовремено сазнавање потребних података о противнику (бројност, распоред и кретање непријатељске војске, наоружавање, стање морала и слично) не само да олакшава планирање и извођење операција већ је уједно и предуслов за било какве озбиљније активности у домену рата, спољне политике, спољне трговине. С друге стране информациони рат представља и коришћење информација као циља напада, као посебног оружја (средства ратовања)[27].

Поред наведених, егзистирају и многа друга одређења овог појма, при чему је основни узрок различитости у информативној револуцији и брзином еволуције сајберпростора микрорачунара и додатних информационих технологија. Неспорна је чињеница да је у току прави бум технологије, те да је живот незамислив без компјутерских средстава, отвара сасвим нове могућности коришћења и у ратне сврхе. С тим у вези појављују се могућности напада на противничке информационе системе – рушење веб-сајта влада страних држава, уношење на њега садржаја по сопственом избору, непримећено убацивање погрешних информација у информациони систем противника, и друго[28]. Међутим оно што информативни рат чини примамљивим јесте широки спектар асиметричних могућности за смањење борбеног потенцијала непријатеља. Због свог значаја који има често се употребљава и синтагма стратегијски информациони рат, која подразумева различите војне и невојне мере (нпр. ометање војног и државног руководства, довођење у заблуду непријатеља, формирање пожељних јавних мишљења, организације анти-владиних активности и слично) као део виталне подршке у циљу смањења способности противника[29].

СПЕЦИФИЧНОСТ УКРАЈИНСКОГ СУКОБА

Оружани сукоби модерног доба одвијају се преко неоружаних (специјалне операције) и оружаних садржаја. Уобичајено, сукоб почиње неоружаним садржајима, наставља се (по потреби) оружаним дејствима у којима и даље

---

[27] Кривокапић, Б.: Енциклопедијски речник међународног права и међународних односа, ЈП Службени глаасник, Београд, 2010, стр. 353-354

[28] Roger C. Molander, Andrew S. Riddile, Peter A. Wilson: Strategic Information warfare, A New Face of War, National Defense Research Institute (RAND), Santa Monica, 1996, p.1-3

[29] Sazonov, V., Müür, K., Mölder, H.: Russian Information campaign against the Ukrainian state and Defence Force, NATO Strategic Communications Centre of Excellence Estonian National Defence College, Tartu, 2016, p. 67-68

трају неоружана; неоружана дејства трају непрекидно, док се оружана, ако до њих дође, догађају повремено и ациклично. С тим у вези, савремени рат у многим својим деловима и у односу на своје појавне феномене, добија нове димензије, јер „утицај политичке власти на војне операције постаје све већи, противречан и често неоријентисан на решење проблема. Међународно право је постало ограничавајући фактор за вођење операција, при чему се примена противничких и сопствених психолошких операција добија на све већем значају. Ко успе да задобије сопствена и противничка „срца и умове“, или да их не изгуби, добиће рат. У почетној фази оружаног напада не може се искључити и привредни рат уз комбинацију са психолошким операцијама, укључујући уцењивање, привредне блокаде, заплену или блокирање имовине у иностранству, привредне преваре других држава и слично“[30].

Посматрано кроз призму Украјине интензивна борба за „срца и умове” украјинског становништва почела још 2004. године, кроз активности политичких актера у овој држави; за једне да их добију, а за друге да их не изгубе. Многе околности као што је неспособност тадашње политичке елите Украјине да недвосмислено одреди стратешко опредељење између ЕУ и Руске Федерације утицали су на ескалацију унутрашњих сукоба крајем 2013. године и почетак протеста на стварање атмосфере екстремног насиља кијевском Тргу независности (Мајдану), који су од краја новембра до почетка децембра прерасли у масовне и насилне свакодневне протесте. Јануковичев споразум о економској помоћи с Русијом, науштрб преговора с Европском унијом, „проевропски” опредељени грађани Украјине окарактерисали су као издају националних интереса. Западни медији одмах су ове догађаје описали као украјинску револуцију, али је тешко сложити се с тим да су догађаји на „Еуромајдану” одговарали појму револуције. Револуција подразумева радикалну промену друштвеног система и радикално превладавање, тј. укидање, постојећих друштвених односа. За разлику од тога, захтеви демонстраната на „Еуромајдану” састојали су се од залагања за промену власти унутар истог, капиталистичког, система друштвених односа. У најкраћем, захтеви демонстраната били су за напуштање блиских односа са Руском Федерацијом и стварање партнерских са Сједињеним Америчким Државама и Европском унијом. Сви ови догађаји умногоме подсећају на обојену револуцију али према украјинском сценарију.

Од 2014. године, током Украјинске кризе улога стварне војне интервенције била је ниска у односу на различите форме асиметричног рата као што су информативни рат, економске мере, сајбер рат и психолошки рат на свим нивоима. Наведене форме асиметричног рат називају се једним именом хибридни рат, појам који је често коришћен у описивању сложености украјинске кризе. С тим у вези значајно је напоменути да се у хибридном рату оружана сила углавном користи као средство одвраћања а не као средство отворене агресије. Међутим оно што је било ново у овом сукобу је висока ефикасност у многим случајевима скоро реална временска координација различитих средстава од политичких, војних, специјалних операција до

[30] Lätsch, D., Moccand D.:Moderne Verteidigung, Schweizer Armee, Military Power Revue, 2/2010, p. 3–10

информационих мера и активности[31]. У таквим околностима иако релативно невидљив, незамислив је значај служби безбедности сукобљених страна. С тим у вези, амерички Стејт Департмент је истакао да Русија наставља да спинује лажи и неистине како би оправдала своје илегалне акције у Украјини. Тако, на пример, тврдњу Русије да руски агенти нису активни у Украјини оповргава наводним чињеницама да је украјинска влада у априлу 2014. године ухапсила више од десетак Руса за које се сумња да су припадници руских обавештајних служби. Истичу да су многи од њих у моменту хапшења били наоружани. У првој недељи априла 2014. године, влада Украјине је добила информацију да су руски „гру" официри активирали појединце у Харкову и Доњецку, са саветима и инструкцијама да се воде протести, заузимају и држе под опсадом зграде владе, одузима оружје из владиних магацина и да их премештају за друге насилне акције[32]. На крају, али не без значаја који одражава специфичност украјинског оружаног сукоба је и утицај глобалног тренда приватизације на рат и учешће великог броја плаћеника на обе стране, што у многоме употпуњује слику сложености украјинског сукоба и разгранатост његових форми.

ИНФОРМАЦИОНО РАТОВАЊЕ У УКРАЈИНИ

Ратови који су се водили или се воде после распада Источног блока, спадају у групу ратова под називом ратови савременог доба. На савремене ратове је веома тешко применити класични Клаузевицев приступ, који подразумева да рат започиње објавом рата, те да се заснива на суровим, али легитимним поступцима. Актуелна руска војна доктрина из децембра 2014. године експлицитно наводи да су у савременим ратним дешавањима информациона супериорност је преко потребна да би се постигла победа на физичком бојном пољу. У поређењу са ратом у Грузији 2008[33]. године, када је Русија погрешно оценила важност информационог ратовања и на крају је изгубила информативни рат са Западом, Русија је научила своје лекције и сада поклања више пажње улози информација у светлу високе технологије, стратешких комуникација и савременог рата.

За рат у Украјини могло се рећи да у полеђини има наду „бољег живота" који нуде велике силе, а да је странама у сукобу све остало подређено и дозвољено у остварењу тог циља. Савременим оружаним сукобима циљ је потпуна стратешка парализа непријатеља и ланчани „домино" ефекат урушавања капацитета непријатеља да пруже успешан отпор, циљањем на чворне и виталне тачке не само система одбране, већ друштвеног система као целине. Да би се то остварило, примењује се метод који ратну ситуацију посматра као скуп међусобно повезаних друштвених подсистема које је потребно онеспособити, било директно оружаним путем, било путем економских акција, циљањем информационих токова или пак путем

[31] Sazonov, V.,Kristiina, M., Holger M.: Russian Information campaign against the Ukrainian state and Defence Force, NATO Strategic Communications Centre of Excellence Estonian National Defence College, Tartu, 2016, p. 67-68

[32] Амерички Стејт Department, „Nastavak ruske fikcije još deset lažnih tvrdnji o Ukrajini", Novi vek, broj 7, 2014, str. 14-22.

[33] Niedermaier, K.: Countdown to War in Georgia. Russia's Foreign Policy and Media Coverage of the Conflict in South Ossetia and Abkhazia, Minneapolis: East View Press, 2008, pp. 452-455

дипломатског деловања заснованог највећим делом на методу притиска на вршење одређене радње или одвраћања силом.
Када је реч о информационом ратовању руске стране у Украјинском сукобу, на западу се најчешће се спомињу Russia Today и Спутник као носиоци информационе кампање преко мас медија. Поред тога коришћени су и многи телевизијски канали као што су Руски национални телевизијски канали LifeNews, Россия1, Россия24, Первый канал, НТВ, РЕН ТВ, као и многи други и они забрањени у Украјини, али које је могуће пратити преко сателита.
Међутим, они су само јасно уочљиви елементи у веома широком спектру укључујући оне које су били прикривени у својим активностима. С тим у вези медији су имали сасвим другачији приступ и различите форме информација, од једноставне измишљотине, преко конфузија са полуистинама, до софистицираних аргумента. То је имало за циљ стварање доминације информација од стране Руске стране. Један од циљева је и ширење панике међу Украјинцима, стварање и одржавање неповерења између украјинске државе и украјинске војске и деморализација војника и њихових команди. Руска пропагандна машинерија није имала за циљ само војнике, већ и њихове рођаке и пријатеље. Циљ је поделити породицу и друге друштвене групе, узимајући у обзир процене даљег погоршања сукоба у складу са етничким, верским, језичким, политичким и регионалним идентитетом. У остваривању овог циља између осталог се користе и различите методе манипулације информацијама у мас медијима а ради остваривања превласти у информативно-психолошком сукобу. Према Руским изворима основни принципи медијске кампање су:

– скривање критичних (важних) информација,
– скривање драгоцених у маси бескорисних информација,
– поједностављење, потврде и понављање информација,
– „директне“ лажи које имају сврху дезинформације домаћег становништва и међународне јавности,
– увођење забране за одређене облике информација или категорија вести,
– употреба концепата и термина чији значење је нејасно, што отежава стварање праве слике догађаја,
– препознавањем слика, познати политичари или познате личности могу учествовати у акцијама и на тај начин вршити утицај на њихове следбенике и њихов поглед на догађаје и
– пружање негативних информација,које је ће јавност лакше прихватити него када се ради о позитивним[34].

Руски концепти борбених дејстава су у сталном развоју и будуће војне акције неће личити на досадашње. С друге стране према проценама САД-а источна Украјина поред осталог представља уједно и „настанак“ лабораторије за будуће ратовање у овом веку. У овом сукобу Русија је искористила свој приступ високо софистицираној и ефикасној технологији за напада, укључујући ГПС преваре у циљу савладавања навигација и система вођења[35].

[34] Kuleshov Y. et al.: Информационно-психологическое противоборство в современных условиях: теория и практика Information-Psychological Warfare In Modern Conditions, Vestnik Akademii Voyennykh Nauk No. 1 (46), 2014., p. 107.
[35] Giles K.: Handbook of Russian Information Warfare, NATO Defense College, Rome, 2016, p. 64

За Русију, информативни рат није активност ограничено искључиво на ратни период или на почетну фазу сукоба пре него што почну непријатељства, што између осталог подразумева и припрему информација о борбени простор. За разлику од других облика и метода супротстављања, информационо ратовање се спроводи и у миру.

ЗАКЉУЧАК

Савременим оружаним сукобима циљ је потпуна стратешка парализа непријатеља и ланчани „домино“ ефекат урушавања капацитета непријатеља да пруже успешан отпор, циљањем на чворне и виталне тачке не само система одбране, већ друштвеног система као целине. Да би се то остварило, примењује се метод који ратну ситуацију посматра као скуп међусобно повезаних друштвених подсистема које је потребно онеспособити, било директно оружаним путем, било путем економских акција, циљањем информационих токова или пак путем дипломатског деловања заснованог највећим делом на методу притиска на вршење одређене радње или одвраћања силом.

Информациони рат се у многим државама и војним групацијама ставља у ниво оружја за масовно уништење и равноправно учествује у остварењу стратешких циљева упоредо са оружјем за масовно уништење, класичним војним снагама, економијом, политичко дипломатским и обавештајним снагама, те је предмет стратегије и тактике на највишим нивоима власти и оружаних снага. Појављује се као претходница војних операција, током операција као њихов део и у експлоатацији њихових резултата

Информациони рат намеће велике обавезе и рад обавештајнобезбедносних служби, а чије се обавезе, место и улога мењају проширењем на читав спектар информација из свих области функционисања неке државе, а појачани су и захтеви за провером и контролом више пута прикупљених и проверених информација. V ту сврху у водећим земљама проширују се обавештајно-безбедносни капацитети, са

новим и специфичним областима интересовања, а рад у миру, по интензитету се не разликује од рада у рату. На основу праћења, протока и садржаја информација процењују се будуће кризне ситуације, интензитет будућих сукоба, правци и циљеви напада и одбране, те употреба снага и средстава војних и финансијских ефектива. Информацијама се усмеравају догађаји, политика, реаговања, сукоби, подршка и последице.

Истовремено морамо нагласити да се са развојем нових технологија јављају и нови видови претњи које такође треба пратити, односно развијати технике и технологије за заштиту, уз коришћење најсавременијих уређаја и система.

С друге стране, ратно поље је у савременим ратовима нестабилно, без чврстих граница и прожима цивилни живот и све поре друштва. У тим условима учинити од своје слабости предност и заобићи силу свог противника како би се постигла несразмерна штетност је карактеристика савремених асиметричних ратова. Сувишно је рећи да и поред привидних линија фронта у Украјини, ратни вихор провејава целом Украјином носећи са собом дах нових облика рата не бирајући жртве на свом путу.

Заједно са другим руским инструментима моћи, концепт информативног рат, постао је предмет изненадног и интензивног интереса на Западу почетком Украјинске кризе 2014. године. Међутим, овде не треба тражити сензационализам јер се не ради о феномену, већ у томе да је Руска моћ била подцењена од краја Совјетског Савеза.

ЛИТЕРАТУРА

1. Američki Stejt Department, „Nastavak ruske fikcije još deset lažnih tvrdnji o Ukrajini", Novi vek, broj 7, 2014.
2. Giles K.: Handbook of Russian Information Warfare, NATO Defense College, Rome, 2016.
3. Кривокапић, Б.: Енциклопедијски речник међународног права и међународних односа, ЈП Службени глаасник, Београд, 2010.
4. Kuleshov Y. et al.: Информационно-психологическое противоборство в современных условиях: теория и практика Information-Psychological Warfare In Modern Conditions, Vestnik Akademii Voyennykh Nauk No. 1 (46), 2014.
5. Lätsch, D., Moccand D.:Moderne Verteidigung, Schweizer Armee, Military Power Revue, 2/2010.
6. Niedermaier, K.: Countdown to War in Georgia. Russia's Foreign Policy and Media Coverage of the Conflict in South Ossetia and Abkhazia, Minneapolis: East View Press, 2008.
7. Roger C. Molander, Andrew S. Riddile, Peter A. Wilson: Strategic Information warfare, A New Face of War, National Defense Research Institute (RAND), Santa Monica, 1996.
8. Sazonov, V., Müür, K., Mölder, H.: Russian Information campaign against the Ukrainian state and Defence Force, NATO Strategic Communications Centre of Excellence Estonian National Defence College, Tartu, 2016.

Doc. dr Milanović Sedžad
Ministar privrede SBK
sedzadmilanovic@ymail.com
Doc. dr Pajević Maid
Visoka škola „Logos centar“ Mostar
mpajevic.logos2013@gmail.com
Mr Dizdarević Sandi
Tužilaštvo HNK
sandi_lps@hotmail.com

Poslovna obavještajna djelatnost i špijunaža: sličnosti i razlike

Autori ističu da u suvremenim uslovima poslovanja koje karakterizira ubrzana globalizacija i hiperkonkurencija poslovne informacije predstavljaju istovremeno moć, kapital i znanje, konkurentsku prednost odnosno ključni resurs upravljanja. Pravovremena, sadržajna i tačna poslovna informacija jest preduslov donošenja kvalitetne poslovne odluke, a time i ostvarenja poslovnog uspjeha. Efikasno upravljanje podacima i informacijama, poslovnim subjektima omogućuje donošenje efikasnih strateških, taktičkih i operativnih odluka. Autori naglašavaju da business intelligence podrazumijeva i korjenite promjene u koncepciji poslovnog promišljanja i funkcioniranju. »Business intelligence« (poslovno-obavještajna aktivnost) je aktivnost u poslovnom svijetu koju planiraju, organiziraju, i provode poslovni subjekti, pri čemu ta aktivnost podrazumijeva proces legalnog prikupljanja javnih i svima dostupnih podataka etičkim sredstvima, njihovu analizu i pretvaranje u gotove poslovno obavještajne analize (»znanje«) radi pružanja podrške menadžerima poslovnog subjekta u cilju donošenja i realizacije što kvalitetnijih poslovnih odluka, što je u suprotnosti sa špijunažom kao ilegalnom i nemoralnom aktivnosti. S tim u vezi, autori pokušavaju da daju odgovore na dva problemska pitanja. Kako napraviti distinkciju između poslovne obavještajne djelatnosti i špijunaže i kako poslovno obavještajna djelatnost može pomoću menadžeru da ponudi odgovore na sljedeće izazove u poslovnom ambijentu koji se reflektiraju kroz sljedeća podpitanja: Kakva je informacija potrebna? Kada je informacija potrebna? Ko je treba? Gdje je potrebna? Zašto je potrebna? Koliko to košta? Kako poboljšati konkuretnost na tržištu?
Ključne riječi: Korporativna sigurnost, špijunaža, poslovna obavještajna djelatnost, business intelligence i competitive intelligence.

Business intelligence and espionage: similarities and differences

The authors point out that in contemporary business environments characterized by accelerated globalization and hypercompetition business information is simultaneously the power, capital and knowledge, as a competitive advantage, and key management resource. Timely, accurate and correct business information is a prerequisite for making a quality business decision and thus achieving business success. Efficient data and information management enables businesses to make effective strategic, tactical and operational decisions. The authors point out that business intelligence implies root changes in the business concept and functioning concept. "Business Intelligence" is an activity in the business world that is planned,

organized, and run by business entities. This activity implies the process of legal collection of public and all available data by ethical means, their analysis and conversion into a business intelligence analysis ("Knowledge") in order to provide support to the managers of a business entity in order to make and realize quality business decisions as opposed to spying that is illegal and immoral activity. In this connection, the authors are trying to answer two problem questions. How to make a distinction between business intelligence and espionage and How business intelligence can help the manager to respond to the following challenges in the business environment reflect through the following sub-questions: What information is needed? When is information needed? Who needs it? Where is it necessary? Why is it necessary? How much does it cost? How to Improve Market Competitiveness?

Key words: Corporate Security, Espionage, Business Intelligence, Business Intelligence and Competitive Intelligence

Uvodna razmatranja

U današnjoj epohi gospodarskog razvoja jedne zemlje, u okviru kojih djeluju korporacije postoji niz otežavajućih faktora za stabilno poslovanje, između kojih se posebno ističu: prikupljanje poslovnih informacija, i njihova obrada, te zaštita vlastitih informativnih kapitala. Sigurnost kao znanost predstavlja dinamički proces prilagođavajući se društvenim tokovima. Đozić pravilno zaključuje da: "Danas u svijetu egzistiraju brojni pojmovi koji se izravno ili neizravno vežu s područjem koje obuhvaća pojam gospodarske špijunaže".[36] Razvojem društva i gospodarstva razvijale su se i potrebe za poslovno obavještajnom djelatnosti i za razvoj sofisticiranih alata za prikupljanje, obradu i analizu informacija. Upravo iz tih razloga, Brkić i Dizdarević ukazuju da: "Najmanja neopreznost srednjeg i top menadžmenta može imati nepopravljive posljedice, dok s druge strane na tržištu opstaju ona preduzeća koja raspolažu sa pravovremenom i kvalitetnom informacijom, jer ko raspolaže sa pravovremenom i kvalitetnom informacijom taj opstaje na tržištu".[37] Znanstvenici se slažu u činjenici da nije svako prikupljanje informacija gospodarska špijunaža. Ovakvo stajalište predstavlja temeljni cilj u radu kojim se žele pružiti promišljanja autora vezanih za distinkcije između poslovno obavještajne djelatnosti i špijunaže. Za pravilnu distinkciju elemenata koji ulaze u sastav pojmova poslovno obavještajne djelatnosti i špijunaže koristiti će se ponderi, poput sredstva kojim se prikupljaju informacije, zone u okviru kojih se vrši prikupljanje poslovnih informacija, pozadina zbog kojih se prikupljaju informacije i pravni element kojim se određuje klasifikacija poslovne informacije. Upravo ponder "tajne poslovne informacije" Pajević pravilno sintetizuje u paradigmu špijunaže, na način da se: "Prodire u institucije i objekte stranih država preko kojih se može doći do privrednih, naučnih, geografskih i drugih tajni". Evidentno je da se "tajna poslovna informacija" javlja kao fundamentalan element temeljem kojih se može napraviti primarna distinkcija između poslovno obavještajne djelatnosti i špijunaže. Jedno od ključnih pitanja

[36] Đozić, T. (2012). Gospodarska špijunaža, paradigma modernog svijeta, str. 55.
[37] Brkić, K., Dizdarević, S. (2017). Metodi, trendovi i alati u korporativnoj sigurnosti, poslovna špijunaža-mit ili stvarnost, Međunarodna konferencija IUT, Zbornik radova.

pojavljuje se u vidu zašto je konkretna informacija potrebna, kada i kome, i kako će se ista pravilno iskoristiti za prosperitet preduzeća? Navedena pitanja, samim svojim postavljanjem određuju i domen te način prikupljanja, odnosno da li je neophodno prodrijeti u sivu zonu drugog preduzeća ili ostati u plavoj dozvoljenoj zoni. Odgovori na postavljena pitanja omogućavaju menadžeru sigurnosti kreiranju strateških smjernica koji prate cjelokupnu korporativno poslovnu politiku. Na ovakav način korporativna sigurnost kroz poslovno obavještajnu djelatnost postaje centralni proaktivno-analitički odjel za pružanje fundamentalne potpore top menadžmentu u donošenju značajnih poslovnih odluka.

POSLOVNO OBAVJEŠTAJNA DJELATNOST

U svakodnevnom životnom procesu, svaka individua ima potrebu za prikupljanje informacija temeljem kojih kreira vlastito ponašanje, i donosi značajne životne odluke. Naučnici se nalaze u kontinuiranom prikupljanju podataka temeljem kojih provjeravaju vlastita istraživanja, kreiraju nove teorije i riješavaju mnoge znanstvene dileme. Menadžeri različitih korporacija na svakodnevnom nivou koriste i upotrebljavaju informacije u cilju donošenja poslovnih odluka. Ovakvo prikupljanje informacija oslanja se na vlastite potrebe, bez jasnog formalnog i strukturalnog elementa, čime se kao takvo ne može smatrati poslovno obavještajnom djelatnošću. Autori knjige Privatna bezbjednost, ukazuju da: "Organizovanje prikupljanja informacija na promišljen način, za specifične ciljeve i rezultate zahtjeva formalnu strukturu".[38] Pored strukture, ističe se i efektivana upotreba informacija, kao i efektivna kontrola informacija. Efektivna formalna upotreba zahtjeva disciplinovano prikupljanje, analizu, distribuciju i primjenu dobijenih informacija. Redefiniranje obavještajne djelatnosti odvijalo se kroz različite istorijske i društvene faze. Do kraja XX vijaka, obavještajno prikupljanje podataka bilo je u isključivoj nadležnosti države i njenih specijaliziranih službi. Pajević ukazuje i pravilno zaključuje da je evolucija čovječanstva doživjela nekoliko obavještajnih revolucija. Kao posebno interesantnu, Pajević ukazuje na: "Privatizaciju"obavještajne djelatnosti u smislu da korporacije sistematično koriste obavještajne informacije u cilju veće konkurentnosti, razvitka i profita".[39] Stevan Dedijer je 70-tih godina XX vijeka započeo pionirski proces izučavanja i razvijanja poslovne obavještajne djelatnosti koji je u tim godinama ukazao da se na godišnjoj razini za poslove prikupljanja poslovnih informacija utroši oko 70 milijardi dolara. Prema Zebiću, poslovno obavještajna djelatnost predstavlja: "Legalno i etičko, sustavno i smišljeni process definiranja, prikupljanja i analiziranja informacija o konkurentima, potrošaćima, kao i bilo kojem drugom aspektu vanjske ili unutarnje okoline poduzeća te diseminiranja proizvoda tog procesa menadžmentu poduzeća radi podrške prilikom donošenja strateških odluka ključnih za poslovanje preduzeća".[40] Trivan također u svojoj studiji ukazuje na bitne elemente poslovno obavještajne djelatnosti. Trivan ističe da: "Savremeno poslovno odlučivanje je kompleksan process koji zahtjeva mnoštvo raznovrsnih informacija, kako internih, tj. onih koje potiču iz korporacije, tako i esternih, koje dolaaze iz

[38] Daničić, M., Stajić, Lj. (2008). Privatna bezbjednost, Banja Luka, str. 225.
[39] Pajević, M. (2013). Savremene obavještajne teorije, Mostar, str. 253.
[40] Zebić, O. (2010). Poslovno obavještavanje i oblikovanje poslovnih strategija hrvatskih preduzeća, Specijalistički poslijediplomski rad, Sveučilište u Zagrebu, str. 7/8.

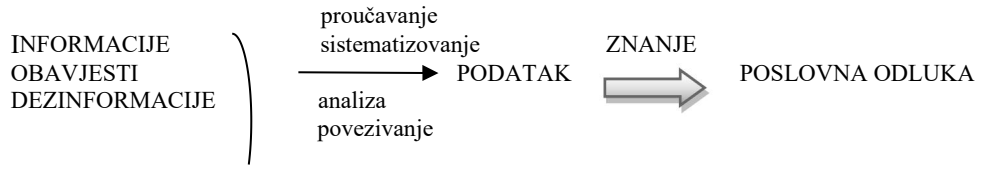
njenog okruženja".[41] Ekonomsko obavještajni procesni okvir predstavlja fundamentum u poslovno obavještajnom djelovanju. Pajević ekonomsko obavještajni procesni okvir dijeli:

- "Definiranje ekonomsko-obavještajnih ciljeva
- Identifikacije izvora, organiziranja informacijskih izvora i prikupljanja
- informacija,
- Analize i ocjena
- Izvještavanje i diseminacija"[42].

Bilandžić, u svom pristupu korporativnoj sigurnosti ukazuje da pod pojmom poslovno obavještajne djelatnosti se podrazumjeva legalno prikupljanje poslovnih informacija, tj. javno dostupnih podataka, obradu tih informacija u poslovne analize radi pružanja podrške menadžmentu korporacije u donošenju i realizaciji što kvalitetnijih poslovnih odluka za očuvanje njenog položaja u poslovnom okruženju. Uže definisanje poslovno obavještajne djelatnosti za razliku od Bilandžića pruža Rudan, prema kome ista predstavlja: "Djelatnost praćenja spoljnog okruženja kompanije u traganju za informacijama koje su relevantne za process odlučivanja u okviru poslovnog subjekta".[43] Slično promišljanje Rudanu, ima i Mujanović prema kome je poslovno obavještajna djelatnost usmjerena isključivo na prikupljanje, tretiranje, analiziranje i korištenje strateških informacija za neku kompaniju. Prema Mujanoviću, u pitanju je legalan i etički dopušten način prikupljanja informacija, koji se vrši korišćenjem savremene tehnologije ili angažovanjem ljudskog faktora.[44] Bazdan ističe da poslovno obavještajna djelatnost, odnosno poslovno obavještajna služba ima primarnu zadaću provoditi i realizirati dio gospodarskih ciljeva čelnog menadžmenta, kojim rukovodi glavni i izvršni director, primjenom legalnih metoda djelovanja.[45] Zebić ukazuje i pravilno uviđa da je osnovni kriterij za postojanje poslovno obavještajna djelatnost njeno legalno i etičko provođenje. Isti autor, ukazuje: "Korištenje OSINT[46] metoda i legalnih i benignih aspekata HUMINT metoda poslovno obavještajne djalatnost dodatno utvrđuju prethodnu navedenu činjenicu o zakonitom i moralnom djelovanju poslovno obavještajnog sustava i procesa".[47] Kao vrlo bitna odrednica poslovno obavještajne djelatnosti, u kojoj se slaže većina autora jeste znanje. Sam proces poslovno obavještajne djelatnosti odvija se kroz određivanje zone gdje se treba tragati za informacijom, prikupljanjem, obrađivanjem, sređivanjem, analiziranjem i dostavljanjem. Na narednoj slici prikazan je krajnji ishod skupa informacija koje predstavlja podršku top menadžmentu.

---

[41] Trivan, D. (2012). Korporativna bezbjednost, Beograd, str. 111.
[42] Pajević, M. (2017). Obavještajne studije, Kiseljak, str. 212.
[43] Rudan, V. (2008). Konkurencija na nišanu-Teorijski i praktični aspekti istraživanja konkurencije, Hesperiaedu, Beograd, str. 95.
[44] Preuzeto iz knjige Trivan, D. (2012). Korporativna bezbjednost, Beograd, str. 114.
[45] Bazdan, Z. (2009). Menadžeri moraju znati: poslovno obavještajna djelatnost kreira najvažniji resurs upravljanja, Poslovna izvrsnost Zagreb, Zagreb, str. 62.
[46] OSINT-*(Open source intelligence)*-Prikupljanje obavještajnih podataka iz otvorenih izvora: prikupljanje obavještajnih podataka iz širokog mnoštva javno dostupnih izvora (mediji, vladine informacije, naučnih publikacija). HUMINT-(*Human intelligence*): prikupljanje podataka iz ljudskih izvora. Pajević, M. (2017). Obavještajne studije, Kiseljak, Skraćenice.
[47] Zebić, O. (2010). Poslovno obavještavanje i oblikovanje poslovnih strategija hrvatskih preduzeća, Specijalistički poslijediplomski rad, Sveučilište u Zagrebu, str. 10.



Bilandžić, pravilno ističe da se distinkcija između poslovno obavještajne djelatnosti i špijunaže može odrediti temeljem zona u okviru kojih se vrši prikupljanje informacija, obavjesti i podataka. Isti autor ističe postojanje tri zone: bijela zona, siva zona i crna zona. Na narednoj slici prikazane su zone prikupljanja podataka i informacija po Bilandžiji.

Slika1. Zone prikupljanja informacija

Izvor: Bilandžić, M. (2008) Poslovno-obavještajno djelovanje - Business Intelligence u praksi, Zagreb, AGM

INFORMACIJE I POSLOVNE INFORMACIJE

U današnjoj epohi razvoja IT tehnologije poslazeći od općeg kao posebnom ističe se opterećenost sa velikim spektrom javno dostupnih informacija. Putem medija plasiraju se sve vrste informacija, uključujući i informacije o poslovnim uspjesima ali i neuspjesima određenih poslovnih korporacija. Društvene mreže, poput facbooka, instangrama i drugih omogućavaju prikupljanje velikog broja dostupnih obavjesti i informacija. Već u samom početku uviđa se prostorna otvorenost i dostupnost velike količne obavjesti i informacija. Informacije ovakvog karaktera, po svojoj suštini mogu predstavljati samo materijal "sirovog karaktera", od kojeg se može poći u prikupljanje vjerodostojne informacije. S druge strane, informacije ovakve dostupnosti mogu se koristiti kao potvrđujuće, u odnosu na već postojeću informaciju. Zebić pod informacijom podrazumjeva: "Značenje koje se pridružuje podacima uz pomoć poznatih konvencija što se koriste za njihovo interpretiranje".[48] Vidović ističe da se: "Upravo na temelju informacija i uz pomoć njih donose odluke, obavljaju najrazličitiji zadaci, uspostavljaju odnosi, planiraju aktivnosti, stječu nova znanja i spoznaje".[49] Isti autori ukazuju da je neophodno napraviti jasnu razliku između podatka i informacije, te da isti ne predstavljaju sinonime. Identično stajalište ističu Brkić i Dizdarević, ukazujući da: "U praktičnom smislu podatak ima

[48] Zebić, O. (2010). Poslovno obavještavanje i oblikovanje poslovnih strategija hrvatskih preduzeća, Specijalistički poslijediplomski rad, Sveučilište u Zagrebu, str. 14.
[49] Vidović, D. Karlović, L. Ostojić A. (2011). Korporativna sigurnost, Zagreb, str. 93.

veću snagu jer predstavlja već utvrđenu činjenicu. Informacija je dio činjenice, odnosno podatka koja je rezultat određene vrste saznanja".[50] Iako ne postoji jasna distinkcija između pojmova podatak, obavjest, informacija, jer se veoma često isti isprepliću. Upravo iz tih razloga Zebić pravilno ističe i zaključuje da se u krajnjoj instanci mogu nazvati zajedničkim nazivnikom "intelligence". Trivan u svojoj studiji pruža dosta široku definiciju poslovnih informacija, prema kome su to: "Sva saznanja koja su u funkciji unutrašnjeg i spoljnog djelovanja korporacija, tj. sve infromacije za poslovanje i obavljanje poslovnih interesa i ciljeva".[51] U pravnom smislu, podatak je direktno vezan za termin poslovna tajna, prema kojem se ista definiše kao: "Podatak ili isprava koja je zakonom, drugim propisom ili općim aktom privrednog društva, ustanove ili druge pravne osobe određen poslovnom tajnom, a koji predstavlja proizvodnu tajnu, rezultat istraživačkog ili konstrukcijskog rada, te drugi podatak zbog čijeg bi priopćavanja neovlaštenoj osobi mogle nastupiti štetne posljedice za njezine privredne interese".[52] Iz pravne definicije evidentno je nekoliko bitnih elemenata, koji se odnose na strukturu u kojoj se mogu javiti podaci. To mogu slike, dokumenti, video zapisi, kriptovane poruke i dr. Upravo i sam zakonodavac kroz odredbe Zakona o krivičnom postupku ukazuje da pod zabilješkom se ima smatrati: "Spisi, slova, riječi ili brojevi i njihovi ekvivalenti, zapisane rukopisom, otkucane pisaćom mašinom, odštampane, fotokopirane, fotografisane, zabilježene magnetskim impulsima, mehanički ili elektronski ili nekim drugim vidom sakupljanja podataka".[53] Ako je jasna definicija poslovno obavještajne djelatnosti kao legalnog i etičkog djelanja s ciljem dolaska do informacija, Brkić i Dizdarević u svojoj studiji pravilno postavljaju pitanje: kako onda dolazi do prodiranja, odnosno curenja informacija i poslovnih tajni korporacija i preduzeća? Pored postavljenog pitanja, daje se i jasan odgovor: "nizom aktivnosti koje se nazivaju Špijunaža".[54] Sam tim prikupljanje informacija više ne predstavlja trošak, već potrebu i investiciju.

POSLOVNA ŠPIJUNAŽA

Osnovna distinkcija između poslovne obavještajne djelatnosti i špijunaže najeklatantnije se može opisati kroz primjer, kada su svojetski inžinjeri 1974. godine u okviru kulturno-tehničke saradnje između SAD-a i SSSR-a posjetili tvornicu Boeinga u Tacomi. Tom prilikom operativci su uz pomoć cipela, čiji su đonovi bili premazani ljepilom, sakupljali metalne strugotine avionskih legura, s cilje kasnijeg proučavanja materijala. Na ovom primjeru vidljivo je neetičko djelovanje, korištenjem tajnih sredstava s ciljem dolaska do tuđih tajni. Aleksić ističe da pod špijunažom se najkraće treba podrazumjevati: "krađu tuđih otkrića, pronalazaka ili patenata, zatim tehnoloških procesa proizvodnje za čije su ispitavanje i usavršavanje usložene ogromne svote novca i dugogodišnji naporni rad".[55] Quinn iznosi kako process poslovno obavještajnog djelovanja vidi kao proces prikupljanja

[50] Brkić, K., Dizdarević, S. (2017). Metodi, trendovi i alati u korporativnoj sigurnosti, poslovna špijunaža-mit ili stvarnost, Međunarodna konferencija IUT, Zbornik radova.
[51] Trivan, D. (2012). Korporativna bezbjednost, Beograd, str. 111.
[52] Krivični zakon Federacije Bosne i Hercegovine, član 2. stav. 24. („Službene novine F BiH, broj: 09/03").
[53] Zakon o krivičnom postupku Federacije BiH, član 21. tačka n) („Službene novine F BiH, broj: 35/03, 37/03, 56/03").
[54] Brkić, K., Dizdarević, S. (2017). Metodi, trendovi i alati u korporativnoj sigurnosti, poslovna špijunaža-mit ili stvarnost, Međunarodna konferencija IUT, Zbornik radova.
[55] Aleksić, L.Ž. (1979). Kriminalistika. Beograd, str. 377.

poslovnih ili konkurentskih informacija putem legalnih i etičkih metoda, dok pod gospodarska špijunaža predstavlja "potajno prikupljanje osjetljivih, restriktivnih ili posebno klasificiranih informacija, s time da industrijska špijunaža obuhvata i krađu informacija od svojih izravnih poslovnih konkurenata". Nači rada u okviru poslovne špijunaže uvijek je tajan, te time i sredstva koja se koriste predstavljaju svojevrsnu paradigmu. Kanadski stručnjak Potter, ukazuje da se ekonomska špijunaža direktno vezuje za karakter informacije za kojom se traga. Takve informacije mogu pomoći jednoj državi nauštrb druge, što će se posebno ogledati u različitim poslovima gospodarske prirode, investicijama, produktivnosti, konkurentnosti ili gospodarskom rastu.[56] Upravo sam Potter, ukazuje na zone u okviru kojih se može prodrijeti u svijet tuđih tajni, klasificirajući ih u:

- primarna ili zelena i sekundarna ili žuta zona. Radi se o zonama u okviru kojih se podaci prikupljaju kroz otvorene i poluotvorene izvore,
- taktička-gospodarska ili crvena zona. U ovoj zoni zbog osjetljivosti informacija moguće je prodrijeti jedino kroz zatvorene izvore, ili korištenjem tajnih sredstava.

Brkić i Dizdarević, ističu da je jedan od mogućih i čini se najednostavnijih načina u okviru poslovne špijunaže vrbovanje informatora ili osoba unutar konkurentske korporacije. Kao drugi model javlja se mogućnost infiltracije vlastitih kadrova u konkurentsku firmu, ili u nauci i struci poznati pod terminom "rezidentni operativci". Pored nelagalnog i netičkog, kao vrlo bitan faktor u špijunaži je i samo korištenje potajnih i tajnih sredstava, od različitih mikročipova do presretanja informacija. Međutim, u posljednjih dvadeset godina kako u nauci tako i u struci vodi se znanstvana diskusija da li se špijunaža ima i treba smatrati nelagalnom i neetičnom djelatnosti. Zagovornici da se ista ne treba smatrati nelagalnom ističu dva ključna elementa:

- presretanje informacija, vrbovanje i korištenje informatora pod određenim uvjetima može se u skladu sa zakonom provoditi protiv određenih osoba u odnosu na koje postoje osnovi sumnje da su izvršili krivično djelo,
- špijunaža prema ovoj grupi autora, veoma često koristi se kao posljednje sredstvo u krajnjem negativnom ishodu poslovno obavještajne djelatnosti.

Ako se promatraju ovakva stajališta evidentno je isticanje maksime, pod kojom se djelatnosti poput špijunaže provode, "da cilj opravdava sredstvo". Zakonom se mogu provoditi tajne mjere i radnje samo u odnosu na osobe za koje postoje osnovana sumnja da su počinile krivično djelo, a nikako u odnosu na osobe/peronifikatore korporacije s ciljem dolaska do njihovih tajni. S druge strane, obavještajna djelatnost kao zakonska predispozicija sigrunosti dozvoljena je utemeljena kroz ustav i zakone, dok je djelatnost špijunaže zabranjena međunarodnim konvencijama i inkriminisana kao krivično djelo nacionalnim zakonodavstvima.

ZAKLJUČNA RAZMATRANJA

Osnovni distinkcioni elementi između poslovno obavještajne djelatnosti i špijunaže mogu se podjeliti u nekoliko ključnih grupa sa nizom podklasifikacija. Prvu grupu čine pravni elementi prema kojima je obavještajna, pa time i poslovno obavještajna djelatnost uređena ustavom, zakonskim i podzakonskim aktima, dok je špijunaža kao sredstvo zabranjena međunarodnim konvencijama te kao takva inkriminisana

[56] Potter, E. (1998). Exonomic intelligence & National Security, Carlton University Press & The Center for trade Policy and Law, Canada.

krivičnim zakonima. Drugu grupu čini sam karakter informacije za kojom se traga. Veći broj poslovnih informacije korporacija dostupan je široj javnosti, te kao takve iste se mogu koristiti. Upravo način prikupljanja, objedinjavanja, analize i korištenja predstavlja skup alata i znanja koje se nazivaju poslovno obavještajna djelatnost, jer kao takva koristit će se za donošenje budućih poslovnih odluka. Svaka korporacija nastoji osjetljive informacije klasificirati kao poslovnu tajnu, i u tom kontekstu dolazak do iste moguće je korištenjem isključivo polutajnih i tajnih metoda i sredstava, odnosno špijunažom. Treću grupu distinkcionih elemenata čine stučno znanstveni. Sredstva i alati koji se koriste u okviru poslovno obavještajne djelatnosti preuzeta su primarno iz različitih nauka, sintetizovana kao takva u kontekstu opsluživanja top menadžmenta s ciljem donošenja pravilnih odluka. Sredstva i alati u okviru špijunaže predstavljaju tajna, sofisticirana i modifikovana elektronička oruđa, pomoću kojih se primjenom tajnih metoda i tajnih nezakonitih sredstava prodire u tuđi poslovni ambijent, s ciljem krađe podataka i informacija. Novitet u odnosu na poslovno obavještajnu djelatnost proizašao je iz razvoja kapitalizma, i prodiranja velikih korporacija na međunarodno tržište. Obavještajna djelatnost bila je primarno u nadležnosti država s ciljem zaštite nacionalne sigurnosti, i kao takva opstala je do danas. Poslovno obavještajna djelatnost predstavlja svojevrsnu komercijalizaciju, odnosno privatizaciju djelatnosti za potrebe korporacije. Distinkciju između poslovne obavještajne djelatnosti i špijunaže najslikovitije opisao je Pajević u svojoj studiji ukazujući da "cilj obavještajne djelatnosti je da svojim sredstvima i metodama dođe do najvažnijih podataka ili da rješava najbitnije problem za jednu zemlju, a ne samo da prikuplja podatke o drugoj zemlju".[57]

LITERATURA

1. Aleksić, L.Ž. (1979). *Kriminalistika.* Beograd.
2. Bazdan, Z. (2009). *Menadžeri moraju znati: poslovno obavještajna djelatnost kreira najvažniji resurs upravljanja,* Poslovna izvrsnost Zagreb, Zagreb.
3. Brkić, K., Dizdarević, S. (2017). *Metodi, trendovi i alati u korporativnoj sigurnosti, poslovna špijunaža-mit ili stvarnost*, Međunarodna konferencija IUT, Zbornik radova.
4. Daničić, M., Stajić, Lj. (2008). *Privatna bezbjednost,* Banja Luka.
5. Đozić, T. (2012). *Gospodarska špijunaža*, paradigma modernog svijeta.
6. Krivični zakon Federacije Bosne i Hercegovine, član 2. stav. 24. („Službene novine F BiH, broj: 09/03").
7. Pajević, M. (2013). *Savremene obavještajne teorije*, Mostar.
8. Pajević, M. (2017). *Obavještajne studije,* Kiseljak.
9. Potter, E. (1998). Exonomic *intelligence & National Security, Carlton University Press & The Center for trade Policy and Law,* Canada.
10. Rudan, V. (2008). *Konkurencija na nišanu-Teorijski i praktični aspekti istraživanja konkurencije*, Hesperiaedu, Beograd.
11. Trivan, D. (2012). *Korporativna bezbjednost,* Beograd.
12. Vidović, D. Karlović, L. Ostojić A. (2011). *Korporativna sigurnost*, Zagreb.
13. Zakon o krivičnom postupku Federacije BiH, član 21. tačka n) („Službene novine F BiH, broj: 35/03, 37/03, 56/03").
14. Zebić, O. (2010). *Poslovno obavještavanje i oblikovanje poslovnih strategija hrvatskih preduzeća*, Specijalistički poslijediplomski rad, Sveučilište u Zagrebu.

[57] Pajević, M. (2013). Savremene obavještajne teorije, Mostar, str. 136.

проф. д-р Томо Борисов
заместник ректор на ВУСИ
Пловдив, Бугарија

проф. д-р Ненко Дойков
директор на Лаборатория за
специализирани изследвания
на рисковете и сигурността-НБУ

ОСНОВИ НА ПОДГОТОВКАТА НА КОРПОРАЦИИТЕ ЗА ОТГОВОР НА ТЕРОРИСТИЧНО НАПАДЕНИЕ

SUMMARY

This report defends the view that, in modern conditions, in order to prevent the emergence of a crisis situation and to respond adequately to terrorist attacks, corporations need to structure a highly efficient system to be used by the various organizations involved in special operations to deal with accidents caused by terrorist activity. For this purpose, we will analyze the measures that need to be taken to prepare a corporation to respond to a terrorist attack.

Due to the limited format of a report, this study can not fully elaborate on the overall counter-terrorism policy, but our ambition is to outline the context and specificities of today's conditions.

Keywords: Threat Zone, Public Safety Staff, Emergency Response, Dangerous Materials, Eight-Step Process.

РЕЗЮМЕ

В този доклад се защитава тезата, че в съвременните условия, за да не се допусне разрастването на дадена кризисна ситуация и за да се реагира адекватно на терористични нападения, е необходимо корпорациите да структурират високоефективна система, която да бъде използвана от различните организации участващи в специални операции за справяне с инциденти, предизвикани от терористична дейност. За тази цел ще бъдат анализирани мерките, които трябва да бъдат взети, за да се подготви една корпорация, за да отговори на терористично нападение.
Основните въпроси на които ще търсим отговор са:

Ако терористичния акт е извършен срещу корпорацията, какво може и какво трябва да се направи в отговор?
Как една компания да се възстанови от такава трагедия?
Какво е въздействието върху бизнеса и служителите?

Поради ограничения формат на един доклад, в настоящото изследване не може в детайли да се разработи цялостната антитеористична политика, но нашата амбиция е да очертаем рамките и спецификата при съвременните условия.

Ключови думи: зона на застрашеност, персонал за обществена безопасност, спешни реагирания на инциденти, опасни материали, осем-стъпков процес.

УВОД

Светът, в който живеем, от една страна, предлага по-добри перспективи за бъдещето, но от друга - изправени сме пред редица непознати по своя мащаб и характер предизвикателства и заплахи.
Събитията в началото на XXI век показаха, че в голямата си част, международните отношения са зависими от глобалния тероризъм, състоящ се от множество клетки разположени в различни държави.
Терористите се организират бързо. Те нямат скрупули и бюрократични пречки, разполагат с достатъчно средства и могат да привлекат за престъпните си цели водещи специалисти от различни области.
Терористите от новото поколение проявяват все по-активно стремеж за замяна на експлозивите с компютри, конвенционалните оръжия с биологични и химически.
За недопускането на горепосочените слабости ние в редица наши изследвания многократно сме защитавали тезата, че по-доброто ниво на осведомеността и обучението на гражданите може да помогне на службите по прилагането на закона.
Внимателното изучаване на програмите за борба с тероризма в Русия, САЩ, Франция, Израел, Англия, Испания, Швеция, Турция, Полша и Холандия могат да ни подскажат серия от мерки, които могат да помогнат в сегашното кризисно време.
Изключително важно условие за ефективно противодействие на терористичната дейност е да бъде разработена система от политики и практики за своевременно реагиране с цел недопускане (*предотвратяване*) на терористичен акт.
В днешния свят, след трагичните събития от 11 септември 2001г. и последвалата глобална война с тероризма, необходимостта за бизнес планиране при извънредни ситуации в случай на терористични атаки, трябва да бъде основен приоритет на всички държавни и частни структури.
Необходимостта се подсилва и от наличието на множество опасности предизвикани от природни бедствия, нови пандемии и техногенни аварии.
Събитията от последните години ни дават основание да заявим, че редица опасности имат потенциал за нарушаване на непрекъснатостта на работа на бизнеса в засегнатите географски региони или пазарен сектор.

Ето защо всички организации трябва да имат аварийни планове за действия при извънредна ситуация. Тези планове трябва да бъдат разработени по такъв начин, че да се позволи незабавен отговор на извънредна ситуация и ефективно управление при криза.

1. ОСНОВИ НА СИСТЕМАТА ЗА УПРАВЛЕНИЕ ПРИ ИЗВЪНРЕДНИ СИТУАЦИИ

Много може да се научи от миналото. Чрез анализиране на отминалите събития, служителите от правоохранителните и правораздавателните

структури могат да научат за това какво се е случило и как тези "изводи" може да се приложат за бъдещи действия.
Нагласата на терористите и престъпниците, които често използват различни тактики е едно сложно и интересно проучване, но знанието как тези лица и групи действат е важна стъпка в процеса на улавяне и в крайна сметка на неутрализиране на тяхната дейност.
Като се имат предвид сегашните тенденции в тероризма, подготовката за реализирането на конкретен терористичен акт, изглежда и е трудна задача, тъй като сценариите са много разнообразни и различни.
Това наистина може да изглежда трудна задача, но има доста неща, които държавните агенции за безопасност могат да направят, за да идентифицират потенциални цели и да се подготвят за събитието.
В световната история има редица събития, разделени от десетки години, които са имали и ще продължават да имат значително влияние върху начина ни на мислене, начина ни на живот и провеждането на операции на "улично ниво" от занимаващите се с обществената сигурност.
В последните години, правоприлагащите органи и службите за спешно реагиране на страните от демократичната общност са изправени пред предизвикателства, които преди това са били извън сферата на вероятност. През 1998 г. Осама бен Ладен обяви придобиването на оръжия с технология за масово унищожение за "религиозен дълг"[58]. Въз основа на информацията, извлечена от американските военни операции в Афганистан стана известно, че терористични клетки на "Ал Кайда", действащи на свобода, като цяло все още търсят тази възможност.
Въпреки тези констатации ние считаме, че всеки, който се надява терористите да не използват тези оръжия, ако ги придобият е в голямо заблуждение, защото **НАДЕЖДАТА НЕ Е СТРАТЕГИЯ!**
Много често инцидентите, които налагат провеждането на специални операции, включват различни опасни престъпления и тежки аварии, терористичните заплахи, нелегалните лаборатории за опасни вещества, инциденти с взривни вещества и други престъпления, свързани с използване на опасни материали.
Дали са определени като опасни материали, оръжия за масово унищожение, незаконни вещества, или са използвани други подобни термини и акроними, това са материали, които представляват сериозна краткосрочна или дългосрочна опасност за всички, които са в зоната на застрашеност.
В много отношения реагирането на тези инциденти, потенциално съчетават предизвикателствата на прилагането на закона при криминално събитие, предизвикателствата на инциденти с опасни материали, и предизвикателствата на оказване на спешна медицинска помощ при масово произшествие.
Това е изключително трудна задача, защото действащите на терен екипи обикновено включват професионалисти по прилагането на закона, пожарната

[58] На 02.05. 2011г. президентът на САЩ Барак Обама обяви, че терорист номер едно Осама бин Ладен е бил убит при ръководена от американски специални сили операция.

и спешните медицински екипи, както и членове на организации, отговарящи за инцидентите с опасни материали и специалните екипи за действия [59] .
Много често тези професионалисти в специализираната литература се включват обобщено в общността на персонала на службите за запазване на обществената безопасност. Ние също в това изследване ще използваме термина **персонал за обществена безопасност** за да очертаем един широк кръг от специалисти, които се занимават с прилагане на закона, пожарната и спасителната служби, спешните медицински услуги и справянето с извънредни ситуации.
Сигурността и здравето на служителите от службите за обществена безопасност, работещи на място на инцидент, който може да съдържа опасни материали, е от първостепенна важност. Независимо от своя размер или естество, всеки инцидент поставя реагиращите в потенциално враждебна (опасна) среда.
Докато предотвратяването на излагането на опасни материали е винаги първостепенна грижа, персонала трябва също да оцени заплахата от противника, стреса от работата в лични защитни облекла и оборудване, физическите условия на труд, както и подходящите процедури за обеззаразяване на базата на обхвата и мащаба на инцидента.
Инцидентите с опасни материали се характеризират с рискова работната среда, които могат да представляват непосредствена опасност за живота и здравето на персонала за обществена безопасност.
Когато изследването е предназначено за такава разнообразна аудитория, използването на специфичната професионална терминология се затруднява не само поради нейното многообразие, но и поради различното и специфичното й прилагане.
В специализираната литература и практическите наръчници се използват широка гама от термини, определения и съкращения за описване на химични, биологични, радиологични и взривни материали, които могат да бъдат използвани в престъпно или терористично събитие.
Задачата, която сме си поставили в това изследване не е да напишем учебник по управленска терминология и дефиниции, а и реалността е такава, че всеки един термин, който ние ще използваме сега, вероятно ще се промени във времето. Нашата цел е да представим един алгоритъм за адекватни действия и реагиране на инциденти с опасни материали.
Светът през последните десетилетия се е променил и общността на органите за обществена безопасност трябва също да се променят с него.
Ако искаме нашите реагиращи и спасяващи операции да се извършват безопасно и ефективно в бъдеще, ние трябва да преосмислим начина, по който ръководим нашия бизнес и живот. Сигурността трябва да бъде включена в културата на обществената безопасност и трябва да се превърне в рутинна за това как да работим, а не изключение.

[59] Тактически звена за бързи действия, екипи за локализиране, транспортиране и обезвреждане на взривни вещества, и на различни други държавни и местни органи, имащи правомощия в специфични области, като Агенцията за ядрено регулиране, Министерството на околната среда и водите, кметовете на общини, областни управители и други.

През следващите години, ние трябва да очакваме, че престъпници и терористи ще планират операции срещу нас, като използват най-новите разузнавателни методи и технологии. Жестокостите, извършени в Съединените щати на 11-ти септември 2001 година насочват вниманието ни към вътрешния и международния тероризъм, но истината е, че има десетки насилствени престъпни деяния, които се случват и в нашата страна всяка година, които включват използването на подобни терористични тактики и оръжия.

Примерите включват употребата на високи технологии, температурни катализатори, концентрирани киселини и основи, както и на самоделни взривни устройства при извършване на жестоки престъпления и убийства.

Освен това при неотдавнашните инциденти, в редица държави сме свидетели на използването на капани и вторични взривни устройства от престъпници и терористи с цел да се преодолеят точно службите за спешна помощ.

Реагирането на тези видове инциденти ясно поставя аварийните отговорници в изключителна опасност, а специалните мерки за сигурност са задължителни и оправдани на местопрестъплението.

Нуждата да променим начина, по който извършваме работата си при опасни ситуации, не се ограничава обаче само до отговора за спешно реагиране, а включва също и необходимостта да се защити определена критична информация за някои наши планове, процедури, обучение и оборудване, които ние използваме в провеждането на специалните операции.

Спешните реагирания на инциденти, включващи опасни материали използвани от престъпници и терористи, са екстремно опасни и при овладяването на инцидентите трябва да се вземат всички необходими предпазни мерки. Винаги имайте предвид най-лошия сценарии и поставяйте личната безопасност на първо място.

Въпреки, че реагирането на инциденти с огнестрелни оръжия, взривни вещества и други опасни материали, са довели до наранявания и смърт на много пожарникари, полицейски служители и медицински персонал, реагирането на тези инциденти представлява осъзнат, а в повечето случаи и дългосрочен здравословен риск за реагиращите.

В последните години се появиха много нови решения и технологии, но поради ограничения формат на един научен доклад, считаме, че не е възможно в това изследване да се обхване целия спектър на проблемите и препоръките за разрешаването на всеки тип спешен случай или криминално престъпление, който може да възникне.

Операциите за реагиране на място трябва винаги да се основават на структурирана и стандартизирана система от протоколи и процедури.

Независимо от естеството на инцидента, както и от ответната реакция, уповаването на стандартизирани процедури ще доведе до последователност на тактическата операция, независимо от включения персонал.

Ако дадена ситуация потенциално включва опасни материали или средства за масово унищожение, упованието на стандартизирани тактически процедури за реакция, ще помогне да се сведе до минимум рискът от излагане на опасност за всички реагиращи.

В редица наши изследвания сме анализирали голяма част от проблемите съпътстващи противодействието на тероризма и сме стигнали до

обобщаващия извод, че терористичната заплаха е много аморфна и неопределена, което я прави много трудна за предотвратяване, а планирането срещу нея сложно, което понякога води до неадекватни реакции[60].
Всичко това налага при ответните действия да се използват изпитани и нетолкова познати похвати и техники.
В този анализ ще представим една система за управление на екипите за намеса при извънредни ситуации, които могат да бъдат предизвикани от използването на материали, класифицирани като "опасни".
Тази система е известна като осем-стъпков процес.
Анализираният от нас в това изследване, осем-стъпков процес е възприет и се използва широко в много страни от обществения и частния сектор от екипите, реагиращи при управление на извънредни ситуации с опасни материали.
Той също така служи като пример за структурирана система, която може да се използва от правоприлагащите органи и персонала за специални операции при инциденти, свързани с опасни вещества и материали.

2. ОСЕМ - СТЪПКОВ ПРОЦЕС

Много експерти ще твърдят, че реагирането на служителите от обществената безопасност при терористични събития е нещо ново. Въпреки, че природата на "лошите момчета", може да се е променила, реалността е, че специалистите по обществената безопасност работят в отговор на терористичните събития в продължение на много години. Това е важно, тъй като спешния отговор на тероризма и криминалните събития, които могат да включват опасни материали или оръжия за масово унищожение не е нова мярка, а просто продължение на това, което много от специалистите по обществената безопасност вече са правили в работата си при спешното реагиране.
Придобитият опит както от проведените учения, така и от анализа на реалните събития показва, че критичните фактори за успех в първия час на реагиране типично ще бъдат:

- Способност да разпознавате уликите, че инцидентът може да включва комбинация от терористична престъпна дейност и опасни материали или оръжия за масово унищожение;
- Възможност да получите контрол на мястото на инцидента по подходящ начин и да отделите реагиращите от проблема;
- Възможност за създаване на единна командна структура между основните „играчи”.

Способността първоначално да се преценят и оценят уликите ще зависи от количеството и качеството на информацията, която се предоставя на персонала за обществена безопасност чрез различни съобщения.

---

[60] Дойков, Н. Основни препоръки и правила за поведение при терористични заплахи С. 2009г., Дойков, Н. Основи на тактическите действия в населени места-С. 2011 , Дойков, Н. Противодействие на тероризма - С.2011 , Дойков, Н. Планиране и вземане на решение за управление на кризисни ситуации при терористичен акт. С.2007г.

Какво своевременно трябва да знаят реагиращите?

Освен основните **кой, какво, и къде**, има и някои други фактори, които могат да бъдат улики и те включват:

- Дали инцидента е в основната цел, която е запланирана?
- Има ли запис на предишни заплахи на това място?
- Има ли множество пострадали? Известни или неизвестни са причините?
- Има ли доклади за необичайни миризми? Експлозии? Опасни материали?
- Има ли първореагиращи на място?
- Има ли някакви вторично възникнали събития?

Можем да приемем, че осем-стъпковия процес очертава основните тактически функции, които да бъдат оценени и приложени при инциденти, свързани с опасни материали.

Както всички операции за сигурност, осем-стъпковия процес трябва да се разглежда като гъвкава насока, а не като твърдо правило.

Отделните служби и агенции трябва да решат кое е най-доброто за тях.

Осем-стъпковия процес предлага няколко предимства.

Първо, той се основава на осъзнатото разбиране, че мнозинството от инцидентите, свързани с опасни материали са незначителни по своя характер и обикновено включват ограничени количества от опасните вещества.

Второ, той също така се основава на действието на първореагиращите единици и определя ролята и отговорностите на всяко ниво на реагиране.

Осем-стъпковия процес предоставя гъвкава система за управление, която се разширява докато обхвата и мащаба на инцидента растат, и накрая, той осигурява последователна управленска структура, независимо от класа на включените опасни материали.

По същество, има осем основни функции, които трябва да бъдат оценени в извънредни ситуации, потенциално включващи опасни материали и оръжия за масово унищожение.

Тези осем функции обикновено следват времевата линия на изпълнение на инцидента.

Функциите са:

1. Управление на мястото и контрол върху инцидента;

Управлението на мястото и контрола върху инцидента е и управление, и осигуряване на физическото разположение на инцидента. Реалността е, че не можете безопасно и ефективно да се справите с инцидента, ако нямате контрол на сцената.

2. Определяне на проблема;

Основната цел на стъпка 2 е да се определи обхвата и същността на проблема, включително вида и характера на опасните материали. Определянето на надеждността и сериозността на проблема трябва да се извършва незабавно, включително признаване, идентификация и проверка на материалите, които участват и на потенциални или съществуващи опасности за живота.

3. Оценка на опасностите и риска;

Основната цел на тази стъпка е да се оценят присъстващите опасности, да се оцени степента на риска, както и да се създаде инцидентен план за действие, за да се разреши проблема. Въз основа на процеса на оценка на риска, определете дали на инцидента трябва да се отговори нападателно, отбранително, или чрез ненамеса.

4. Избор на лични защитни облекла и екипировка;

Целта е да се гарантира, че целият персонал за спешно реагиране е с подходящо облекло и лични предпазни средства за очакваните задачи. Изборът на лични защитни облекла ще зависи от опасностите и свойствата на съответните материали, както и от целите, които трябва да бъдат изпълнени (нападателни, отбранителни, не намесващи се).

5. Управление на информацията и координация на ресурсите;

Тази стъпка касае правилното управление, координация и разпространение на съответните данни и информация в рамките на местопрестъплението. Тази функция не може ефективно да се извършва, освен ако няма единна организация на място.

6. Прилагане на отговорни цели;

Това е фазата, когато реагиращите прилагат най-добрите налични стратегически и тактическите цели, които ще дадат най-благоприятен изход.
Ако инцидентът е в спешна фаза, това е мястото, където ние трябва да направим така, че проблема да изчезне.
Ако инцидентът е във фаза след спешно реагиране, във фокуса на персонала за обществената безопасност най-вероятно ще бъде: запазване на местопрестъплението, разследване и управление.

7. Осигуряващи и почистващи операции;

Целта е да се осигури безопасност едновременно както на службите за спешна помощ, така и на обществеността, чрез намаляване нивото на замърсяване на мястото на инцидента и свеждане до минимум на възможностите за повторно замърсяване след инцидента.

8. Прекратяване на инцидента;

Тази стъпка включва: прекратяване на дейността за спешно реагиране и започване на след аварийните операции за спешно реагиране, включително разследване, реставрация и възстановителни дейности.
Анализа на осем-стъпковия процес, показва, че спешните действия при инциденти, свързани с операциите с опасни материали винаги трябва да се основават на структурирана и стандартизирана система на протоколи и процедури.
Независимо от естеството на инцидента, както и отговора, разчитането на стандартизирани процедури ще доведе до последователност на тактическата операция, независимо от персонала.

Ако ситуацията предполага потенциално опасни материали или средства за масово унищожение, това разчитане на стандартизирани тактически процедури ще помогне да се сведе до минимум риска от излагане на всички реагиращи.
Осем-стъпковия процес е инструмент, използван за тактическо реагиране на опасни материали в извънредни ситуации. Той служи за пример на структурирана система, която може да бъде използвана от правоприлагащите органи при специални операции на персонала за справяне с инциденти с опасни вещества и материали.
Въпреки, че нивото на оборудване, обучение, както и вида персонал, може да варира между отделните организации, там са основните функции и задачи, които трябва да бъдат оценени за последователното изпълнение на основното.
Осем-стъпковия процес осигурява рамката, необходима за да се приведат планирането и готовността в предоставянето на една ефективна система за реагиране и разследване на инциденти, когато са включени опасни материали и оръжия за масово унищожение.

Използвана литература:

1. Дойков, Н. Планиране и вземане на решение за управление на кризисни ситуации при терористичен акт. С.2014г.
2. Доклад на Европол за състоянието и тенденциите на тероризма в ЕС за 2011 г. (TE-SAT 2011)

Prof. dr. Dževad Mahmutović
International University of Sarajevo, Faculty of Law
dzmahmutovic@ius.edu.ba
Prnjavorac Muris
Agency for Protection of People and Property GARDA Ltd Tešanj
e-mail gardadoo@bih.net.ba

UPOTREBA VIDEONADZORA U ISPUNJAVANJU SIGURNOSNIH CILJEVA ILI NARUŠAVANJE PRIVATNOSTI GRAĐANA

USE OF VIDEO SURVEILLANCE IN COMPLIANCE WITH SAFETY OBJECTIVES OR DISRUPTION OF CITIZEN'S PRIVACY

SAŽETAK

Ovim radom se nastoji po ko zna koji put podsjetiti na ubrzani razvoj tehnologija i njihovu široku prisutnost u svakodnevnom ljudskom životu, kao i prednosti koje ta tehnologija donosi. Jedan od tehnoloških noviteta, pored korištenja širokog spektra informacionih tehnologija, koji se posljednje decenije veoma ubrzano razvija i doživljava masovnu upotrebu jesu i sistemi video nadzora. Ovaj rad još jednom potvrđuje da je sistem video nadzora postao važan i masovno korišten resurs prevencije i izgradnje opće sigurnosti ali i da je upitno da li se u svakodnevnici vodi računa o zakonitosti, opravdanosti korištenja, kao i zaštiti privatnosti pojedinca. Nakon detaljne analize autori konstatiraju da je upotreba video nadzora poželjna, uz strogu kontrolu i unaprijeđenje normativnog uređenja ove oblasti.

Ključne riječi: videonadzor, privatnost, ljudska prava, lični podaci, zaštita ličnih podataka.

SUMMARY

This work, for the umpteenth time, aims to admonish of the accelerated development of technologies and their wide presence in everyday human life, as well as the advantages that this technology brings. One of the technological innovations, besides using a wide range of information technologies, which has been developing rapidly and experiencing massive use in the last decade, are also video surveillance systems. This work, once again, confirms that the video surveillance system has become an important and massive resource of prevention and building of general security, but also that it is questionable whether in the everyday life the legality, the justification of use, and the protection of the privacy of the individuals are taken into account. After a detailed analysis, the authors conclude that the use of video surveillance is desirable, with strict control and improvement of the normative regulation of this area.

Keywords: video surveillance, privacy, human rights, personal data, personal data protection.

1. UVOD

Ovim radom se nastoji ukazati na ubrzani razvoj tehnologija i njihovu široku prisutnost u svakodnevnom ljudskom životu, kao i prednosti koje ta tehnologija donosi. Jedan od tehnoloških noviteta, pored korištenja širokog spektra informacionih tehnologija, koji se posljednje decenije veoma ubrzano razvija i doživljava masovnu upotrebu jesu i sistemi videonadzora. U ovom radu će se objasniti pojam videonadzora uopšte kao i ukazati na prednosti koje donosi njegova svakodnevna upotreba, ali i otvoriti neka pitanja koja prate upotrebu videonadzora i analiza snimaka pribavljenih putem videonadzora. U prvom redu se ta pitanja odnose na rješavanje sve prisutnije dileme i pružanja odgovora na pitanje: "Gdje je granica između prava na privatnost i potrebe za sigurnošću". Također, pokušaće se razjasniti obaveza i zakonitost korištenja videonadzora uopšte, posebno sa aspekta zaštite ličnih podataka ,a u skladu sa aktuelnim zakonskim rješenjima. Predmet i problem ovog rada je prednost upotrebe videonadzora od strane različitih korisnika ali i obaveze koje proizilaze iz upotrebe videonadzora koji je mehanizam za prikupljanje i obradu ličnih podataka.
Cilj rada je ukazati na značaj sistema videonadzora i nesumnjive prednosti koje ova tehnologija donosi, ali i obaveze zaštite privatnosti i zakonitog korištenja i obrade podataka pribavljenih putem videonadzora te osiguranja uslova da ne dođe do zloupotrebe istih.
Hipoteza koja se postavlja pred ovaj rad je da je sistem videonadzora postao važan i masovno korišten resurs prevencije i izgradnje opće sigurnosti , i da je upitno da li se u svakodnevnici vodi računa o zakonitosti, opravdanosti korištenja, kao i zaštiti privatnosti pojedinca.

2. POJAM VIDEONADZORA

Svakodnevno u životu se susrećemo sa pojmom videonadzora koji polako postaje normalan i sastavni dio naših života i doživljavamo ga nezaobilaznim i podrazumijevajućim. U dnevnoj štampi i izvještajima medija smo u prilici primiti informacije o novim „važnim projektima" uvođenja videonadzora javnih površina, ili uvođenja video nadzora u obrazovnim institucijama koji će pomoći u rješavanju sigurnosti u i oko škola. Elektronski mediji, također , vrlo često kroz emisije različitih sadržaja ukazuju na široku upotrebu videonadzora, tako da nam je svakodnevni život nalik na popularne serijale (reality) tipa „big brother". Za stručnu javnost, a i kroz vlastita praktična iskustva i izvještaje stručnih časopisa je već odavno poznato da na godišnjem nivou iz godine u godinu se bilježi rast prodaje sistema videonadzora i očekuje se nastavak tog trenda. Imajući u vidu rezultate istraživanja Centra za sigurnosne studije Sarajevo, u kojem je urađena analiza „Trenda privatne sigurnosti u BiH", i objavljena u martu 2017 g., uočavamo veliki broj privrednih subjekata koji su po osnovu važećih zakonskih propisa ovlašteni za obavljanje poslova tehničke zaštite u koje se ubrajaju i poslovi ugradnje videonadzora. Po tom istraživanju 2016. godine, na prostoru Federacije Bosne i Hercegovine (F BiH) je registrovano 125 pravnih subjekata koji se bave poslovima privatne zaštite, u entitetu RS je registrovano 44 takva subjekta dok je na prostoru Distrikta Brčko registrovano 10 subjekata sa odobrenjem za obavljanje poslova zaštite u koje, kako smo već naveli spadaju i poslovi ugradnje sistema videonadzora. Ovom broju

svakako treba dodati i odgovarajući broj pravnih lica koja se bave projektiranjem i ugradnjom videonadzora za potrebe Ministarstva unutrašnjih poslova (MUP) F BiH koja nisu u obavezi posjedovati posebno odobrenje, a naročito se uočava i jaka aktivnost velikog broja privatnih subjekata iz oblasti distribucije informatičke opreme i elektroinstalacijskih radova koja postavljaju sisteme videonadzora bez potrebnih odobrenja. Iz svega navedenog jasno je da na prostoru BiH je veoma razgranata aktivnost instaliranja videonadzornih sistema koji vjerovatno građane BiH nadziru na svakom koraku, pri čemu je upitna zakonitost ugradnje i opravdanost samog korištenja nadzora sa aspekta postojećeg normativnog uređenja Prije nego se upustimo u ukazivanje praktičnih koristi upotrebe videonadzora i obrade zapisa sa istih, potrebno je objasniti šta u stvari znači taj pojam.

Sa stručno – tehničkog aspekta, videonadzor ili CCTV – C*losed Circuit Television, tj televizija zatvorenog kruga,* što je doslovno prevedeno značenje sa engleskog jezika, je zatvoreni sistem koji funkcionira na sistemu zatvorene petlje u kojoj pristup do informacija, a to su u ovom slučaju videosignali sa raznih kamera, ima samo određeni krug ljudi preko određenih video monitora. Kako vidimo, osnovna razlika između videonadzora kao televizije zatvorenog kruga i "normalne televizije" je što kod videonadzora signal nije emitovan istovremeno svim korisnicima koji su u području prijema signala. (Delišimunović-Kričanić, 2001: str. 89).

Upravo ta karakteristika videonadzora kao televizije zatvorenog kruga čiji je signal dostupan samo određenom broju ljudi, koji su u prilici da zadiru u privatnost onih koji se nadziru videonadzorom, nameće obavezu korisnicima sistema videonadzora da poštuju zagarantovana i univerzalna ljudska prava koja su ugrađena u temelje demokratskih društava, te da preduzmu potrebne mjere da zapisi videonadzora ne budu dostupni neovlaštenim licima čime se preventivno djeluje na sprječavanju zloupotreba podataka sa videonadzora.

Potrebno je naglasiti da postoji i zakonsko definisanje pojma videonadzora, pa ćemo za potrebe ovog rada navesti šta se smatra pod pojmom videonadzora u smislu normativnih akata koji definišu oblast privatne zaštite u FBiH.

Videonadzor - predstavlja sistem tehničke zaštite čija je osnovna funkcija registracija, otkrivanje i potraga kretanja unutar štićenog objekta, a u svrhu odvraćanja i otežavanja počinjenja krađe, provale, razbojništva i dr., kako bi se olakšali identifikacija i pronalazak počinitelja tih djela pomoću videozapisa; (Uredba o poslovima tehničke zaštite koji se odnose na korištenje alarmnih sistema, videonadzora ili drugih tehničkih sredstava i opreme, te poslove intervencije u slučaju aktiviranja alarmnog sistema - "Službene novine Federacije BiH", br. 78/08 i 67/13). Dakle, u F BiH po aktuelnim propisima, a upravo zbog karakterisitika videonadzora kao sistema kojim se zadire u temeljna ljudska prava, poslovi ugradnje sistema videonadzora su uglavnom povjereni pravnim subjektima koji su u obavezi ishodovati odobrenje MUP-a za obavljanje tehničke zaštite u što se između ostalog ubrajaju i poslovi ugradnje videonadzora.

2.1. Elementi sistema videonadzora

Svaki sistem videonadzora čine osnovni elementi: videokamera, prijenosnik video signala, monitor, uređaj za prijem i obradu signala, kao i odgovarajući broj dodatnih uređaja koji poboljšavaju efikasnost i perfomanse samog sistema.

Videokamera je prvi i osnovni element sistema videonadzora, te predstavlja ulazni dio sistema ili „oko“ sistema videonadzora.

Prijenosni medij (prijenosnik signala) predstavlja transportni put za video signal od kamere do uređaja za obradu video signala i do monitora za prikaz signala u obliku slike.

Monitor videonadzora je uređaj koji prima signal sa kamera ili uređaja za obradu signala i emituje ga posmatraču u obliku prepoznatljive slike.

Uređaj za obradu signala (DVR-rekorder) je prijemni uređaj signala sa kamera u kojem se signal obrađuje, pohranjuje najčešće na hard disk smješten u uređaju i dalje distribuira shodno tehničkim karakteristikama. U pogledu sigurnosti, obrade ali i obaveza zaštite podataka pribavljenih putem video nadzora, ovaj uređaj predstavlja najvitalniji dio sistema obzirom da na njemu ostaje zapis/snimak video nadzora u zavisnosti od kapaciteta memorije koji kasnije može biti predmetom analize. Efekat korištenja sistema videonadzora u najvećem postotku, pored kvalitete kamera, zavisi i od ovog uređaja. Posebna pažnja se treba pokloniti izboru mjesta za smještaj centralne jedinice videonadzora (kako ovaj uređaj još nazivaju), te u cilju preveniranja mogućih zloupotreba pohranjenih zapisa procedurama propisati uslove pristupa prostoru centralne jedinice i cjelokupnog sistema zaštite od neovlaštenog pristupa i korištenja uređajem za obradu signala videonadzora.

Dodatni/pomoćni uređaji su uređaji koji ubrzavaju i olakšavaju rad sistema videonadzora, proširuju mogućnosti i maksimalno prilagođavaju sistem zahtjevima korisnika.

3. UPOTREBA SISTEMA VIDEONADZORA

Već smo u uvodnom izlaganju naglasili da je korištenje videonadzorima postala masovna pojava. Prednosti koje pružaju sistemi videonadzora su višestruke te će se za potrebe rada navesti kao primjer korištenje videonadzora na javnom mjestu, a naročito će se obraditi korištenje videonadzora na radnom mjestu, obzirom na činjenicu da je to veoma rasprostranjen oblik korištenja video nadzora

3.1. Videonadzor na javnom mjestu

Pod javnim površinama podrazumijevaju se prostori u kojima slobodno borave građani bez naročitih ograničenja uz obavezu poštivanja opšte prihvaćenih pozitivnih normi ponašanja. Javne površine/mjesta se mogu razlikovati prema namjeni te to mogu biti javne saobraćajne površine, javne zelene površine (parkovi, šetališta, dječija igrališta, odmorišta i sl.), zatim, uređeni prostori za rekreaciju i bavljenje sportskim aktivnostima i drugi prostori na kojima se svakodnevno okuplja i

boravi veći broj ljudi (trgovine, trgovački centri i sl.). Na svim ovim mjestima bi građani trebali svoje aktivnosti obavljati neometano i uz osiguravanje potrebne sigurnosti njihovog boravka. Vrlo često su baš ovakva mjesta ona na kojima se na različite načine ispoljavaju sigurnosno negativna dešavanja te javna vlast mjerama kriminalne prevencije, između ostalog, se vrlo često odlučuje na korištenje videonadzora kao sredstva prevencije i osiguravanja potrebne sigurnosti lica koja borave na javnim mjestima. Prema rezultatima istraživanja primjene video nadzora na javnim mjestima u 7 evropskih zemalja (V. Britanija, Španija, Mađarska, Austrija, Njemačka, Norveška, Danska,) sudeći po kvalitetu i rasprostranjenosti primjene na prvom mjestu je V. Britanija, a na posljednjem Austrija. Najčešće lokacije koje se nadziru i gdje može doći do potrebe analize zapisa videonadzora su: željezničke stanice, podzemne željeznice, finansijske ustanove, objekti od posebnog značaja (ambasade), muzeji, bolnice kao i saobraćajnice, parking prostori, raskrsnice, trgovi i sl. Primjera radi u V. Britaniji 40 000 kamera pokriva 500 gradova. (Kovačević - Lepojević, Žunić-Pavlović, 2012: str. 331). Prema istraživačkoj kompaniji IHS globalno tržište sigurnosne opreme u nadzoru gradova u protekle tri godine je u velikom zamahu, a u 2017 godini je prešlo vrijednost od tri milijarde dolara i predviđa se i dalji rast u prosjeku od 14,6 % godišnje. Kao glavni razlozi se navode inicijative vlada da se organima reda omogući bolje regulisanje javne sigurnosti i smanjenje kriminala (časopis A&SADRIA, april 2018,br 133: str. 12). Videonadzor na javnom mjestu ima jak preventivni uticaj, analizom snimljenih zapisa videonadzora se omogućava rekonstrukcija štetnog događaja, olakšava identifikacija i donošenje zaključaka u kreiranju daljnjih politika sigurnosti. Uprkos nedvojbenoj koristi prilikom korištenja videonadzora se mora voditi računa o poštivanju i zaštiti prava građana u skladu sa univerzalno prihvaćenim načelima i standardima. Navešćemo veoma pozitivan primjer Slovenije, Makedonije i Crne Gore, koji bi BiH društvo trebalo slijediti, gdje zakoni predviđaju da se za uspostavljanje videonadzora u stambenim zgradama traži saglasnost vlasnika stanova pri čemu je potrebno objasniti svrsishodnost i opravdanost razloga uvođenja nadzora. Provedena istraživanja mišljenja građana npr. u R.Hrvatskoj ukazuju na to da građani uglavnom nemaju negativan stav prema videonadzoru i shvataju njegove prednosti koje donosi općoj sigurnosti, ali svakako zahtjevaju jaču kontrolu čuvanja i postupanja sa snimljenim podacima radi izbjegavanja eventualnih zloupotreba. Ovakvi stavovi građana ne čude ukoliko imamo na umu da je još T.Hobs u „Levijatanu“ iznosio stavove o spremnosti ljudi da se odreknu dijela prava a radi postizanja veće kolektivne sigurnosti. Značaj javno privatnog partnerskog odnosa građana u modernoj Evropi je prepoznatljiv već više decenija. Zajedničko rješavanje pitanja urbane sigurnosti je postalo uobičajeni model učešća građana u kreiranju sigurnijeg ambijenta svoje lokalne zajednice. Još od 1987. godine djeluje EFUS (Evropski forum za urbanu sigurnost), koji okuplja veliki broj evropskih gradova. Osnovni cilj EFUS-a je osnažiti politike prevencije kriminaliteta ali i promovirati ulogu lokalnih zajednica u donošenju nacionalnih i evropskih zakona i politika koji se tiču sigurnosti zajednica, a jedan od važnijih projekata ovog tijela jeste donošenje "Evropske povelje o demokratskom korištenju videonadzora", koji primjenjuje sve veći broj evropskih gradova koji uvode videonadzor javnih površina.

Što se tiče BiH značajan napredak bi se postigao kada bi se kvalitetnije pristupilo implementaciji projekta "Rad Policije u Zajednici" (RPZ), koji pored dijelova RPZ

policajac kao kvartovski policajac, zatim policajac u školi, predviđa i postojanje "Foruma sigurnosti lokalne zajednice" kao lokalnih tijela koji okupljaju građane koji definišu, zajedno sa MUP politike bitne za urbanu sigurnost i prevenciju. I u praksi korištenja videonadzora javnih površina lokalnih zajednica bi ovo tijelo imalo značajnu ulogu u prevazilaženju dilema oko videonadzora kao potrebe ili zloupotrebe a što je veoma dobro rješeno u gradu Zagrebu gdje su vijeća za prevenciju i građansku kontrolu zasigurno u mnogome doprinijela da su danas stavovi građana o videonadzoru veoma pozitivni i da nema mjesta zloupotrebama a što u prvim projektima videonadzora javnih površina baš i nije bio slučaj

3.2. Korištenje videonadzora na radnom mjestu

Analizom zapisa videonadzora poslovnih procesa poslodavac dobija korisne informacije o slabim i kritičnim tačkama i ponašanjima što mu omogućava da u budućnosti kreira kvalitetniju sigurnosnu politiku u cilju zaštite sigurnosti i zdravlja na radu ali i da zaštiti vlastite poslovne interese.

Izričito se, i u propisima koji regulišu oblast tehničke zaštite npr.u F BiH , već u samom startu instalaterima sistema videonadzora zabranjuje postavljanje video nadzora na način kojim se grubo narušava privatnost nadziranih lica .U Uredbi o poslovima tehničke zaštite koji se odnose na upotrebu alarmnih sistema, videonadzora i drugih tehničkih sredstava i opreme, te poslove intervencije u slučaju aktiviranja alarmnog sistema., (Sl.novine F BiH 72/15).u članu 2. između ostalog stoji *,“ Poslovi tehničke zaštite , a koji se odnose na alarmni sistem, videonadzor i druga tehnička sredstva utvrđena ovom uredbom, ne smiju biti ugrađeni niti se koristiti u svrhu ugrožavanja i povrede privatnosti i sigurnosti drugih lica, već isključivo radi zaštite objekta ili ličnosti koji se štite tim sredstvima. Ugrožavanje i povreda privatnosti i sigurnosti postoji kada ugrađeni alarmni sistem, videonadzor i druga tehnička sredstva obuhvataju zaštitu objekta ili ličnosti van perimetra zaštite“.* Imperativ zaštite minimuma privatnosti radnika u odnosu na zaštitne mjere mora biti ispoštovan.

U skladu sa Zakonom o zaštiti ličnih podataka poslodavac koji koristi sistem videonadzora poslovnih procesa, pojavljuje se u ulozi "kontrolora" te je dužan urediti sva pitanja koja se odnose na prikupljanje, korištenje, čuvanje i zaštitu osobnih podataka svojih radnika, pa tako i osobnih podataka prikupljenih video nadzornom kamerom. Namjera je da radnici budu informirani o obradi njihovih podataka, prvenstveno o tome u koju svrhu se obrađuju njihovi lični podaci. Također, radnici moraju biti informirani ko ima pravo na pristup podacima, kao i ko ima pravo na ispravak podataka koji se na njih odnose, zatim o primateljima ili kategorijama primatelja ličnih podataka, te da li se radi o dobrovoljnom ili obveznom davanju podataka, kao i o mogućim posljedicama uskraćivanja davanja podataka. Sve ove informacije i procedure detaljno će biti regulisane pravilnikom, kao podzakonskim aktom. Pored ovih procedura, pravilnikom je potrebno odrediti i osobe ovlaštene za pristup podacima, mjere zaštite podataka u tehničkom, organizacijskom i kadrovskom smislu kako bi se osigurala njihova povjerljivost i razdoblje njihova čuvanja. Napominjemo kako je kod uvođenja, odnosno postavljanja video nadzora potrebno uočljivo i nedvosmisleno označiti – slikom i

tekstom – da se poslovni prostor, odnosno ulaz/izlaz radnika i ostalih osoba, tj. posjetitelja poslovnog prostora snima video nadzornom kamerom.

Video nadzor jedno je od sredstava zaštite na radu. Unatoč tome, nameće se pitanje srsishodnosti video nadzora. S jedne strane, očigledna je korist od video nadzora kao sredstva zaštite na radu primjerice, u prevenciji nasilja, sprečavanju krađe i sličnih kriminalnih radnji. No, s druge strane, video nadzor može zadirati i u privatnost te može postati sredstvo kojim se provode nedopuštene radnje – npr., nad radnicima, koji zbog toga mogu trpjeti psihosocijalne posljedice.

5. UPOTREBA SISTEMA VIDEONADZORA U NORMI I PRAKSI

Upotrebom videonadzora se u većoj ili manjoj mjeri zadire u privatnost i temeljna prava i slobode pojedinaca. Razni međunarodni ali i domaći normativni akti regulišu obavezu zaštite ličnih podataka pojedinaca sa aspekta njegovog prava na lični život, dostojanstvo i privatnost. Svrha zaštite ličnih podataka ogleda se u zaštiti ljudskih prava i temeljnih sloboda u prikupljanju, obradi i korištenju ličnih podataka. Evropska konvencija za zaštitu ljudskih prava i osnovnih sloboda (EKLJP) je u čl. 8 regulisala Pravo na poštivanje privatnog i porodičnog života.

„..svatko ima pravo na poštivanje svog privatnog i porodičnog života, doma i dopisivanja“

„... Javna vlast se neće miješati u ostvarivanje tog prava, osim u skladu sa zakonom i ako je u demokratskom društvu nužno radi interesa državne sigurnosti, javnog reda i mira, ili gospodarske dobrobiti zemlje, te radi sprječavanja nereda ili zločina, radi zaštite zdravlja, morala, prava i sloboda i drugih „

Navedena odredba međunarodnog karaktera ukazuje na potrebu naročitog opreza pri obradi, upotrebi i distribuciji ličnih podataka pribavljenih putem videonadzora.

Kao što znamo zaštitom prava propisanih EKLJP bavi se Evropski sud za ljudska prava (ESLJP) koji je u svojoj dosadašnjoj praksi razmatrao niz predmeta koji su u vezi sa korištenjem podataka koji su dobijeni upotrebom videonadzora. U dosadašnjoj praksi ESLJP nije postavljao posebne standarde za kontinuirano videosnimanje javnih mjesta osim uobičajenog odnosa prema privatnosti u članu 8. EKLJP. Prema slučaju *Friedl pr. Austrije* snimanje javnog događaja ili protesta ne narušava prava osobe (*Friedl pr. Austrije*, br. 15225/89). Jedan od sudaca u tom predmetu je zaključio da je snimka na javnom mjestu poput neželjenoga socijalnog kontakta, ali da ne predstavlja narušavanje prava.
Nadalje ESLJP u predmetu *Peck* nije smatrao spornim engleske sisteme snimanja javnih mjesta već činjenicu da je neumjesna snimka osobe objavljena u medijima (*Peck pr. Ujedinjenog Kraljevstva*, br. 44647/98.).
Sporne su bile situacije kada se prikupljeni podaci sistemski obrađuju i pohranjuju ili se omogućuje uvid u privatnost neosumnjičenih građana. U predmetu *Von Hannover* ESLJP se više bavio objavljivanjem slika u medijima nego pravima ugroženima tokom snimanja (*Von Hannover pr. Njemačke*, br. 59320/00.), a isto je naglasio i u slučaju *Sciacca* prema kojem objavljivanje fotografija može predstavljati

zahvat prava privatnosti, ali ne i samo snimanje istih (*Sciacca pr. Italije*, br. 50774/99.).

U slučaju Marper ESLJP je tražio donošenje zakonskih normi o pohranjivanju i uporabi, ako se radi o sistemskom prikupljanju podataka neosumnjičenih osoba (*Marper pr. Ujedinjenog Kraljevstva*, br. 30562/04.)

Europska unija je donoseći Direktivu 95/46/EC uredila odnos prema zaštiti prikupljenih podataka i njihovoj sistemskoj obradi, pri čemu nije ulazila u načine prikupljanja istih.18
Slično je regulirano i u drugim dokumentima Komisije19 ili okvirnoj odluci Vijeća 20 koje se također ne bave načinom prikupljanja ili snimanja već sustavnim pohranjivanjem i obradom podataka koji spadaju u područje privatnosti. U nekim preporukama se obrađuje odnos prema objavljivanju snimki u medijima jer taj aspekt zadire u privatnost.21
U poredbenom pravu nije bilo posebnih poteškoća s uporabom snimki nastalih na javnim mjestima za dokazivanje u kaznenom postupku. Iako je videosnimanje na području Engleske najučestalije, u engleskome pravnom sustavu uopće ne postoji izričiti zakonski izvor koji regulira navedeno područje već se snimanje provodi oslanjanjem na opća pravna načela o nepostojanju zaštite privatnosti u takvim okolnostima. U američkom se pravu od 1967. godine smatra da osoba na javnom mjestu ne može imati imunitet uočavanja od strane drugih osoba, prema odluci Saveznog vrhovnog suda u predmetu Katz.22 U odluci Knotts je sud utvrdio da građani ne mogu imati razborito očekivanje privatnosti na događajima koji su dostupni javnosti s obzirom na to da službenici policije ionako mogu uočiti takve događaje.

Temeljni dokument vezan za lične podatke u BiH su Zakon o zaštiti ličnih podataka (Sl.glasnik BiH 49/06 i 76/11). Po ovom propisu lični podaci su bilo koja informacija koja se odnosi na fizičko lice na osnovu koje je identifikovano ili pomoću koje se može utvrditi identitet lica. Nesumnjivo je da obardom zapisa videonadzora je moguće u odgovarajućim okolnostima utvrditi identitet nekog lica, pa podaci sa videonadzora vrlo često imaju karakter ličnog podatka. Pomenuti normativni akt poznaje definira niz ključnih pojmova važnih za problematiku ovog rada. Tako pojam *nosioc ličnog podatka* podrazumijeva fizičko lice čiji se identitet može ustanoviti ili identificirati, neposredni ili posredno, naročito na osnovu JMB, te jednog ili više faktora karakterističnih za fizički, fiziološki, mentalni, ekonomski, kulturni ili socijalni identitet tog lica.

Nadalje, *Zbirka ličnih podataka* je bilo koji sistemski skup ličnih podataka koji su dostupni prema posebnim kriterijumima, bilo da su centralizovani, decentralizovani ili razvrstani na funkcionalnom i geografskom osnovu ili postavljeni u skladu sa posebnim kriterijimima koji se odnose na lice i koji omogučavaju nesmetan pristup ličnim podacima u dosijeu. Smatram da arhiva zapisa videonadzora na DVR centralnom uređaju ima obilježja zbirke ličnih podataka. U pojmovima definisanim zakonom o zaštiti ličnih podataka nevedeno je:

Kontrolor je svaki javni organ, fizičko ili pravno lice, agencija ili drugi organ koji samostalno ili zajedno sa drugim vodi, obrađuje i utvrđuje svrhu i način obrade ličnih podataka na osnovu zakona ili propisa.U svjetlu ovog pojmovnog određenja a u vezi sa upotrebom videonadzora, kontrolorom se može smatrati „vlasnik i naručilac „ za čije potrebe je ovlaštena agencija izvršila instaliranje videonadzora.

Obrađivač je fizičko ili pravno lice, agencija ili drugi organ koji obrađuje lične podatke u ime kontrolora. Dakle u situacijama kada instalaterima sistema od strane vlasnika sistema ili organa policije dođe zahtjev za skidanjem snimaka videonadzora, tada su instalateri i agencije u kojima su zaposleni vrlo vjerovatno u ulozi obrađivača ličnih podataka u smislu zakona.

Zakon o zaštiti ličnih podataka je direktno doveo u vezu videonadzor sa ličnim podacima u čl.21a, gdje stoji

(Obrada ličnih podataka putem video-nadzora)

(1) Snimci pohranjeni putem video-nadzora na određenom prostoru na osnovu kojih se može identifikovati nosilac podataka predstavljaju zbirku ličnih podataka.

(2) Kontrolor koji vrši video-nadzor dužan je da donese odluku koja će sadržavati pravila obrade s ciljem poštovanja prava na zaštitu privatnosti i ličnog života nosioca podataka, ako video-nadzor nije propisan zakonom.

(3) Kontrolor koji vrši video-nadzor dužan je da na vidnom mjestu istakne obavještenje o vršenju video-nadzora i kontakt putem kojeg se mogu dobiti pojedinosti o video-nadzoru.

Da bi se stekao uvid u praktično tumačenje ovih propisa, kao i obavezu korisnika videonadzora, prenosi se mišljenje Agencije za zaštitu ličnih podataka BiH od 23.10.2013. godine u kojem je Agenciji postavljeno pitanje da li postoji zakonska prepreka za uspostavljanje videonadzora u preduzeću zbog učestalih krađa i da li jedno preduzeće može imati videonadzor, koje uslove mora ispuniti, koje su potencijalne opasnosti od kontrolnih i inspekcijskih organa i moguće sankcije. U dostavljenom odgovoru Agencija se prije svega poziva na već pomenuti čl.21a Zakona. Dalje se u mišljenju navodi da kada videonadzor nije propisan zakonom, kontrolor mora odrediti svrhu njegove uspostave. Pri tome se mora uzeti u obzir da li je postavljanje video nadzora zaista neophodno i da li bi za postizanje predmetnog cilja bilo dovoljno neko drugo rješenje. Dalje se navodi, da je nesporna činjenica da kontrolori često imaju interes za uspostavu videonadzora, kao neophodne mjere tehničke zaštite imovine kontrolora, štoje opravdano.Tom prilikom se vrši prikupljanje podataka o zaposlenicima iz razloga što su videonadzorom pokriveni ulazi, izlazi, hodnici koji vode prema skladištima, prilazi npr. kotlovnici itd. U tom slučaju, po mišljenju Agencije kontrolor u skladu sa članom 21a Zakona mora donijeti odluku o uspostavi videonadzora i na vidnom mjestu postaviti obavještenje o vršenju videonadzora a prije njegove uspostave informisati radnike o njegovoj svrsi u skladu sa čl.22. Bitna odrednica koja se uočava u navedenom mišljenju Agencije iz 2013. godine jesta da Agencija navodi da prilikom donošenja adekvatne

odluke o pravilima obrade ličnih podataka putem videonadzora, potrebno je obuhvatiti i propisati sve pojedinosti obrade ličnih podataka te navesti svrhu uspostave video nadzora, vrstu ličnih podataka koji se obrađuju, davanje video zapisa trećoj strani, te rokovi čuvanja zapisa videonadzora i dr. Iako za potrebe ovog rada nije vršeno terensko istraživanje da bi se došlo do provjerenih podataka, iz ličnog praktičnog iskustva se može, sa velikim stepenom vjerovatnoće, ustvrditi da u ovom pogledu još uvijek vlada velika neinformisanost i neusklađenost sa aktuelnim propisima. U prilog tvrdnji govori podatak iz godišnjeg izvještaja Agencije za zaštitu ličnih podataka za 2013. godine da je Agencija u toku 2013 godine zaprimila 5 (pet) prigovora u vezi sa obradom ličnih podataka i svi su rješeni na način da je doneseno rješenje kojim se u cjelosti ili djelimično usvajaju prigovori nosilaca ličnih podataka. Interesantno je da je različita struktura kontrolora protiv kojih je podnesen prigovor te bez navođenja punog naziva navešće se samo priroda djelatnosti kojom se bave (Federalna ministarstva, osnovno školska ustanova, pekara, stambeni objekat, privredno društvo za distribuciju energenata).

Važan korak u podizanju svijesti o značaju odgovornog odnosa prema privatnosti građana i njihovim ličnim podacima predstavlja i presuda Suda BiH iz 2015. godine kojom se ukazuje na neadekvatno korištenje videonadzora i obradu zapisa videonadzora čak i od jednog od Ministarstava u Vladi F BiH, kojem je Agencija za zaštitu ličnih podataka BiH prije presude naložila mjere za otklanjanje uočenih nepravilnosti prijavljenih od nosioca ličnih podataka. Nameće se pitanje, da li bi u slučaju bolje informisanosti nosilaca ličnih podataka, a obzirom na nedovoljnu informisanost kontrolora, bilo više podnesenih prigovora koji bi bili rješeni u korist nosilaca podataka. Svakako, da ova problematika zahtijeva posebno istraživanje, a u svakom slučaju je potrebno uložiti dodatni napor u cilju ispravnijeg shvatanja koristi upotrebe videonadzora, ali i opasnosti zloupotrebe obrade zapisa i podataka video nadzora.

Prije samog zaključka bitno je podsjetiti i na stupanje na snagu nove odredbe EU o GDPR (General Data Protection Regulation) ili "Opšta Uredba o zaštiti ličnih podataka EU" koja stupa na snagu 25. 05. 2018. godine i obavezujuća je za sve članice EU ali i izvan nje. Ova Uredba predstavlja obavezujući skup pravila kojim se reguliše upravljanje i zaštita ličnih podataka na prostoru EU i očekuje se da njenom primjenom dođe do bolje zaštite i veće kontrole nad korištenjem i obradom ličnih podataka građana.Posljedice neusklađenosti sa odredbama navedene Uredbe za organizacije mogu biti velike i u pogledu novčanih kazni, a u zavisnosti od težine nepoštivanja iznositi čak do 4% prometa ili 20 milijuna eura ovisno koji je iznos viši. Zasigurno je da će nova GDPR Uredba imati i uticaj na primjenu videonadzora i korištenje i zaštitu podataka pribavljenih putem videonadzora.

ZAKLJUČAK

U savremenoj svakodnevnici videonadzor predstavlja „normalnu pojavu“ na koju građanin pojedinac više ne obraća posebnu pažnju. Istovremeno benefiti koji se ostvaruju korištenjem videonadzora su višestruki, pogotovo sa aspekta preventivnog djelovanja i odvraćanja, te olakšane rekonstrukcije i identifikacije okolnosti pod kojima dolazi do narušavanja sigurnosnog stanja. Rezultati obrade

zapisa video nadzora su veoma koristan resurs u redefinisanju sigurnosnih politika svakog onog ko se video nadzorom koristi. Međutim, nesporno je da se video nadzorom zadire u privatnost i slobode građana i pojedinca, što je univerzalna međunarodno definisana kategorija koja se štiti. Analizom odredbi Zakona o zaštiti ličnih podataka BiH se uočava tendencija države da kroz normativni okvir ispuni međunarodne obaveze i poštivanje temeljnih sloboda i prava pojedinca. Ipak, na osnovu podataka Agencije za zaštitu ličnih podataka, nameće se zaključak da u implementaciji i prilikom svakodnevnog korištenja videonadzora postoji malo znanja od strane korisnika, o uslovima pod kojima se video nadzor može koristiti na zakonit način. Korisnici/kontrolori su u praksi svjesni i praktično se uvjerili u prednosti korištenja video nadzora, istovremeno, u velikom broju slučajeva ne provodeći obavezu donošenja odluka kojima se ukazuje na srsishodnost uspostavljanja video nadzora i ostvarivanja obavezne komunikacije sa onima koji se nadziru. Time je otvoren prostor mnogim zloupotrebama u prvom redu privatnosti. S tim u vezi u budućnosti se očekuje ekspanzija i trend rasta tržišta i prodaje video nadzornih komponenti pa je nužno potrebno jačati i kontrolne kapacitete kako bi se postigao optimum demokratske i zakonite upotrebe i manipulacije podataka pribavljenih putem video nadzora.

LITERATURA:

- Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

- M. Kovačević – Lepojević, V. Žunić-Pavlović, Primena videonadzora u kontroli kriminala, Pregledni rad, Beograd: Fakultet za specijalnu edukaciju i rehabilitaciju;
- M.Kričanić-D.Delišimunović (2001), Zaštita i sigurnost finansijskih institucija, Zagreb: Tectus d.o.o.
- Agencija za zaštitu ličnih podataka (2013), Mišljenja, Srajevo: AZLP;
- Zakon o zaštiti ličnih podataka (Sl. glasnik BiH, 9/06i 76/11);
- Izvještaj o zaštiti ličnih podataka u BiH za 2011, Agencija za zaštitu ličnih podataka;
- Izvještaj za zaštitu ličnih podataka za 2013, Agencija za zaštitu ličnih podataka;
- Sud BiH, Presuda r: S13 U014576 14, od 06.10.2015.g.;
- Predmet ESLJP *Friedl pr. Austrije*, br. 15225/89.
- Predmet ESLJP *Peck pr. Ujedinjenog Kraljevstva*, br. 44647/98.
- Predmet ESLJP *Von Hannover pr. Njemačke*, br. 59320/00.
- Predmet ESLJP *Sciacca pr. Italije*, br. 50774/99.
- Predmet ESLJP *Marper pr. Ujedinjenog Kraljevstva*, br. 30562/04.

Помлад асс. м-р Мимоза Стаменковска
Европски Универзитет Република Македонија
е-маил: mimoza.stamenkovska@eurm.edu.mk
Проф. д-р Алекса Стаменковски

КРИМИНАЛИСТИЧКА ФОРЕНЗИКА

АПСТРАКТ

За различни криминални случаи се потребни различните видови криминалистички истражувања. На пример, за откривање подметнувања на пожар, убиства или киднапирања се користат различни техники. Во различните случаи, истражувачите на криминалните дела мора да бидат во состојба да дојдат и да анализираат докази, да ги лоцираат обвинетите и да ги откријат жртвите. Форензичките аспекти на истражувањата на криминалните дела создаваат можност да се дојде до развивање и одржување на ресурси за истражување како што се: истражувачки прирачници, податоци за исчезнати лица и да спроведуваат курсеви за обучување на истражувачите.
Форензиката значи користење на научни методи за решавање на криминалот. Форензичките истражувања претставуваат прибирање и анализирање на сите физички докази поврзани со криминалот со цел да се дојде до заклучоци во врска со обвинетиот. Истражувачите прават анализа на крв, течности, отисоци од прсти, остатоци, хард дискови, компјутери и други технологии за да утврдат како настанал криминалот.

Клучни зборови: истражувања, техники, докази, методи, жртви, технологии.

ABSTRACT

Different types of crime investigations are needed in different cases. For example, investigators use different techniques to solve arson, murder and kidnapping. In various cases, investigators must be able to find and analyze evidence, locate suspects and identify victims. Forensic aspects of investigations, making awards to fund the creation and maintenance of investigative resources such as investigation manuals, missing persons databases, and training courses.
Forensics are the scientific methods used to solve a crime. Forensic investigation is the gathering and analysis of all crime-related physical evidence in order to come to a conclusion about a suspect. Investigators will look at blood, fluid, or fingerprints, residue, hard drives, computers, or other technology to establish how a crime took place.

Key words: investigations, techniques, evidence, victims, technology.

1. Основни карактеристики на криминалистичките истражувања

Криминалистиката како предмет на интерес го има криминалитетот и деликвентот, односно во центарот на нејзиното внимание се наоѓаат откривањето и спречувањето на кривичните дела и нивните сторители.

Криминалистиката претставува посебна наука, која како трихотомна целост се преточува во систем на научни сознанија со техничка, тактичка и методична димензија. Во нејзиниот состав влегуваат криминалистичка техника, криминалистичка тактика и криминалистичка методика.
Криминалистичката форензика користи криминалистичко–технички средства, тактички начини и криминалистичко-методични правила за откривање, докажување, и разјаснување на кривични дела. Во откривањето и докажувањето на кривичните дела се користат достигувањата на криминалистичката техника и тактика, како и нивните криминалистички средства, начини и препораки, така што практично значи нивна конкретизација и приспособување кон условите за докажување на кривични дела на типичен начин. Таа не е ништо друго, туку целокупност на примената на стандардни методи, начини и средства од техниката и тактиката на конкретен оперативен, односно кривичен предмет, во специфичните услови на криминалистичка контрола, обработка и кривична постапка за одделни видови на кривични дела и сторители.
Голем број на хемичари, физичари, биолози, молекуларни биолози, технолози и многу други, со своите изуми дале придонес во развојот на истражната техника и во проучувањето на однесувањата кои предизвикуваат појава на криминални дела (криминолози, психолози, психијатри, социполози и други).
Истражувањето на криминалот опфаќа обезбедување на докази, користење на технологија, барање и одземање, користење на гаранции. Штом полицијата има сознанија дека се случило криминално дело го отпочнува процесот на истражување со потврдувањето дека криминалното дело нависнина се случило за што ќе се прибират податоци за поддршка на апсењето и ако е возможно да се потврди оптужбата и да се проследи до судот со основано сомнение. Доказите се прибираат во законска постапка. Тие можат да бидат во форма на изјави на сведоци, физички објекти, форензички докази, ДНК извештаи, отисоци од прсти и слично.

2. Улогата на криминалистичката форензика во истражувањето на криминалот

Форензиката е поврзана со примена на научни методи за решавање на кривични дела, вклучувајќи испитување на предметите или супстанциите кои се вклучени во кривичното дело.[61]
Криминалистиката форензика е дел од форензичкта наука која се дефинира како област на примена на научни методи на фундаменталните и применетите науки за обработка на криминални настани.
Поимот форензика потекнува од латинскиот јазик од зборот *forensic* што значи отворен суд - јавност, што всушност значи јавно да бидат изнесени факти кои се поврзани со некое криминално дело. Кога нешто се опишува како форензичко, обично значи дека тоа е поврзано со изнаоѓање докази за решавање на криминал. Тоа, исто така, може да значи дека тоа има врска со судовите или со правниот систем.[62]

[61] Forensic Meaning in the Cambridge English Dictionary, https://dictionary.cambridge.org/dictionary/english/forensic
[62] Forensic - Dictionary Definition, Vocabulary.com, https://www.vocabulary.com/dictionary/forensic

Според научните области кои се применуваат форензиката се дели на форензика на фундаментални и форензика на применети науки.
Криминалистичката форензика ги применува методите на основните и применетите науки за разјаснување и решавање и реконструкција на криминалните настани со цел прибавување на докази. Криминалистичката форензика е само друг назив за криминалистичката техника. Во криминалистичката форензика се користат поимите:[63]

- Криминален настан,
- Место на криминалниот настан (криминалистичка - форензичка сцена, лице место, место на злочинот),
- Докази - резултати на обработката.

Форензичката наука или како често се нарекува само форензика претставува практична примена на науката по прашањата од правото. Во криминалистичкото право, форензичката наука може да помогне да се докаже вината или невиноста на оптуженият. Во цивилните активности форензиката може да помогне да се реши широк спектар на правни прашања преку идентификација, анализи и оценки на физички докази. Форензичката наука користи многу различни научни принципи вклучувајќи ја биологијата, физиката и хемијата. Полето на покритите на форензичката наука покрива:[64]

- Испитување на документи,
- ДНК анализа,
- Електронски/дигитални медиуми,
- Отисоци од прсти,
- Техники на аутопсија,
- Форензички инжињеринг,
- Лингвистика,
- Форензичка антропологија,
- Патологија,
- Економија,
- Сметководство и финансиски менаџмент,
- Биологија,
- Ентомологија,
- Токсикологија и уште многу друго.

Форензичка наука е било која наука која се користи за потребите на правото за да се обезбедат научни докази за судска употреба, односно за криминалистички истраги и судење. Форензичката наука е мултидисциплинарна принципиелно водена од хемијата и биологијата, но исто така и од физиката, геологијата, психологијата, општествените науки и слично.
Форензичката наука е примена на природните науки за работи сврзани со правото. Во практиката форензичката наука е водена од физиката, хемијата и биологијата и од други научни принципи и методи. Форензиката се однесува на препознавањето, идентификувањето, индивидуализацијата и оценката на физичките докази. Форензичките научници, своите наоди ги презентираат како експертски сведоци пред судот. Форензиката е научна анализа и

[63] Ljiljana Mašković: Kriminalistička tehnika, Kriminalističko-policijska akademija Beograd, 2010
[64] Sally Kane: Forensic Science, legalcareers.about.com › ... › Glossary of Legal Terms › Glossary: F - O

документирање на докази потребни за правни постапки. Форензиката ги определува научните факти од доказите, ги оценува и сведочи како експертски сведок во цивилните судови и другите правни постапки. Таа е во одговорност на адвокатите, судиите при пресудувањето, одбраната и во пресудувањето на вината или невиноста не некој поединец обвинет за сторен прекршок. Форензиката е должност на форензичките научници да ги презентираат научните факти на коректен и објективен начин потпрен на прифаќањето на научните методи за да се олесни донесувањето на одлуката.[65]

Форензиката е примена на научна технологија за обезбедување на точни и објективни информации кои се однесуваат на работи кои настанале при извршувањето на некое криминално дело. Форензичарите анализираат докази, обезбедуваат експертски докази, се обучуваат за препознавање, прибирање и чување на физички докази. Физички доказ е се′ што е користено, оставено, преместено, променето или контаминирано за време на извршувањето на криминалното дело, како од страна на осомничените така и од страна на жртвите.

Слика број 1:

Извор: Forensic Science, peer.tamu.edu/NSF_Files/Forensic%20Scientists.ppt

[65] David Webb:Definition of Forensic Science- All About Forensic Science, www.all-about-forensic-science.com/definition-of-forensic-science.html

Функциите на форензичката наука се:[66]

- Да врши анализа на физички докази;
- Да ги применува принципите и техниките на физичките и природните науки со цел да се идентификуваат многуте видови докази кои можат да се вратат во текот на истрагите за криминал;
- Да биде експертски сведок;
- Да поседува одредена вештина или знаење во професијата која ќе му помогне на судот во утврдувањето на вистината;
- Да врши сложена лабораториска анализа за физички докази, да изработува аналитички пристапи кон предметот што може да вклучува истражување и / или генерирање или модифицирање на методи, да толкува аналитички резултати, да подготвува писмени извештаи и да сведочи како вештак во судовите.

Форензичката наука игра витална улога во системот на кривичната правда преку обезбедување научно засновани информации преку анализа на физички докази. Во текот на истрагата, доказите се собираат на место на злосторство или од лице, се анализираат во криминална лабораторија, а потоа резултатите се презентираат пред суд. Форензичарите ги анализираат доказите добиени од полициските службеници и детективи, а потоа подготвуваат детални извештаи за нивните наоди. Форензичката наука може да ја насочи кривичната истрага во вистинска насока или да обезбеди доказ за вина или невиност на осомничениот.

Форензиката или анализата на местото на злосторот, вклучува наука која се применува за обезбедување правни докази кои им помагаат на обвинители, адвокати и судии во разбирањето на физичките докази за сторено кривично дело или да се идентификува и да се осуди криминалец. Форензичките научници вршат физички и хемиски анализи за кривични доаѓање до докази најдени на местото на настанувањето на кривичното дело, за жртвата или за двете. Форензичките научници користат математички принципи, методи за решавање на проблемите, комплексни инструменти и микроскопски техники за испитување за да ги анализираат доказите. Форензичарите вршат поврзување на кривичните дела врз основа на физички докази, даваат информации и ги објаснуваат резултатите на суд. Процесот на форензичката анализа се состои од:[67]

- Прибирање докази,
- Пријавување и анализа на времето,
- Анализа на медиуми,
- Пребарување докази,
- Обновување докази,
- Анализа на доказите,
- Известување.

[66] An Introduction to Forensic Science, www.hcs.stier.org/Downloads/IntroductiontoForensics.ppt
[67] Forensic Analysis, http://hepwww.rl.ac.uk/Sysman/June2010/talks/Day2/HEPSYSMAM_Workshop_Ma.pptx

Слика број 2:

Извор: Forensic Analysis,
http://hepwww.rl.ac.uk/Sysman/June2010/talks/Day2/HEPSYSMAM_Workshop_Ma.pptx

3. Форензички докази

Форензичките докази опфаќаат предмети кои можат да потврдат дека е сторено кривично дело или може да доведат до поврзување меѓу сторителот на кривичното дело и неговата жртва или меѓу кривичното дело и неговиот сторител.

Како форензички докази кои се земаат од местото на настанување на криминалот се зема широк спектар на материјали или траги кои се сметаат за вредни докази за истрагата. Тие форензички примероци можат да бидат:[68]

- Биолошки докази (на пример, крв, телесни течности, коса и други ткива),
- Латентни докази заотпечатоци (на пр., отпечатоци од прсти, отпечатоци од дланка, отпечатоци од нога),
- Обувки и траги од гуми,

[68] Crime Scene Investigation: Guides for Law Enforcement
https://www.nij.gov/topics/law-enforcement/investigations/crime-scene/guides/Pages/welcome.a

- Барање траги (на пр., влакна, траги на почвата, вегетацијата, стаклените предмети),
- Дигитални докази (на пример, евиденција на мобилен телефон, дневници на Интернет, е-пораки)
- Прибор,
- Лекови,
- Огнено оружје.

Во текот на истрагата, форензичките докази се собираат на местото на злосторство и се анализираат во криминалистичка лабораторија, а потоа резултатите се презентираат на суд. Секое место на криминален настан или на злосторствио е уникатно, и секој случај претставува посебен предизвик.
Со физичките докази мора да се постапува на начин кој спречува каква била промена во содржината на доказот меѓу времето од земањето од местото на злосторството и примањето во лабораторијата. Резултатите од лабораторијата можат да:

- Покажат колку се веродостојни за сведочење,
- Го утврдат идентитетот на осомничените или на жртвите,
- Покажат дали осомничените се невини или да се поврзат со криминалното дело и жртвата.

Заклучок

Форензиката претставува примена на научни методи за решавање на криминал. Форензиката се спроведува со спроведување на истраги со кои се врши собирање на форензички докази кои потоа се анализираат со цел да се дојде до заклучок за криминалот и осомничениот.
Форензичката наука користи многу различни дисциплини како антропологија, балистика, биологија/ДНК, хемиска криминалистика, тајни лаборатории, испитување на местото на настанот, испитување на документи, отпечатоци од прсти, анализа на недозволени дроги, компјутерска форензика, дигитални слики, аудио-видео анализа, ентомологија, одонтологија и токсикологија.
Форензиката може да ја докаже вината или невиноста на обвинетиот во кривичното право и може да помогне во решавањето на широк спектар правни прашања во граѓанските активности преку идентификација, анализа и евалуација на физички и други докази.

Литература

1. An Introduction to Forensic Science, www.hcs.stier.org/Downloads/IntroductiontoForensics.ppt
2. Crime Scene Investigation: Guides for Law Enforcement https://www.nij.gov/topics/law-enforcement/investigations/crime-scene/guides/Pages/welcome.a
3. David Webb: Definition of Forensic Science- All About Forensic Science, www.all-about-forensic-science.com/definition-of-forensic-science.html
4. Fisher, B. A. J., Techniques of crime scene investigation. (7th ed.), New York, NY: CRC Press, 2004.

5. Forensic Analysis, http://hepwww.rl.ac.uk/Sysman/June2010/talks/Day2/HEPSYSMAM_Workshop_Ma.ppt
6. Forensic Meaning in the Cambridge English Dictionary https://dictionary.cambridge.org/dictionary/english/forensic
7. Forensic - Dictionary Definition : Vocabulary.com https://www.vocabulary.com/dictionary/forensic
8. Forensic Science, peer.tamu.edu/NSF_Files/Forensic%20Scientists.ppt
9. Giles, A., The forensic examination of documents. In P.C.White (Ed.), Crime scene to court: The essentials of forensic science (2nd ed., pp. 142-171). Cambridge, UK: The Royal Society of Chemistry, 2004.
10. Lee, H. C., Cracking cases: The science of solving crimes, Amherst, NY: Prometheus Books, 2002.
11. Ljiljana Mašković: Kriminalistička tehnika, Kriminalističko-policijska akademija Beograd, 2010.
12. Platt, R., Crime scene: The ultimate guide to forensic science. New York, New York: DK Publishing, Inc., 2003.
13. Ramsland, K., The forensic science of crime scene investigation, New York: Berkley Boulevard Books, 2001.
14. Sally Kane: Forensic Science, 2018, https://www.thebalancecareers.com/the-definition-of-forensic-science-2164401
15. Weedn, V. W., DNA analysis. In C.H.Wecht & J. T. Rago (Eds.), Forensic science and law: Investigative applications in criminal, civil, and family justice (pp. 418-427). CRC, 2006.

Professor, PhD Aleksandra Stankovska
Faculty of Economy –
European University – Republic of Macedonia
Bul. Kliment Ohridski, 68, 1000 Skopje
+389 2 320 2020
e-mail: aleksandra.stankovska@eurm.edu.mk

CYBER CRIME IN BANKING SECTOR

Abstract

The subject of this paper is the current cyber-crime problems in global banking sector. As financial institutions shift to digital channels like online banking and mobile transactions, the attack surface grows, and there is more to protect. Banks are among the most sophisticated enterprises in the world from a security perspective. This is largely because security and online banking go hand-in-hand. *Cybercriminal activity is one of the biggest challenges that humanity will face in the next two decades.*

The paper gives a brief overview of cybercrime scenario in the banking sector and impact of cybercrimes on bank finances. Cybercriminals have developed advanced techniques to not only cause theft of finances and finances information but also to espionage businesses and access important business information which indirect impacts the bank's finances. To improve cybersecurity, banks must elevate the topic and address threats holistically to the highest levels of the organization in a manner that they understand.

Key words: cyber-crime, online banking, mobile transaction, bank finances & cyber – security.

Introduction

Cyber-attacks have become increasingly targeted and complex due to more sophisticated pieces of malware being leveraged and the increasing threat of professional cyber organizations. These cyber criminals are attempting to steal valuable data, such as intellectual property, personal identifiable information, health records, financial data, and are resorting to highly profitable strategies such as monetizing data access through the use of advanced ransomware techniques or by disrupting overall business operations through Distributed Denial of Service (DDoS) attacks.

The term cyber has two constitutive elements, i.e. it relates to electronic communication networks and virtual reality. Both characteristics distinguish cyber risk fundamentally from other types of risks. Firstly, the virtual reality emphasizes, the intangible nature of, and therefore, the difficulties in assessing the losses. Secondly, networks are closely connected to the term cyberspace, which is frequently used synonymously with the Internet. While the Internet might be the main source of cyber threats, cyberspace describes more generally every network that connects IT systems.

With online technology rapidly moving from computers to the palms of our hands, cybercriminals and hackers are evolving their methods to fit the times. In addition to traditional threats to operational resilience, financial institutions and financial market infrastructures are facing growing challenges in the form of cybersecurity threats. The extensive reliance on technology by financial institutions and financial market infrastructures, coupled with the high degree of interconnectedness between them, increases the sector's vulnerability to a cyber-attack. Cybersecurity is a complex and multifaceted challenge that is growing in importance. It is an issue that not only affects the banks and government agencies that are frequently highlighted through the press; its implications continue to expand beyond that. To counter new and emerging threats, organizations will need to learn from previous threats across a range of industries to proactively meet the challenges ahead.

There have been increasing numbers of cyber-attacks reported in recent years across all industries and it is costing the United States an absolute fortune in cyber security. In 2016 there were widely reported attacks on PayPal, Twitter and Spotify to name a just a few of the big companies that have been targeted. The number of cyber-attacks across the world is increasing and businesses are spending more and more money in deterring the crime.

The banking sector is one of the industries that are most at risk, given the nature of the data that they hold. This means that banks have had to dedicate significant funds on developing their digital infrastructure to strengthen their cyber security. Financial sector faced almost three times the cyber-attacks as compared to that of the other industries. Customers are using biometrics for banking activities such as authentication for mobile banking, transaction at ATMs and payments. With increasing risks of cyber threats, banks are facing an unprecedented challenge of data breaches and are therefore strengthening their cyber security postures.

As well as spending more on software to reduce the chances of an attack, companies now spend more on resources dedicated to preventing cyber-attacks. This means that extra IT personnel are required, extra training for all staff and more resources allocated to analyzing their cyber security and performing risk assessments. It also means that more robust policies and processes must be introduced. This can vary from developing and delivering online training for staff to raise awareness about the risks of cyber security, to employing a whole team of experts to audit the processes. It is certainly becoming a very costly affair.

Methodology

To achieve the object of this paper, the cyber-risk and cyber-security data has been collected. The primary information is mostly from websites, books, journals, etc.

Analysis and discussion

Banks use standardized electronic messages, made up of codes and identifiers, a sort of a common financial language, to make international payments and move money around the world. There are checks and balances, policies, and procedures in place to comply with legal requirements, validate the parties involved, detect irregularities, and looking out for anything suspicious, anything out of the ordinary. Transactions are checked against special databases such as those containing information on blacklisted individuals and entities or those under government

sanctions. Hundreds of billions of dollars are at stake so it is hardly surprising there are so many controls built into the system. But even with all these financial fortifications in place and armies of back-office staffers monitoring money movements, now and again hackers manage to get way with very large sums of money.

Cyber-attacks not only cost businesses from the initial financial sting, they are also impacted by the reputational damage that the attacks can cause for years to come. If somebody feels that their money isn't safe with a bank, then they are likely to close their account and go to another one that they feel will protect their money better. The more publicity that a cyber-attack attracts, the higher the reputational damage will be. As mentioned before, the government is committed to driving down and eventually eradicating the threat of cyber-attacks. Greater cyber security laws are being ratified and harder punishments will be a deterrent for many would-be cyber criminals.

The cyber security industry has known for some time that underground markets have sprung up in cyber-crime community which specializes in the buying and selling of information stolen from company computer networks. At one time any stolen information had to be immediately tradable to be of value. What has changed is that hackers are now quite happy to harvest as much information as possible and are prepared to sit on that information until such time as it has a real value. That's the major concern, and that's what's troubling the security industry.

U.S. regulators warned that denial of service attacks which disable ATMs and bank websites were rising dramatically. From these attacks criminals were able to extract funds from accounts far in excess of cash balances or ATM control limits. According to Michael Coates, director of product security at cyber-security firm, Shape Security, although banks are doing all within their powers to limit the damage that hackers can wreak, they are failing as the hackers are always staying two steps ahead of them. The reasons for this failure he put down to the complexity of current banking computing systems which afforded more opportunities for hackers to target various parts of the network and transaction systems[1].

Most cyber security assessment programs, while well-intentioned, are highly theoretical and based on known cyber-attack practices. The reality, however, is very different. Fast-moving, dynamic threats are creating new challenges every day. Banks should focus on deploying practical testing scenarios that focus inside the perimeter to ultimately make the crooks' job as difficult as possible[2].

The banks are attractive targets and they are under a constant barrage of cyber threats, so purely on the basis of statistics, if there are millions of attempts every year, there is a fair chance a few major incidents will take place." One area where banks need to improve is communicating internally and externally about cyber-attacks.

An important part of assessing the potential for systemic risk from a cyber-attack understands the channels that could propagate the effects of an attack across the financial system. The potential seriousness of such attacks depends on the degree to which an entity's business operations are impaired. A cyber-attack that results in

[1] https://www.krypsys.com/malware/cyber-attacks-target-global-financial-sector

[2] https://www.computerweekly.com/news/450417135/Banks-suffer-average-of-85-attempted-serious-cyber-attacks-a-year-and-one-third-are-successful

the theft of financial or proprietary data does not affect the core functions of the financial institution.

Table 1

WORLD INTERNET USAGE AND POPULATION STATISTICS DEC 31, 2017

World Regions	Population (2018 Est.)	Population % of World	Internet Users 31 Dec 2017	Penetration Rate (% Pop.)	Growth 2000-2018	Internet Users %
Africa	1,287,914,329	16.9 %	453,329,534	35.2%	9,941 %	10.9 %
Asia	4,207,588,157	55.1 %	2,023,630,194	48.1 %	1,670 %	48.7 %
Europa	827,650,849	10.8 %	704,833,752	85.2 %	570 %	17.0 %
Latin America/ Caribbean	652,047,996	8.5 %	437,001,277	67.0 %	2,318 %	10.5 %
Middle East	254,438,981	3.3 %	164,037,259	64.5 %	4,893 %	3.9 %
North America	363,844,662	4.8 %	345,660,847	95.0 %	219 %	8.3 %
Oceania/Australia	41,273,454	0.6 %	28,439,277	68.9 %	273 %	0.7 %
WORLD TOTAL	7,634,758,428	100.0 %	4,156,932,140	54.4 %	1,052 %	100.0 %

Source: https://www.internetworldstats.com/stats.htm

The role of cybersecurity within an organization, even for those who have previously considered themselves immune to needing IT security, has become central to appropriate risk management practices. The fundamental importance of IT for firms today cannot be underestimated. Knowing the risks related to using IT must be captured and understood by executive management and the board as part of the organization's overall risk-management strategy. The voice of this analysis comes from the CISO (Chief Information Security Officer)[3]. This necessitates that cybersecurity practices be present on the executive agenda. Specifically, the CISO, regardless of reporting relationships, should provide guidance and expertise on the following[4]:

1. Cybersecurity practices, procedures, and metrics;
2. Data and asset classification from a security and risk – perspective (including privacy impacts);
3. Vigilance and monitoring of cybersecurity activities and trends;
4. Oversight of auditing and governance practices including liaised with internal and external audit;

[3] Bonney Hayslip Stamper, Bill Bonney, CISO Desk Reference Guide: A Practical Guide for CISOs, Volume 1, CISO DRG Joint Venture, 2016, pp17.
[4] Ibidem, pp.18.

5. Incident response in collaboration with the organization's counsel;
6. Security services implementation;
7. Security training; &
8. Holistic risk management and risk assessment reporting (including vendor and business processes).

Analysis of more than 15 billion transactions over a 12 month period by the Threat Metrix Digital Identity Network revealed a 40 per cent increase in cybercriminal activity targeting the financial sector, with a record 21 million fraud attacks and 45 million bot attacks detected in the last three months of 2015 alone. The analysis also revealed that the financial sector is facing the highest number of organized attacks and multi-channel threats in 2016, with the biggest emerging threat for financial institutions being bot attacks, which increased 10 times in the last three months of 2015 compared with the same period in 2014. A worst-case attack scenario could see a major bank or financial institution completely paralyzed for days, leading to billions in potential lost revenue[5].

According to PwC's most recent Global State of Information Security® (GSIS) Survey, the most common type of cyberattack in 2016 was phishing. Firms also faced growing risks due to business email compromise, ransomware, and distributed denial of service (DDoS) attacks. And criminals and other threat actors aren't giving up, as shown by the SWIFT incident and rising concerns over payment systems.

Cybersecurity isn't a partisan issue. Financial institutions will be pushed to collaborate more with regulatory bodies to collectively share information. They'll have better visibility into emerging threats—and a greater responsibility to prepare for them. Most firms have realized the benefits of working together and with governmental bodies to prevent cyberattacks. The coming year will be no different. Industry collaboration will grow through venues such as Financial Services Information Sharing and Analysis Center (FS-ISAC) and new initiatives such as the Financial Systemic Analysis & Resilience Center (FSARC) and Sheltered Harbor.

Firms must already comply with industry, state, federal, and international privacy regulations. The CFPB recently announced consumers can give permission for third parties to access their information. Firms will likely share blame for mishandled data. Combining cloud services with tools like artificial intelligence and blockchain will introduce new risks—and require new approaches to combating those risks. As business goes digital, cyber spend increases. In fact, 54% of US financial services respondents to our GSIS survey plan to spend more on beefing up security in the mobile channel[6].

Blockchains could potentially help improve cyber defense as the platform can secure, prevent fraudulent activities through consensus mechanisms, and detect data tampering based on its underlying characteristics of immutability, transparency, auditability, data encryption & operational resilience (including no single point of failure)[7].

According to a 2017 IBM Study of 3,000 global C-suite executives, 33 percent of organizations, across industries, are considering or actively engaged with Blockchain.

---

[5] Mark Camillo, Cybersecurity: Risks and management of risks for global banks and financial institutions available at. https://www.aig.co.uk/content/dam/aig/emea/united-kingdom/documents/Insights/jrmfi-mark-camillo-article-mar-2017.pdf

[6] https://www.pwc.ch/en/publications/2017/pwc_top_financial_services_issues_2017_en.pdf

[7] https://www2.deloitte.com/content/dam/Deloitte/ie/Documents/Technology/IE_C_BlockchainandCyberPOV_0417.pdf

Improvements in security against fraud and cybercrime make up 56 percent of the reason business leaders are currently using or considering adopting blockchain in their organizations[8].

Blockchain has a number of benefits: it is implicitly secure, adaptable, cost-effective and universally accessible. People are starting to wake up to the practical uses of blockchain and its potential to revolutionize industries and solve age-old problems – one of which is cybercrime. Traditionally, organizations store information on centralized systems and challenge people to prove they know the information stored, before acting on their instructions. However, recent high profile cases of cybercrime have emphasized that our personal information is no longer secure. The Equifax data breach, in which the personal information of 143 million Americans and 400,000 Britons may have been stolen in the summer of 2017, is just one example.

The ONS recorded six million cases of fraud and cybercrime in England and Wales in 2015/16, which cost the UK £11 billion. However, with few alternatives, consumers have no choice but to place their trust in organisations when it comes to managing and handling their personal details securely[9]. That is until now. The application of blockchain technology could provide the solution to the cybercrime epidemic. In addition, as the blockchain network is decentralised, it avoids the inflexibility, inefficiencies, costs and weaknesses embedded in centralised systems.

The cyber insurance market is very small at present compared to other lines of business, but is expected to increase significantly in the coming years. The U.S. is far ahead of Europe and Asia, for example, with regard to reporting requirements. The main insurability problems are the lack of data, risk of change, accumulation risk, and potential moral hazard problems[10].

Estimating the costs caused by cyber risk is difficult, as there is high uncertainty and no accepted source of information. The incentive of affected institutions not to communicate cyber risk incidents and limited notification requirements contribute their share to the information deficit. Some types of cybercrime may even cause no costs at all or cannot be quantifiable (e.g. spread of racism, mobbing, trading of illegal drugs).

The 'WannaCry' ransomware attack in May 2017, infecting over 200,000 systems in more than 150 countries in less than a day, demonstrated the immediate global impact that a single coordinated cyber-attack can have. Cyber risks, and the system-wide spillovers associated with those risks crystalizing, are not limited by national borders and their spread cannot be easily controlled by national laws or authorities working in isolation, particularly not in the financial sector.

Equally, from a bank's perspective, emerging regulatory regimes for cyber resilience that develop unevenly create the potential for overlaps and gaps. This could give rise to significant complexity and costs which may even unintentionally weaken their efforts to defend against cyber-attacks in future.

2018 will be an important year for the regulation of cyber resilience in banks. One of the biggest challenges in cyber regulation that executives at internationally-active banks often point to is the sheer number of rules and procedures related to cyber

[8] https://medium.com/swarmdotmarket/blockchain-in-cyber-security-who-is-who-269d89feadc1
[9] https://www.ibtimes.co.uk/blockchain-solution-cybercrime-epidemic-1660702
[10] https://www.ivw.unisg.ch/_/media/internet/content/dateien/instituteundcenters/ivw/studien/studie-10-key-questions.pdf

that are emerging in jurisdictions where they operate, and the lack of alignment between many of them.

Conclusion

Any risk emerging from the use of information and communication technology that compromises the confidentiality, availability, or integrity of data or services. The impairment of operational technology (eventually leads to business disruption, infrastructure breakdown, and physical damage to humans and property. Cyber risk is either caused naturally or is man-made, where the latter can emerge from human failure, cyber criminality, cyberwar, and cyber terrorism. It is characterized by interdependencies, potential extreme events, high uncertainty with respect to data and modelling approach, and risk of change. Today, most banks are either completely hacked or could be easily be hacked. The truth is that most banks are not doing the right things in the right places, making it easier for hackers and malware to infiltrate an organization that it needs to be. Most banks are highly inefficient at computer security defense, and wonder why they are still so easily hackable while at same time throwing ever growing amounts of capital, resources, and people at the problem.

Reference

1. Bonney Hayslip Stamper, Bill Bonney, CISO Desk Reference Guide: A Practical Guide for CISOs, Volume 1, CISO DRG Joint Venture, 2016.
2. Mark Camillo, Cybersecurity: Risks and management of risks for global banks and financial institutions, available at https://www.aig.co.uk/content/dam/aig/emea/united-kingdom/documents/Insights/jrmfi-mark-camillo-article-mar-2017.pdf
3. Schwartz, J. (2016) 'Show me the money: Financial sector a big target for cyberattacks', available at: https://www.mediapro.com/blog/ financial-sector-target-cyberattacks/ (accessed November 2016).
4. North Carolina Journal of Law & Technology Volume 18, Issue 2: December 2016 233 Is Cyberattack The Next Pearl Harbor? Lawrence J. Trautman available http://ncjolt.org/wp-content/uploads/2016/12/Trautman_Final.pdf
5. https://www.ivw.unisg.ch/_/media/internet/content/dateien/instituteundcenters/ivw/studien/studie-10-key-questions.pdf
6. http://www.ijcrar.com/vol-2-2/A.R.%20Raghavan%20and%20Latha%20Parthiban.pdf
7. https://www2.deloitte.com/content/dam/Deloitte/ie/Documents/Technology/IE_C_BlockchainandCyberPOV_0417.pdf
8. https://medium.com/swarmdotmarket/blockchain-in-cyber-security-who-is-who-269d89feadc1
9. https://www.ibtimes.co.uk/blockchain-solution-cybercrime-epidemic-1660702

Asst. Prof. Anis Sefidanoski
European University - R.M
anis.sefidanoski@eurm.edu.mk

"Artificial Intelligence for the future of Knowledge Management"

Abstract

Knowledge is the greatest and most valuable corporate asset a company can have. Data on its own has no meaning, only when interpreted by some kind of data processing transforms to information and eventually becomes knowledge. With every customer interaction we learn more and get closer in providing the best possible customer service and experience. Employees are using valuable time and information dealing with dispersed data and information silos. Documents, charts, multimedia, project plans, conversations are scattered all over the corporate networks systems, making them hard to access and manage. Customer involvement and user satisfaction quantification is crucial to knowledge management but absent in the state of the art Knowledge Management (KM) solutions.
Artificial Intelligence (AI) based knowledge management platform aims to make information tangible, measurable and omnipresent in order to create 360 degree awareness of your corporate knowledge using cutting edge technologies, i.e. Big Data, Machine Learning (ML), Internet of Things (IoT), Natural Language Processing (NLP) and predictive analytics, combined with the power of the new communication paradigms and interaction styles. Ubiquitous capture, processing and dissemination of knowledge will deliver unified and continuous knowledge management experience and evolve the way organization learns and works.

Keywords: Knowledge Management, Artificial Intelligence, Big Data, Machine Learning, Digitalization, Virtualization, Automation

Доц. д-р Анис Сефиданоски
Европски Универзитет - Р. М
anis.sefidanoski@eurm.edu.mk

"Вештачка интелигенција за идното управување со знаењето"

Апстракт

Знаењето е најголемото и највредното корпоративно богатство кое една компанија може да го има. Самостојните податоци немаат никакво значење и само кога истите се толкуваат со некој вид на технологија за обработка на податоци се претвараат во информација која на крајот станува знаење. Со секоја интеракција на модерните купувачи дознаваме повеќе за нив и се приближуваме кон обезбедување на најдобра можна услуга и искуство на нашите клиенти. Вработените професионалци користат драгоцено време и информации кои се занимаваат со дисперзирани податоци и информациски

силоси. Документи, графикони, мултимедијални податоци, проектни планови и разговори, расфрлани низ целиот систем на корпоративни мрежи, што ги прави скоро невозможни за пристап и управување. Инклузијата на клиентите и квантификацијата на задоволството на корисниците е од клучно значење за управувањето со знаењето, елементи кои сеуште отсуствуваат во современите решенија за управување со знаењето (Knowledge Management, KM).

Платформите за управување со знаење базирани на вештачка интелигенција (Artificial Intelligence, AI) имаат за цел да ги направат информациите опипливи, мерливи и сеприсутни, со цел да се создаде интегрирана свесност за корпоративното знаење од 360 степени, преку користење на најсовремените технологии, т.е. Big Data, Машинско учење (Machine Learning, ML), Интернет на работите (Internet of Things, IoT), Обработка на природен јазик (Natural Language Processing, NLP) и предвидувачка анализа, во комбинација со моќта на новите комуникациски парадигми и стилови на интеракција. Сеприсутното регистрирање, обработка и дисеминација на знаењето ќе овозможи унифицирано и континуирано искуство во управувањето со знаење, со што ќе се овозможи еволутивен и органски развој на методологијата со помош на која корпоративната организација учи и работи.

Клучни зборови: *Управување со знаење, Вештачка интелигенција, Машинско учење, Дигитализација, Виртуализација, Автоматизација*

Вовед

Ефикасното управување со знаењето, како суштински процес на секоја модерна организација, безброј пати се редефинирале во форма на различни корпоративни методологии, техники и технологии, со цел да се зголемат резултатите и бенефитите од истата. Традиционалните методи за управување со знаење како што се книгите и упатствата, предавањата и аудиовизулените презентации, базите на податоци, електронските пребарувачи, вклучуваат повеќе ограничувања од кои најголемото е степенот на релевантноста, кое всушност новите информатички технологии постојано се стремат да го надминат. Недостатокот или ограниченоста на степенот на адекватно претставување на податоците и информациите кои се извечени од истите, исто така го носи со себе и ризикот за несоодветно толкување на знаењето кое произлегува од интеракцијата помеѓу корисникот и информацијата.

Благодарение на најновиот технолошки развој во рамките на новите технологии, денес имаме можност да реализираме софистицирани платформи за управување со знаењето, со цел за максимизирање на продуктивноста и бенефитите од колаборативната работа и комуникација на далечина со помош на компјутер. Синергијата на трите главни претставници на новите технологии: вештачката интелигенција (Artificial Intelligence, AI), виртуелната реалност (Virtual Reality, VR) и системите за управување од далечина (Remote Control, RC), комбинирани со моќта на интернетот и веб сервисите, го претставуваат темелот на развојната платформа која претставува предмет на научно и практично истражување на овој труд.

1. Методологија на управување со знаењето

Спротивно на традиционалните парадигми на вештачката интелигенција, предложеното решение кое е предмет на трудот се стреми да воведе нов концепт во машинското учење и интеракцијата помеѓу човекот и компјутерот (Human-Computer Interaction, HCI).[69] Со помош на најновите технологии базирани на машинско учење (Machine Learnng, ML), развојната платформа имплементира интерактивни аватари (Interactive Avatars) кои ја вршат менторската улога во секоја од активностите при управувањето со знаењето. Наместо да одговараат на поставени прашања или задачи од страна на корисниците, виртуелните ментори оркестрираат активности кои корисниците мора индивидуално или групно да ги извршат, според претхондо детално дефинирани процедури. Соодветните процедури се опишани на еден или повеќе од традиционалните-offline медиуми, како и во базата на знаење (Knowledge Database) на платформата, која постојано е ажурирана и синхронизирана од страна на сите активни корисници. Мноштво на паралелно соодветни одговори во форма на вкрстени процедури се еваулирани во реално време за секоја поединечна активност на корисникот, според што се врши и рангирање на релевантноста на самите податоци. Дополнителниот модул за самоевалуација на корисниците овозможува надградување на базата на знаење со нови процедури во форма на одговори, односно прашања кои ги користи виртуелниот ментор.

1.1 Нова парадигма за размена на знаењето

Содржините кои се генеририрани во самиот процес на управување со знаењето, при интеракција со и помеѓу корисниците, менторите, како и вештачката интелигенција (Artificial Intelligence, AI), се чуваат на страна на интегрираната платформа од каде се локално синхронизирани со секој претходно регистриран и автентикуван корисник. Во текот на демонстрацијата на користење на одредена техника или технологија која е предмет на обуката, предложената платформа за секоја успешно извршена активност генерира интерактивни скрипти за само-евалуација (self-evaluation) и понатамошна автоматизација (automation) на процесот на учење. Секој чекор од поединечните активности дефинирани во одреден курс е зачуван во форма на мултимедијална содржина која вклучува интерактивна графика и звук, со цел да се емулира целосно околината поврзана со вештината која треба да ја совлада корисникот. Надминувајќи ги класичните платформи и системи за автоматско генерирање на кориснички упатства, кои вклучуваат серија на слики од работната околина со маркирани зони на поединечни активности, платформата ја емулира интегрално алатката која се користи за изичување на одредена техника, со тоа што целата постапка е интерактивно презентирана на корисникот преку хипермедијална апликација.[70] Исто така, бидејќи за секоја задача можат да постојат мноштво логички и валидни

[69] Bransford, J., Brown, A., & Cocking, R. R. (2000). "Technology to support learning". In J. Bransford, A. Brown, & R. R. Cocking. How people learn: Brain, mind, experience. Washington, DC: National Academies Press

[70] Ross, S., Morrison, G., & Lowther, D. (2010). "Educational technology research past and present: balancing rigor and relevance to impact learning". Contemporary Educational Technology

процедури, самите корисници можат да генерираат свои работни скрипти, при што секој поединечен чекор е евалуиран во реално време од страна на модулот базиран на машинско учење (Machine Learning, ML), со тоа што се споредуваат процедурите кои претходно биле генерирани од страна на другите корисници, земајќи ги во предвид резултатите од нивните активности. Сите содржини кои се генерирани од страна на корисниците на платформата, вклучувајќи ги и мултимедијалните скрипти за виртуелна обука, се достапни преку веб модул поставен на интернет во форма на интерактивен водич, односно квиз за евалуација на постигнатиот степен на знаење. Учесниците во обуките имаат исто така можност взаемно да ги отценуваат резултатите и постигнатиот успех од колаборативната работа, при што се нуди зголемена мотивација и транспарентност за придонесите на поединечни корисници.

2. Сеприсутност vs. централизација на информациите

Благодарение на интеграцијата на управувањето со знаењето, како и централизираната база на знаење, корисниците можат да имаат директна синхрона и асинхрона комуникација помеѓу себе, при што нивните улоги се релативни на целите. Во сооднос со постигнатиот степен на совладување на потребните знаења и добивање на неопходните информации, секој корисник може да ја превземе улогата на ментор, користејќи ги неограничено бенефициите на надградената интелигенција (Augmented Intelligence, AI), и да колаборира со сите останати учесници во обуката кои се наоѓаат на пониско ниво. Секој допринес кој е автоматски детектиран од страна на системите на платформата, благодарение на функцијата за само-евалуација, се препознава во форма на дигитален сертификат за зголемени привилегии, афирмација во рамки на социјалната мрежа, како и добивка на виртуелни средства за уплата на нови напредни курсеви за обука во рамки на инсталацијата на предложеното решение.

2.1 Управување со податоци од далечина

Како и во сите останати компоненти на предложената платформа, така и во модулот за далечинско управување на информациски системи, нашата теза се труди да воведе иновација со цел да се зголеми ефикасноста на функционалноста и да се понуди ново корисничко искуство за сите актери во процесот на размена на знаења. Класичниот модел на далечинско управување со компјутер (Remote Desktop Control) вклучува два физички или виртуелни компјутерски системи кои се наоѓаат на две физички одделени локации, односно два физички или виртуелно индивидуални хоста (Virtual Hosts). Модулот за далечинско управување на виртуелен компјутер на далечина, предлага два виртуелни компјутери на еден физички хост постоавен на платофрмата, со што се овозможува синхроно поврзување на повеќе корисници на една или повеќе истанци од виртуелните работни околини. Впрочем, традиционалното далечинско управување со компјутер еден кон еден (one to one), се заменува со еден кон многу (one to many), многу кон еден (many to one) и многу кон многу (many to many). Овој концепт практично го дозволува релативизирањето на улогите на учесниците во

процесот на обука, т.е. секој корисник може да ја врши функцијата на ментор и обратно. Пристапот е овозможен од сите платформи, а за секој поединечен хардверски уред од кој се најавува корисникот се изработени посебни адаптабилни апликации достапни на истата адреса. Мобилните апликации за паметни телефони, таблети, паметни часовници и други мобилни уреди, се имплементираат со помош на сервиси базирани на GPS локација (Location Based Services), кои понатаму се синхронизираат со актуалниот профил на корисникот. Нотификациите и достапноста на корисниците и менторите овозможуваат континуирана активност, мотивација и целосно инволвирање на учесниците во секоја од активностите на обуката.

Предложениот модел за далечинско управување со работна околина исто така гарантира максимална приватност за крајните корисници, бидејќи на ниту една од инволвираните страни не се пристапува до приватните хардверски ресурси или софтверски содржини. Корисниците воедно можат да колаборираат преку споделување на своите виртуелни околини, без притоа да се грижат за приватноста. Исто така, сите работни сесии преку модулот за управување на далечина можат да се снимаат на серверска страна, со цел подоцна да се користат во мултимедијалната архива на секој корисник, како и во форма на интерактивни видео курсеви за идните корисници.

3. Вештачка интелигенција за ефикасно учење

Со цел да се зголеми ефикасноста, како и да се автоматизираат менторските активности во процесот на управување со знаењето, се воведуваат виртуелни агенти кои се во постојана интеракција со косисниците. Виртуелните агенти можат да бидат ограничени на текстуална и вербална комуникација, но во одредени сценарија истите овозможуваат и директна комуникација со помош на тродимензионални интерактивни аватари. Главната цел на виртуелниот агент е максимално да го помогне и поддржи корисникот при процесот на учење, со што истиот има задача да презентира, коригира и информира во секоја дадена ситуација на виртуелна тродимензионална сцена[71]. Некои од системите за управување со знаење исто така имплементираат агенти со тродимензионални аватари кои имаат функција на модули за мониторинг, односно следење на работата на корисникот. Во овој случај најчесто се работи за функционалност од психолошка перспектива, бидејќи корисниците стануваат поодговорни во присуство на друг корисник[72]. Во апликациите за групна соработка (Collaborative Work), односно повеќекорисничките системи за управување со знаење, агентите исто така наоѓаат примена со цел поефикасно да ги координираат групите при извршувањето на нивните заеднички задачи. Доколку виртуелниот агент користи техники и технологии базирани на машинско учење и вештачка интелигенција, истиот има можност

[71] Blascovich, J., Bailenson, J. (2011). "Infinite Reality: Avatars, Eternal Life, New Worlds, and the Dawn of the Virtual Revolution", Harper Collins

[72] Bear, Amy (27 April 2010). "Me, My Self, My Character, and I: Role-playing Identities in Ludic Space.". Online Conference on Networks and Communities

да ги разбира и детално елаборира сите превземени активности од страна на учесниците[73].

3.1 Виртуелни агенти за асистенција

Виртуелните агенти базирани на вештачка интелигенција користат технологии и техники од машинското учење кои им овозможуваат секогаш да ја надградуваат својата база на знаење преку следење и евалуација на активностите на другите учесници вклучени во процесот на пребарување на информации како и обука. Со цел да се мотивираат корисниците, виртуелните аватари имплементираат и напредни техники за комуникација на човечки емоции. Експресијата на лицето, движењето на екстремитетите и другите делови од човечкото тело, се од круцијална важност при процесот на обука во одредени корпоративни сфери, како што се маркетингот, говорништвото, грижата на корисници, итн. Јазикот на телото претставува исто така неразделив дел од вербалната комуникација и истиот може да понуди дополнителни повратни информации при интеракцијата. Нешто што претставува главна карактеристика и предуслов за сите виртуелни агенти е живописот и веродостојноста на нивното претставување, односно колку кредибилни ќе бидат истите при комуникацијата со учесниците во обуката. Платформи и системи кои инкорпорираат виртуелни агенти, а притоа не ги задоволуваат претходно опишаните аспекти, можат само да го отежнат процесот на учењето и управувањето со знаење, како и да ја намалат ефикасноста кај истиот[74].

Заклучок

Иако проблематиката на платформите и системите за управување со знаењето веќе зафаќа добар сегмент од традиционалните истражувањата[75] во информатичката наука и нејзините применети апликации, во рамките на овој труд се обидовме да предложиме хибридна интеграција на неколку денешни претставници на новите технологии со цел да се понуди ново корисничко искуство при учење и управување со знаење на далечина, како и да се зголеми ефикасноста од примената на информатиката во различните области на корпоративната и бизнис сфера. Балансот помеѓу предностите и ограничувањата кои ги нудат новите технологии, како и конзервацијата на традиционалните стилови и методлогии за онлајн учење, претставуваат двата главни критериуми во текот на нашето истражување. Благодарение на ова успешно ги адресираме сите поставени хипотези на докторскиот труд, без притоа да ја напуштиме рамката на досегашните придонеси и резултати од оваа област, а во исто време да воведеме иновативна парадигма и ново корисничко искуство со помош на симбиоза од повеќето достапни технологии.

---

[73] Nowak, K. L. and Rauh, C. (2005), The Influence of the Avatar on Online Perceptions of Anthropomorphism, Androgyny, Credibility, Homophily, and Attraction. Journal of Computer-Mediated Communication

[74] Maria Popova, Brain Pickings, December 14, 2011, "Alter Ego, Portraits of Gamers next to their Avatars"

[75] Beyerlein, M; Freedman, S.; McGee, G.; Moran, L. (2002). Beyond Teams: Building the Collaborative Organization. The Collaborative Work Systems series, Wiley

Библиографија

1. Bransford, J., Brown, A., & Cocking, R. R. (2000). "Technology to support learning". In J. Bransford, A. Brown, & R. R. Cocking. How people learn: Brain, mind, experience. Washington, DC: National Academies Press
2. Ross, S., Morrison, G., & Lowther, D. (2010). "Educational technology research past and present: balancing rigor and relevance to impact learning". Contemporary Educational Technology
3. Blascovich, J., Bailenson, J. (2011). "Infinite Reality: Avatars, Eternal Life, New Worlds, and the Dawn of the Virtual Revolution", Harper Collins
4. Bear, Amy (27 April 2010). "Me, My Self, My Character, and I: Role-playing Identities in Ludic Space.". Online Conference on Networks and Communities
5. Nowak, K. L. and Rauh, C. (2005), The Influence of the Avatar on Online Perceptions of Anthropomorphism, Androgyny, Credibility, Homophily, and Attraction. Journal of Computer-Mediated Communication
6. Maria Popova, Brain Pickings, December 14, 2011, "Alter Ego, Portraits of Gamers next to their Avatars"
7. Beyerlein, M; Freedman, S.; McGee, G.; Moran, L. (2002). Beyond Teams: Building the Collaborative Organization. The Collaborative Work Systems series, Wiley

Assistant Profesor Tatjana Gerginova, PhD
Faculty of security – Skopje
tanjagerginova@gmail.com

THE SYSTEM FOR SECURING PEOPLE AND PROPERTY IN THE COMPANY – AN IMPORTANT COMPONENT FOR EFFECTIVE BUSINESS OPERATIONS OF THE CORPORATION

Abstract

Within the framework of the paper, the author will define the concept of corporate security and will determine the tasks and characteristics of corporate security. The author analyzes the system for securing people and property in the modern company as an important component for efficient business operations of the modern company, and determines the types of security such as physical security, technical security and security-protection component of the security
In the final part, the author determines the contents to be achieved through the efficient and professional realization of the system for securing persons and property in modern corporations.
The subject of research is defining and analyzing the term corporate security with an overview of the system for securing people and property in a modern company.
Purpose of research is the importance of corporate security in scientific literature and the role and place of the term corporate security in scientific literature.

Key words: corporate security, providing individuals and property in the company, technical security, physical security

INTRODUCTION

Globalization has led to the creation of trade blocs, global companies and global economies. Basic economic aspects of globalization liberalization, attracting investment and privatization. The main role of the market have multinational corporations. In modern conditions in addition to meeting the security of citizens and the state, particular attention is given to the achievement of security in corporations, which includes achieving the protection of employees in the corporation, protection of property owned by business organizations protect profits, business success, and quality of the implementation of business processes in the corporation, protection of service users, protection of information and the reputation of the business organizations of various hazards, risks, property damage, criminal activities etc..[76]
In security theory and practice, there are essential differences in the determination of the term "corporate security", and therefore also in terms of its content. In the scientific literature you can find the following definitions for corporate security.

76 Gerginova, T., *Corporate security,* Publisher Faculty of security – Skopje, 2017.

According to Christopher Kjubig and David Brooks, corporate security is aimed at detecting fraud and offenses, and studies and real cases of corporate crisis, crime, and other crimes for which the professionals in corporate security should be aware of to ensure effective protection of people, operations and resources.[77]
Michael Genser believes that corporate security is adjusted to meet the structural risks for the company, through the application of certain models of simulation for implementing the best security practices in the company.[78]
Nicole Detelhof and Klaus Wolf in their compilation of landscaping materials, corporate security is aimed at corporate security responsibility, which is focused on the role of private business in conflict zones. It provides a picture of the types of contribution to peace and to security by transnational corporations.[79]
Peter Reid believes that corporate security should provide the necessary balance between the level of security in corporate, business and conventional demands of work complemented with wisdom, and thus offered radical but inspired proposal for success. In that direction should be a survey of companies with common sense and logic to better business consistency.[80]
Milan Milosevic suggests that corporate security for its definition is integrated because it includes perform a number of functions that need to be synchronized. As such, it is a function of the corporation that controls and managing the coordination of all activities within the enterprise, and which relate to safety, continuity and reliability. The existence of an effective system of corporate security protects the company from any threatening actions, establishes the basis for making management decisions, provides the top management access to secret information and form processes and procedures that prevent spilling protected data from the corporation.[81]
Ivandikj, Karlovic and Ostojic corporate security defines as a strategic function of the company, which aims at realizing the safety of the business success of the corporation, which means: the elimination of all risks and threats that may affect business activities and achieving business success; reduction of the factors threatening the lowest possible level; business operation in crisis, i.e. overcoming the crisis and re-establish normal operations.[82]
Certain definitions are very broad in its view, regarding corporate security as part of national security in the context of realizing so called Civilian security. In this context, Slobodan Markovic believes that corporate security is a subsystem of national security and it was part of the security structures with a set of social goals that guide the business activities of companies and measure their social responsibility in accordance with the standards and law.[83]

---

[77] Christopher J. Cubbage and David J. Brooks, *Corporate Security in the Asia-Pacific Region:Crisis, Crime, Fraud, and Misconduct,* CRC Press, 2012, pp. 3-16.
[78] Michael Genser, *A Structural Framework for the Pricing of Corporate Securities: Economic and Empirical Issues,* Springer-Verlag New York, LLC, 2005, pp. 196-238.
[79] Nicole Deitelhoff, Klaus Dieter Wolf (Editor), *Corporate Security Responsibility?: Corporate Governance Contributions to Peace and Security in Zones of Conflict,* Palgrave Macmillan, 2010, pp. 2-20.
[80] Peter Reid, *How to Land a Top-Paying Corporate securities research analysts Job,* Emereo Pty Ltd, 2012, pp. 5-25
[81] Milosevik, M., "*The concept and content of corporate security*", in Scientific Conference "Days of security" on the theme: "Corporate security - the risks, threats and protection measures" (Proceedings), Faculty of Safety and Protection of University Synergy, Banja Luka 2010, p. 59-60.
[82] Ivandic Vidovic Darius Karlovic Lydia, Ostojic Allen, Corporate Security, Association of Croatian managers of security - UHMS, Zagreb 2011, p. 34th
[83] Marković I. Free, op. cit. p. 21st

From the said considerations for corporate security, it can be concluded that has a lack of a precise definition of this term. The definition of this term is extremely difficult, because the true nature and scope of the field of corporate security is difficult to determine. Also, the definition is hard to do, because there is a certain division in opinions on what should be of great interest to corporate security, and in order not to enter the field of interest of private security. In this context, some authors even identify these two terms, while others believe that some security managers should take specific security roles to be recognized for corporate security. For example, the director of corporate security should belong to the highest level of middle management of the corporation and its tasks should be goal setting, strategic planning and ensure safety in the company.
The general impression is that the field of corporate security is very important and essential to the work of the corporation. This statement shows our generalization that corporate security is focused on processes and conditions in a particular corporation or better safety management, will mean bringing relevant decisions on how to protect owners and managers, staff, assets and property of certain forms of crime , theft of trade secrets, risk factors etc.

OBJECTIVES OF CORPORATE SECURITY

As objectives of corporate security can be determined: preventive action to eliminate all risks; reduction of threatening effects to a minimum extent; Business operation in crisis and overcome the crisis and again normal operations. For all this to happen, it is necessary normative, organizational and functional consistent security system that will enable safer and more efficient protection of people, property and operations of the corporation.

Other objectives of corporate security; Repair productivity and boost competitiveness, security risks can be reduced to the lowest possible level and to prepare measures to be taken if incidents occur, dangers and damages; The investment of business organization in security systems should be treated as an increase in the total value of the organization, aimed at increasing productivity and continuity of business processes. Apart from normal duties, corporate security must be included in the process of introducing new technologies to be able to predict safety risks and to propose measures that would reduce the risks to a minimum.[84] (Except technical and corporate security, and represents a strategic issue).

VALUES OF CORPORATION

Key values of the corporation are: Reputation of the company in the market, its corporate image (reputation), morale and motivation of employees; The strategic development plans; Analyze competition.

[84] Taken from Bakreski, O., Trivan D. Mitrevski, S., Corporate security system Skopje, 2012, p.85. Broader see: Campbell. GK: Measures and Metrics in Corporate Security, CSO 06 2006; Brennan, J. Walker, S., Security Careers / Defining Jobs, Compensation, Qualifications (indicated in: Veich Tomislav, "Corporate Security" Post no. 3/2007, Zagreb 2007, p. 38).

Corporate image of the company and its reputation in the market is of decisive influence on the survival and development of the corporation. One of the most important activities, when it comes to building and
Preserving the corporate image certainly is assessing the quality of products participating in individual events.[85] Corporations as business entities with better reputations have a competitive advantage over smaller companies or lack good reputation. According to some authors, Better reputation brings profit, protects the corporation during the crisis and prevent it's becoming involved in political disputes in society.

THE SYSTEM FOR SECURING PEOPLE AND PROPERTY IN THE COMPANY – AN IMPORTANT COMPONENT FOR EFFECTIVE BUSINESS OPERATIONS OF THE CORPORATION

In this part of the paper, the author determines the tasks of corporate security and the forms through which the activities regarding the provision of persons and property in the companies in the field of physical security, technical security and the safety and security component of the security are realized.
Corporate security tasks are to be observed and at an early stage effectively prevent any development of threats that endanger the corporation and its operations. Thus understood corporate security covers: Works for the physical and technical protection of the company (Out-Source/Proprietary), Works for administrative security (Administrative Security), Property security and external partnerships (Personnel Security); Personal Security (Protective Security); Fire Safety; Contingency Planning; Information Security; Executive Security; Security of various business events (Event Security); Security of agreed works with state structures; Investigations - Criminal Protection Program and Security Education and Training Program for Education, Development of Intellectual Property, Commodity Measures, etc.
In contemporary global conditions, an important component in achieving an efficient business operation of the corporation is the provision of persons and property in the company. The business of the company is the daily active relationship and work process, aimed at achieving a better and stable position of the company on the market and increasing its assets.
The company's security system for persons and property is one of the security system subsystems. Content, this system covers a range of measures and activities aimed at achieving physical and technical security and safety-protective component in order to prevent criminal activities and other forms, forms of threats to persons and property of enterprises, eliminate possible consequences (removal of possible consequences) and detection of possible perpetrators of criminal offenses, in order to more effectively protect the vital values and successful operations of corporations. The system for securing persons and property in the company is the engagement of the physical component by applying a technical component and

[85] Taken from Bakreski, O., Trivan D. Mitrevski, S., Corporate security system Skopje, 2012, p.107. Broader see: Bentele GÜnther, FrÖhlich Romy, Szyszka Peter, *Hand-buch der Public Relations: Wissenschaftliche Grundlagen und berufliches Handeln,* Verlag fÜr Sozialwissenschaften, Wiesbaden 2005, S. 604-605.

applying modern methods, methods and organization of work (security-protection component) in order to prevent or remediate the occurrence of threats to persons and property of enterprises, from damage or unauthorized appropriation of property of enterprises.[86] It is about subsystems of physical, technical, fire and other security and protection (protection of work, protection of the environment), as well as safety-protective component. So, it is a complex system, constructed from multiple subsystems that have special power, resources, methods, organization, etc.
The basic goals of the system for providing people and property are safe and better working conditions, by providing and protecting the values of the company, in order to achieve a better position of the company on the market and increase profits. The system for providing persons and property in the companies includes a number of normative, operational, information and educational and educational activities and measures that determine and establishes: organization of performance of works from physical and technical security, functioning of the services and the system for physical- technical security; personnel composition of the service for physical and technical security; equipment with necessary means and equipment; training and professional training of workers for physical and technical security for work, etc. Physical security is usually organized in the form of physical security officers (managerial staff and direct executors) consisting of a number of officers possessing weapons and equipment, whose task is to provide the company with all its values and interests. Accordingly, physical protection is the protection of people and property of enterprises from destruction, damage, appropriation and other forms of action dangerous or harmful to the health of people and property of the enterprise.

The physical security can be divided into 4 groups:[87]

- protection of persons and property;
- transport of money and other values;
- Protecting persons (bodyguard - bodyguard) and
- Providing public gatherings.

It is obvious that the grouping of things itself indicates the complexity of this content of the security and its place in the overall security system.
The extension of the activities of physical security, especially refers to the activities related to the transportation of money, protection of persons and provision of public gatherings. Securing is an integral part of the company's regular activities. The manner in which the immediate physical and technical security of persons and property is organized depends on many factors, and above all, the material possibilities, the number of objects that are kept, the nature of the work, and the like. Technical security and protection of persons and property means security provided by means of technical means and devices whose type, purpose, quality and application are determined by special regulations. Technical security is mechanical

[86] Taken from: Daničić, M., Security of people and property companies in Republic of Serbia, Higher School of Interior, Banja Luka, 2005, pp. 15, 16.
[87] Daničiќ, M., & Stajiќ, Lj., Private security, Higher School of Interior, Banja Luka., 2008, p. 29.

and electronic protection of persons and property and it implies an organizational arrangement within the security services in those enterprises in which it is organized.[88]

Technical security is provided in the area of premises or facilities that are provided, that is, during monitoring and security during transportation of persons who are provided directly, then during transportation of money, securities, precious metals and other values upon request interested parties.[89]

Accordingly, technical security is the protection and prevention of unauthorized access to a person or object, documents, funds, etc. using technical means and equipment. His appearance is understandable in the era of technical and technological achievements and, of course, contributes to achieving the efficiency of the security system. However, this does not mean reducing the role of physical security. Man manages the technical means of protection, and at the moment of occurrence of the danger or the conditions for its occurrence, activates and takes measures to prevent or eliminate hazards.[90]

The assets and equipment used for the provision of technical security may be mechanical, electronic or combined. Mechanical means are various types of fences, ramps, special construction structures, safes, vaults and the like. The various types and forms of so-called systems of electronic devices and equipment provide the following: permanent supervision over the security facility from one place, cost-effective engagement of security workers, reconstruction of events, detection of unauthorized persons or illicit state, attaining the psychological effect in preventive sense, provision of control over the work of the security service, control of the introduction of explosive, ionizing and other dangerous substances, quick detection of burglary and sabotage devices, fires and more.[91]

The security-protection component of security, functionally connects the previous two components of the security system, and provides new content that highlights the whole system of providing persons and property of companies to a higher level. This type of protection is directed at the human being as an important factor in any security system and its relations with the internal and external environment and encompasses protection of the property and business operations of companies, including organization and legal regulation. The security-protection component in the broader sense is security-protection management as a way of organizing and managing the system for securing persons and property, while in a narrower sense it is a component of the security system in companies that covers the protection of the property and the overall operation of the company, an adequate organization of the company's operations in terms of protection and its legal regulation.

Subject to the interest of the security-protection component are: subjects of security, sources and forms of threats, method of employing new workers, prevention-prevention of violence at the workplace, proactive and reactive measures for protection of persons and property, culture and communication (including the rules of business ethics with a segment of protection), information protection and information systems, security procedures, intellectual property protection, training of managerial staff and all employees, mandatory check of creditworthiness - the

[88] Ibid, p. 8, 14
[89] Ibid, p. 26, 27.
[90] Daničiќ, M., & Stajiќ, Lj., (2008). *Private security*, Higher School of Interior, Banja Luka., p. 27.
[91] Daničiќ, M., & Stajiќ, Lj., (2008). *Private security*, Higher School of Interior, Banja Luka., p. 27.

benefit, protection of the name and the protection sign of the company. In particular, it is considered that the safety-protective component includes: a culture of business protection (rules of business etiquette with segments of protection); protection of information; protection of intellectual property; protection of the name and trademark of the company; mandatory solvency check; training managers for securing the company and the personal system of business information.[92]

Current findings show that in practice the most common is physical and technical security, while the safety-protective component, which provides new contents of the security system, is practically neglected. Namely, the methods of work of the police and the forms of cooperation with the security system, which were applied in the previous period, are applied today, depending on the source and the forms of threats, the type of company and the degree of endangerment of the stated values of the company. Of course, it is also necessary to take into account the diversity of the property with which the company operates and its importance for the economic development of the country.

The basic prerequisite for the functioning of the system of protection or the system for securing persons and property in the company and the fulfillment of its ultimate purpose - dedicated to profit through efficient protection of persons, property and business operations is, of course, the awareness (opinion, understanding) of management in the company, as well as the consciousness of the owner of the capital for the necessity of existence and functioning of the protection system. This awareness is basically conditioned by specific benefits that the company or the owner can have from the protection system. These benefits are noted in the reduction or elimination of criminal activities, in a safe working environment (both for employees and clients), reducing the cost of removing the consequences, preserving the equipment, goods and assets for work of diminished value, theft and destruction. These benefits are noted in the reduction or elimination of criminal activities, in a safe working environment (both for employees and clients), reducing the cost of removing the consequences, preserving the equipment, goods and assets for work of diminished value, theft and destruction.

CONCLUSION

Corporate security is without doubt a concept that takes care of matters related to security companies and which simply defined as the protection of property and business processes which could have been the prevention and reduction of material losses for the security interests of the owners, profits and property from various hazards, risks and threats. Corporate security is an integral part of the process that manages business risks within the business entity. Specifically speaking, corporate security working to establish plans and implement measures aimed at: protecting the recipient, protection of employees in the business organization, protection of property owned by business organizations, protection of information and the reputation of the business organization of material damages , criminal activities etc..

The system for providing persons and property, i.e. the realization of physical and technical security and safety-protective component, is aimed at preventing criminal activities and other forms, forms of threats to persons and property of enterprises,

[92] Ibid, p. 31

eliminating possible consequences (removal of eventual consequences) and detection of possible perpetrators of criminal offenses, in order to more effectively protect the vital values and successful operations of corporations.
The system for providing persons and property should provide safe and better working conditions, protection of the property and employees in the company, securing and protecting the goals and values of the company in order to achieve a better position of the company on the market and increase profits.
For the efficient business operation of the corporation, security management needs to monitor the external and internal causes of crisis occurring in the corporation: External causes (general market changes, changes in industry, global economic crisis, political changes, legislative changes, natural disasters); Inner causes (inadequate and unusual management, incompetence, immoral leadership, underestimation of public opinion and subordinate, unrealistic goals and demands of trade unions, inefficient communication system, weak organizational culture, dissatisfaction and incompetence of employees, absence of control of employees, inadequate organization work, hardship for jobs).

.

REFERENCES

1. Bakreski, O., Trivan, D., Mitrevski, S., *Corporate security system*, Skopje, 2012.
2. Gerginova, T., *Corporate security,* Publisher Faculty of security – Skopje, 2017.
3. Daničiќ, M., Stajiќ, Lj., *Private security*, Higher School of Interior, Banja Luka, 2008.
4. Danichikj, Milan., *Security of people and property companies in Republic of Serbia* , Banja Luka 2005.
5. Ivandić, Vidović., Darius, Karlović., Lydia, Ostojić, Allen., *Corporate Security*, Association of Croatian managers of security - UHMS, Zagreb, 2011.
6. Markovich Slobodan I., *Fundamentals of corporate and industrial security*, Faculty of Legal and Business Studies, Novi Sad, 2007.
7. Markovich Slobodan I., *Corporative and Corporate Security,* USEE, Faculty of Legal and Business Studies "Dr Lazar Vrkatić", Novi Sad, 2013.
8. Markovich Slobodan I., *Philosophy of Corporate Security,* original scientific paper UDC 316.42 351.74/.75.
9. Milosevik, M., "*The concept and content of corporate security*", in Scientific Conference "Days of security" on the theme: "Corporate security - the risks, threats and protection measures" (Proceedings), Faculty of Safety and Protection of University Synergy, Banja Luka, 2010.
10. Stajić, Lj., The legal framework for private security, Proceedings, Faculty of Law in Novi Sad, no. 1-2 / 2008, p. 383.

Проф. д-р Љупчо Сотироски
Европски Универзитет Република Македонија
Ljupco.sotiroski@eurm.edu.mk

CYBER SECURITY PROTECTION AND IMPLEMENTING OF LEGAL FRAMEWORK

Abstract

This paper aims to present important elements which have a strong impact on the level of cooperation, confidence as well as awareness of subjects involved in the public and private environment that share the need and necessity for the corporative security protection of critical infrastructure.
With the development of information and other technologies, the society has become increasingly complex and vulnerable. The globe faces a high-risks, especially when is concerning the Cyber threats and consequences.
The complexity of the corporate security process identifies and implements all necessary legal measures to manage security risks.
The Cyber threats are directed toward access to, infiltration of, manipulation of or impairment to the integrity, confidentially, security or availability of data, an applications or systems without lawful authority.
The needs of Cyber protection by law are more than necessary. The globalization of the world, and thus indirectly of corporative security, poses serious dilemmas for the modern society about how to continue basing its development on the fundamental requirements related to the free movement of goods, services and people, and directly about how to keep cyber threats at an acceptable risk level.
The crime, facilitated by the network and computer technologies, has become cybercrime, the war, in turn has turned cyber. Cybercrime, cyber war and cyber terrorism are among the emerging phenomena that law needs to accommodate.
The effective legal regulation presumes creation of the viable policy that can adequately address the substance of the problem and the technical complexity on various levels, including legislative interventions in the form of criminalization and harmonization, international cooperation, collaboration with the private sector, professional educational and capacity building in terms of technical support and assistance.
Many countries, especially developing countries, do not have 6criminal laws that specifically address cybercrime. Neither do they have adequate capacity to enforce the laws. The developing countries still have a legal gap in terms of cyber threats and their prevention.
Risks of cyber manifest on various levels, as national as well as international.
Collectively, these concerns are describes by the common umbrella concept of cyber security. The legal framework and adequate regulations and implementation are a necessary tool to protect Cyber threats.

Key words: corporative security, cyber security, regulations, cyber threats, cybercrime, protection, implementation

1. CORPORATIVE SECURITY PROTECTION - INTRODUCTION

Globalization has changed the structure and pace of corporate life, the saturation of traditional markets is taking companies to more risky places, the shift towards a knowledge economy is eroding the importance of 'place' in the business world, new business practices such as offshoring challenge companies to manage at a distance, and new forms of accountability, such as corporate governance and corporate social responsibility, put added pressure on companies to match their words with deeds, wherever they are operating.

At the same time, security risks have become more complex, too. Many of the threats, such as terrorism, organized crime and information security, are asymmetric and networked, making them more difficult to manage.

There is also greater appreciation of the interdependence between a company's risk portfolio and the way it does business: certain types of behavior can enhance or undermine an organization's 'license to operate', and in some cases this can generate risks that would not otherwise exist.

As a result, security has a higher profile in the corporate world today than it did five years ago. Companies are looking for new ways to manage these risks and the portfolio of the security department has widened to include shared responsibility for things such as reputation, corporate governance and regulation, corporate social responsibility and information assurance.

1.1. Characteristics of alignment between Corporate security and the business

There are several characteristics of alignment between Corporative security and the business:

1. The principal role of the security department is to convince colleagues across the business to deliver security through their everyday actions and decisions – not try to do security to or for the company.
2. The security department is in the business of change management rather than enforcement and works through trusted social networks of influence.
3. Security is there to help the company to take risks rather than prevent them and should therefore be at the forefront of new business development.
4. Security constantly responds to new business concerns and, as such, the portfolio of responsibilities and their relative importance will change over time. Security departments should never stand still or become fixed entities. In many companies today, its role is more concerned with overall corporate resilience than 'traditional' security.
5. Security is both a strategic and operational activity and departments must distinguish between these two layers.

1.2. The power and legitimacy of roles

The power and legitimacy of the security department does not come from its expert knowledge, but from its business acumen, people skills, management ability and communication expertise.

Core elements of Corporate Security are the following: Personal security, Physical security, Information security, Corporate governance, Compliance and ethics programs, Crime prevention and detection, Fraud deterrence, Investigations, Risk management, Business continuity planning, Crisis management, Environment, Safety and health

For many years Corporate security has been dominated by a '*defensive' approach,* focused on protection and loss prevention.

The head of security was seen as little more than the 'guard at the gate', someone whose actions invariably stopped people doing their jobs instead of enabling the business to function more effectively. Typically, heads of security came from a narrow talent pool, namely police, armed forces or intelligence.

There are many reasons companies tend to recruit security managers from these backgrounds. The police and armed forces churn out individuals with intensive training in the practice of security and protection, and have hands-on experience that is rarely available elsewhere.

1.3. Number of reasons greater diversity

There are a number of reasons greater diversity is essential within the corporate security function as follows:

1. There is a growing recognition of the strategic importance of security and as a result security departments need to operate at a much more senior level.
2. Matrix organisations require a particular approach to management and leadership, which can be antithetical to those with police or armed services backgrounds.
3. In today's corporate environment, the impact of the security department is proportionate to its ability to persuade individuals and teams all over the company to collaborate and cooperate. This means that dialogue between security specialists and non-specialists is essential.
4. Traditional security skills are associated with an approach where security is perceived as a 'dis-enabler' of business.
5. There is a growing recognition of the value of 'the human element'. According to experts, many security professionals are typically trained to address.
6. Emotional intelligence is critical to effective alignment, but the human element of security and risk management is routinely overshadowed by the emphasis on technical security skills.
7. For security to be aligned with the business, security managers must understand the business and how they contribute towards its objectives.[93]
8. The Chief Security Officer (CSO) is the corporation's top executive who is responsible for security.
9. They direct staff in identifying, developing, implementing and maintaining security processes across the organization.

[93] DEMOS (2006)The Business of Resilience Corporate security for the 21st century, Rachel Briggs and Charlie Edwards

2. CYBER SECURITY THREATS CHALLENGES OPPORTUNITIES

It is only when they go wrong those machines reminding you how powerful they are.
Protecting that upon which we depend should be front of mind for government, business and industry, academia and every individual with a smartphone in their pocket.
Cyber security is developed throughout history, whenever new opportunities are created, there will always be those that exploit them for their own gain.
Despite the threat of viruses and malware almost since the dawn of computing, awareness of the security and sanctity of data with computer systems didn't gain traction until the explosive growth of the internet, whereby the exposure of so many machines on the web provided a veritable playground for hackers to test their skills, bringing down websites, stealing data, or committing fraud. It's something we now call cybercrime.[94] Since then, and with internet penetration globally at an estimated 3.4 billion users (*approximately 46% of the world's population2*), the opportunities for cybercrime have ballooned exponentially. Combating this is a multi-disciplinary affair that spans hardware and software through to policy and people, all of it aimed at both preventing cybercrime occurring in the first place, and minimizing its impact when it does. This is the practice of cyber security.

2.1. Threats in the information age and data manipulation

Every minute, we are seeing about half a million attack attempts that are happening in cyberspace.[95] The nature of threats Cybercrime comes in a variety of forms ranging from denial of service attacks on websites through to theft, blackmail, extortion, manipulation, and destruction. The tools are many and varied, and can include malware, ransom ware, spyware, social engineering, and even alterations to physical devices (for example, ATM skimmers). The biggest threats in Corporative cyber security today are around the large scale proliferation of targeted attacks from breach and email distribution of socially engineered ransom ware to potentially harmful attacks on critical infrastructure like energy networks.[96]

2.2. The future and 100% secure computer -Industry and the individual

Malware is still very popular and growing, but the past year has marked the beginnings of a significant shift toward new threats that are more difficult to detect, including file less attacks, exploits of remote shell and remote control protocols, encrypted infiltrations, and credential theft.[97]
Asia-Pacific is rapidly emerging as a potential market for cyber security solution providers, driven by emerging economies such as China, India and South-East Asian countries.[98]
It should be clear by now that we live in a world reliant on technology, and that this technology can also be vulnerable if it's not designed with security in mind. While some products and services are, many more are not, and to this end the

[94] Cyber security ,Threats Challenges Opportunities ACS, November 2016
[95] Derek Manky, Fortinet Global Security Strategist5 https://www.acs.org.au/content/dam/acs/acs-publications/ACS_Cybersecurity_Guide.pdf,
[96] Rodney Gedda, Senior Analyst, Telsyte,53,
[97] McAfee Labs 2016 Threats Predictions,15
[98] Estimated worth of the cybersecurity industry by 2023

development of cyber security tools, skills, and education is essential to protecting both our infrastructure and way of life.
When it comes to security nobody can never completely eliminate risk, there is only opportunity to minimise and mitigate it and there is no such thing as the 100% secure system. The adage goes that the only truly secure computer is locked in a lead box, buried fifty feet underground, sealed with concrete, with no wired or wireless connections in or out. Ultimately, for the majority of cases, security is about making the cost of entry higher than the value of the assets being protected.

2.3. Opportunity and challenges

The threats are many and varied, but so are the opportunities – technology constantly teases us with new ideas, new products, and new ways of living our lives. It also presents new economic opportunities, new ways of doing business, and new ways to make differences. Security I s as much about software as it is about awareness. It takes sophisticated coding to develop ransom ware, but only one click to activate it. [99]
Many of these devices are always on, always listening, and always communicating AND rising concerns about transparency and privacy. With homeowners unprepared and ill-equipped to detect and remediate most security threats, some highly successful attacks will collect personal info on an ongoing basis. [100] We're entering this world where everything is catalogued and everything is documented and companies and governments will be making decisions about you as an individual based on your data trail. If you want to be considered an individual and not just a data point, then it's in your interest to protect your privacy. [101]

3. LEGAL FRAMEWORK AND ADEQUATE REGULATIONS AND IMPLEMENTATION

There may be legal or regulatory limitations, particularly where the sharing of information could breach privacy laws. Where necessary, reviewing laws and regulations to facilitate better communication and collaboration for the purposes of corporative cyber security may be required.

3.1 The five pillars of cyber security readiness

As the peak body for ICT, the ACS considers the following to be the five core pillars of cyber security readiness.

1. **Education and Awareness-** First and foremost, it's essential that cyber security forms part of the conversation in every organisation, from the lunch room to the boardroom.
2. **Planning and Preparation-** A cyber security incident isn't an 'if' but a 'when', and to that end, preparation is essential.
3. **Detection and Recovery** -When a breach happens, the quicker it is detected and responded to, the greater the chance of minimizing loss – be it financial, reputational, or otherwise.

[99] Rodney Gedda, Senior Analyst, Telsyte 53
[100] McAfee Labs 2016 Threats Predictions15
[101] Josh Lifton, CEO of Crowd Supply 55

4. **Sharing and Collaboration -**As we've covered in this guide, collaboration is essential to mitigating current and future risks

5. **Ethics and Certification-** It may initially seem a less practical pillar, but the difference between a 'white hat' hacker and 'black hat' hacker is mindset

4. THE NEW LAW OF INFORMATION SECURITY

Most businesses are, or soon will be, subject to two key legal obligations:

- A duty to provide reasonable security for their corporate data and information systems
- A duty to disclose security breaches to those who may be adversely affected by such breaches.[102]

4.1. The Duty to Provide Security for Corporate Information

The legal issues surrounding information security are rooted in the fact that, in today's business environment, virtually all of a company's daily transactions, and all of its key records, are created, used, communicated, and stored in electronic form using networked computer technology.

Electronic communications have become the preferred way of doing business, and electronic records have become the primary means for storing information. As a consequence, most business entities are now "*fully dependent upon information technology and the information infrastructure*".[103]

Examples of some of the key sources of the duty to provide security that have been in place for several years include the following:

- Corporate governance legislation and caselaw designed to protect the company and its shareholders, investors, and business partners,
- Laws focused on the personal interests of individual employees, customers, or prospects
- Laws addressing governmental regulatory interests or evidentiary requirements

What Companies need to do?

The essence of the process-oriented approach to security compliance is implementation of a comprehensive written security program that includes:

- **Asset assessment** - identifying the systems and information that need to be protected,
- **Risk assessment**- conducting periodic assessments of the risks faced by the company,
- **Security measures**-developing and implementing security measures designed to manage and control the specific risks identified,
- **Address third parties**- overseeing third party service provider arrangements,
- **Education** - implementing security awareness training and education,
- **Monitoring and testing**- to ensure that the program is properly implemented and effective,

---

[102] What Companies Need to Do Now 1 Thomas J. Smedinghoff2

[103] 1515 National Strategy to Secure Cyberspace, February 14, 2003, at p. 6, available at www.whitehouse.gov/pcipb.

- **Reviewing and adjusting** -to revise the program in light of ongoing changes,
- **Categories of Security Measures**- to be addressed.

The companies are required to consider the following:

- Physical Facility and Device Security Controls,
- Physical Access Controls,
- Technical Access Controls,
- Intrusion Detection Procedures ,
- Employee Procedures ,
- System Modification Procedures,
- Data Integrity, Confidentiality and Storage,
- Data Destruction and Hardware and Media Disposal,
- Procedures regarding final disposition of information and/or hardware on which it resides,
- Audit Controls[104]
- Awareness, Training and Education
- Company actions[105]

Security breaches may be inevitable.

5. CYBER CRIME

Cybercrime, cyber war and cyber terrorism are among the emerging phenomena that law needs to accommodate to the great and serious consideration. Cyber security and Cybercrime are issues that can hardly be separated in an interconnected environment.

The fact that the 2010 UN General Assembly resolution on cybersecurity35 addresses cybercrime as one major challenge underlines this. Cybersecurity36 plays an important role in the ongoing development of information technology, as well as Internet services.

Enhancing cyber security and protecting critical information infrastructures are essential to each nation's security and economic well-being. [106]Making the Internet safer (and protecting Internet users) has become integral to the development of new services as well as government policy.

Deterring cybercrime is an integral component of a national cyber security and critical information infrastructure protection strategy. In particular, this includes the adoption of appropriate legislation against the misuse of ICTs for criminal or other purposes and activities intended to affect the integrity of national critical infrastructures.

At the *national level*, this is a shared responsibility requiring coordinated action related to prevention, preparation, response and recovery from incidents on the part

---

[104] 90 GLB Security Regulations, 12 C.F.R. Part 30 Appendix B, Part III.C;

[105] 126126 See generally, California Department of Consumer Affairs, Office of Privacy Protection, "Recommended Practices on Notification of Security Breach Involving Personal Information," October 10, 2003, available at www.privacy.ca.gov/recommendations/secbreach.pdf.

[106] Understanding cybercrime: Phenomena, challenge and legal response, Cybercrime, Printed in Switzerland Telecommunication Development Sector, ITU, September, 2012

of government authorities, the private sector and citizens. At the regional and international level, this entails cooperation and coordination with relevant partners.
The formulation and implementation of a national framework and strategy for cyber security thus requires a comprehensive approach.

5.1. Cyber security strategies

The development of technical protection systems or the education of users to prevent them from becoming victims of cybercrime – can help to reduce the risk of cybercrime. The development and support of cyber security strategies are a vital element in the fight against cybercrime. The legal, technical and institutional challenges posed by the issue of cyber security are global and far reaching, and can only be addressed through a coherent strategy taking into account the role of different stakeholders and existing initiatives, within a framework of international cooperation.

5.2. International dimensions of cybercrime

E-mails with illegal content often pass through a number of countries during the transfer from sender to recipient, or illegal content is stored outside the country. Within cybercrime investigations, close cooperation between the countries involved is very important. The existing mutual legal assistance agreements are based on formal, complex and often time-consuming procedures, and in addition often do not cover computer-specific investigations.
Setting up procedures for quick response to incidents, as well as requests for international cooperation, is therefore vital.
Consequences for developing countries
Finding response strategies and solutions to the threat of cybercrime is a major challenge, especially for developing countries. A comprehensive anti-cybercrime strategy generally contains technical protection measures, as well as legal instruments.
The development and implementation of these instruments need time. Technical protection measures are especially cost-intensive.
Developing countries need to integrate protection measures into the roll-out of the Internet from the beginning, as although this might initially raise the cost of Internet services, the long-term gains in avoiding the costs and damage inflicted by cybercrime are large and far outweigh any initial outlays on technical protection measures and network safeguards.
The risks associated with weak protection measures could in fact affect developing countries more intensely, due to their less strict safeguards and protection
The ability to protect customers, as well as firms, is a fundamental requirement not only for regular businesses, but also for online or Internet-based businesses. In the absence of Internet security, developing countries could encounter significant difficulties promoting e-business and participating in online service industries.
The development of technical measures to promote cyber security and proper cybercrime legislation is vital for both developed countries and developing countries. Compared with the costs of grafting safeguards and protection measures onto computer networks at a later date, it is likely that initial measures taken right

from the outset will be less expensive. Developing countries need to bring their ant cybercrime strategies into line with international standards from the outset.

5.3. Legal instruments

An increasing number of cybercrimes have an international dimension. As pointed out above, one reason behind this phenomenon is the fact that there is very little need for physical presence of the offender at the place where a service is offered.
Offenders do not therefore generally need to be present at the place where the victim is located. As there is no comprehensive international legal framework and no supranational body able to investigate such offences, transnational crimes require cooperation of authorities in the countries involved.
The mobility of offenders, the independence from presence of the offender and the impact of the offence make it necessary for law-enforcement and judicial authorities to collaborate and assist the state that has assumed jurisdiction.
Due to differences in national law and limited instruments, international cooperation is considered to be one of the major challenges of a globalization of crime.
This is relevant for traditional forms of transnational crimes as well as cybercrime. One of the key demands of investigators in transnational investigations is immediate reaction of their counterparts in the country where the offender is located. Especially when it comes to this issue, traditional instruments of international judicial cooperation in criminal law matters very often do not meet requirements in terms of the speed of investigations in the Internet.

5.4. Mechanisms for international cooperation

For cybercrime investigations, the most relevant formal mechanisms supporting international cooperation are mutual legal assistance and extradition. Other mechanisms such as transfer of prisoners, transfer of proceedings in criminal matters, confiscation of criminal proceeds and asset recovery are less important in practice. In addition to the formal mechanisms, there are informal ways of cooperation such as exchange of intelligence among law-enforcement agencies in different countries.

There are three main scenarios when it comes to identifying the applicable instrument for international cooperation.

1. First, relevant procedures can be part of international agreements, such as the United Nations Convention against Transnational Organized Crime (UNTOC) and its three protocols, or regional conventions, such as the Inter-American Convention on Mutual Assistance in Criminal Matters, the European Convention on Mutual Assistance in Criminal Matters and the Council of Europe Convention on Cybercrime.

2. The second possibility is for procedures to be regulated by bilateral agreements. Such agreements in general refer to specific requests that can be submitted and define the relevant procedures and forms of contact as well as the rights and obligations of the requesting and requested states.

3. The third is related to the International mechanisms.

United Nations Convention against Transnational Organized Crime

The main international instrument for judicial cooperation in criminal matters is the United Nations Convention against Transnational Organized Crime (UNTOC). This

convention contains important instruments for international cooperation, but was not specifically designed to address cybercrime related issues. Nor does it provide specific provisions dealing with urgent requests to preserve data.
Application of the United Nations Convention against Transnational Organized Crime
Based on Article 3, paragraph 1, the convention is only applicable in cybercrime cases if the offence involves an organized crime group. Article 2 of UNTOC defines an organized crime group as a structured group of three or more people.

5.5. Requests for Mutual legal assistance

The procedures for mutual legal assistance are defined in Art. 18. This provision contains a whole set of procedures.
Example: Article 18. Mutual legal assistance
Council of Europe Convention on Cybercrime
The Council of Europe Convention on Cybercrime (*the "Convention on Cybercrime")* addresses the increasing importance of international cooperation in Articles 23 to 35. General Principles for International Cooperation Article 23 of the Council of Europe Convention on Cybercrime defines three general principles regarding international cooperation in cybercrime investigations among members.

Extradition
The extradition of nationals remains one of the most difficult aspects of international cooperation. Requests for extradition very often lead to conflict between the need to protect the citizen and the need to support an ongoing investigation in a country abroad. Article 24 defines the principles of extradition.
*24/7 Network of contacts Cybercrime investigations often require immediate reaction***.**
As explained above, this is especially the case when it comes to the traffic data that are necessary to identify a suspect, as they are often deleted within a rather short period of time.
International Cooperation in the Stanford Draft International Convention
The drafters of the Stanford Draft International Convention (the "Stanford Draft") recognized the importance of the international dimension of cybercrime and the related challenges. In order to address these challenges, they incorporated specific provisions that deal with international cooperation.

5.6. General introduction

Committing a cybercrime automatically involves a number of people and businesses, even if the offender acts alone. Due to the structure of the Internet, the transmission of a simple e-mail requires the service of a number of providers. In addition to the e-mail provider, the transmission involves access providers as well as routers who forward the e-mail to the recipient. The situation is similar for the downloading of movies containing child pornography.
The downloading process involves the content provider who uploaded the pictures (for example on a website), the hosting provider who provided the storage media for the website, the routers who forwarded the files to the user, and finally the access provider who enabled the user to access the Internet.

- European Union Directive on Electronic Commerce

- European Union's E-Commerce Directive.
- Liability of Hosting Provider (European Union Directive).

6. CRIMINAL LAWS THAT SPECIFICALLY ADDRESS CYBERCRIME

Rising cybercrime suggests criminal law does not deter criminals and that a better legal solution is required to prevent further rises.[107]

Criminal sanctions for the conduct of cybercrime were updated in the Serious Crime Act 2015, which came into effect on 3 March 2015. Its provisions include amendments to the Computer Misuse Act 1990 to create criminal penalties of life imprisonment for unauthorized acts that cause serious damage to welfare or security, and 14 years' imprisonment for acts that cause serious damage to the economy or to the environment.
This is not the first time that laws relating to cybercrime have been amended. The Computer Misuse Act has been updated on at least 11 previous occasions over the past 25 years.
As a result, there are a broad range of sanctions available to deal with criminal activity, including unauthorized access to computer systems and unauthorized acts with the intent of disrupting the use of a computer system under the Computer Misuse Act, protection against cyber bullying under the Protection from Harassment Act 1997 and protection against the interception and disclosure of messages under the Wireless Telegraphy Act 2006.

The purpose of the criminal law is to punish and rehabilitate criminals and to deter others from offending, but, despite this, published reports, such as the *Ponemon Institute report on cyber-crime*, indicate that the number of attacks are continuing to increase. One deduction to be drawn from these reports is that the criminal law does not effectively deter criminals and that a better legal solution is required to prevent further rises.

Crime is generally perpetrated by people who feel comfortable with breaking the law, intentionally recklessly or, in some instances, merely in ignorance of the law and the criminal consequences of their acts. Ignoring crimes motivated by moral or religious fundamentalism and inter-state conflict, the anonymous nature of the internet, its lack of borders and the opportunity to industrialize the process of committing crime makes cybercrime an efficient, low-risk activity.
The pervasive use of technology further encourages its adoption.

The Serious Crime Act extends the international reach of the Computer Misuse Act to capture the activities of UK residents committing crimes abroad, and foreign nationals committing crimes within the UK. Enforcing these sanctions will not be so easy. It will rely on international conventions, such as the **Budapest Convention on Cybercrime 2001**, that provide for co-operation between member states and their national law enforcement agencies. However, the sanctions are typically

[107] Can legislation stop cybercrime? https://www.computerweekly.com/opinion/Can-legislation-stop-cyber-crimeStewart James

diluted by the need to achieve consensus between the participants, which reduces the impact of the convention.

7. LEGAL FRAMEWORK AND ADEQUATE REGULATIONS AND IMPLEMENTATION ARE A NECESSARY TOOL TO PROTECT CYBER THREATS[108]

With the development of information and network technologies and the growing interconnectedness of the world, the risks connected to online communication have become increasingly pressing. Due to the global nature of such communication unhindered by physical boundaries, network technologies challenge the existing international legal structure based on such notions as jurisdiction and sovereignty, where each sovereign jurisdiction regulates communication that takes place in its territory.

Online communication, that bypasses geographical and jurisdictional restraints, is a serious concern for the national and international legal orders in their current form. 14

7.1. Legal Problematic, Sovereignty and Jurisdictional Fragmentation

There are two main challenges that the global interconnectedness and its idiosyncratic features present for the legal systems tailored to regulate the 'real world' behavior. These are the problems that for the sake of convenience can be described as that of jurisdictionalfragmentation and that of the attribution of behavior

The following briefly introduces the two major legal problems of the legal regulation of conduct in cyberspace.

The problem of jurisdictional fragmentation follows from the fact that it does not and cannot agree with the global nature of cyberspace. Jurisdiction, inherently linked to the notion of state sovereignty, imposes an area of exclusive responsibility of a sovereign state over its territory and/or its citizens, thus excluding any extra-jurisdictional involvement of other states. The sovereign equality of states is protected by rules of customary public international law. No state, therefore, can claim sovereignty over cyberspace and thus introduce its effective regulation.

I. Attribution: Determining the Responsibility for Harmful Conduct

The legal effects of the conduct in cyberspace can be seen from the perspectives of various participants of online communication, the perspective of an individual (a criminal act, regulated by the national criminal law) and the perspective of a state (an act of aggression regulated by the international law). However, if the effects of the conduct are serious enough to entail consequences for the national security, such conduct can be seen in the dimension of cyber aggression and the international law.

[108] Legal Aspects of Cyber security, Arthur Appazov Faculty of Law University of Copenhagen 20

II. Cyber security as an Umbrella Concept

In general, the literature suggests to distinguishing between various types of cyber security concerns. It separates a basic cyber-attack into three general categories:

- cybercrime,
- cyberterrorism, and
- cyberwarfare.

Cyber espionage is another separate Cyber security concern connected to either state intelligence or such notion as activism. Dividing cyber security into manageable components facilitates the development of national and international law governing the rights and duties of individuals and nations with respect to each category of activity (*with the exception of espionage, there are no legal treaties that regulate espionage, separating cyber espionage as notion that falls outside the legal regulation*).

This approach can help address the shortcomings of present National and International legal frameworks in a more effective manner. 36

Hacking and Hacktivism

Early on in the age of the personal computer, many computer users performed '*hacks'*: legal or illegal computer manipulations (*e.g., access, defacement, redirects*) of computer systems/networks imbued with innovation, style, and technical virtuosity.85 Hacking activity today involves all types of cyber-attacks utilizing the whole range of cybercrime tools. In essence, hacking is an umbrella term that most commonly describes illegal or harmful cyber activity.

Cyber war and Cyber terrorism

Wars are fought within the context of their age with the weapons determined by the prevalent technology of the age. At that, concepts like electronic warfare, information warfare, network warfare, cyberwar and cyberterrorism have been offered to explain the emerging area of conflict. Unlike kinetic weaponry, such as weapons of mass destruction, that cause numerous casualties instantaneously, cyber warfare creates disruptive rather than destructive effects with no less serious consequences.

Criminalization

At the national level, both existing and new (or planned), cybercrime laws most often concern criminalization, indicating a predominant focus on establishing specialized offences for core cybercrime acts. Globally, many jurisdictions tend to perceive their criminal and procedural law frameworks to be sufficient, although this masks large regional differences. While many countries in Europe tend to consider their legislation sufficient, the picture is reversed in Africa, the Americas, Asia and Oceania, where more countries view laws as only partly sufficient or not sufficient at all.

Harmonization of Laws

Many countries have elements of the legal enabling environment addressing cybersecurity and cybercrime, but these national legal frameworks vary widely in terms of the manner in which these issues are addressed. In today's globalized

world, the law consists of a multitude of national, regional and international legal systems.

Interactions between these systems occur at multiple levels. As a result, provisions sometimes contradict each other, leading to collisions of law, or fail to overlap sufficiently, leaving jurisdictional gaps. These differences between national laws lead to the question of whether, and if so, how far, national legal differences in cybercrime laws can and should be reduced. In other words, how important is it to harmonize cybercrime laws? This can be undertaken in a number of ways, including through both binding and non-binding international or regional initiatives.

Incident Reporting and Information Sharing

Because of the difficulties arising when trying to define and identify cybercrime, nationally and cross-nationally comparative statistics on cybercrime are much rarer than for other crime types. The measures that might be wanting are those that would improve transparency through obliging individual and corporate victims, under certain circumstances, disclose data breaches.

Policy Considerations

A viable cyber security framework shall aim at the development of the adequate cyber security culture. Therefore it shall include national and international cooperative efforts to develop standards, methodologies, procedures, and processes that align policy comprising legislation, business, education and technology approaches to address cyber risks.Given the inclusive and comprehensive nature of the desirable policy framework, the private sector will naturally play as significant a role in the implementation of the policy as does the public sector. At that, the policy on cyber security and cybercrime shall be informed by the adequate understanding of the cyber-vulnerability threat on the part of the policy developer.

International Cooperation in Criminal Matters

The natural independent character of the network and information infrastructure and its growing importance for economies, public safety and our society in general makes controlling and countering potential threats a demanding and critical challenge for both governments and enterprises.

Many cybercrime acts involve a transnational dimension, engaging issues of transnational investigations, sovereignty, jurisdiction, extraterritorial evidence, and a requirement for international cooperation.

The issues of cooperation are of utmost importance for any effective regulation of globalized networked technologies. International best practice, if not international cooperation and collaboration, is more evident in the area of cybercrime, perhaps due in part to the near universality of the substantive provisions of the Budapest Convention.

Treaty-Based Approach to Cyber security and Cybercrime

The international community has a clear interest in developing a comprehensive, multilateral cyber security framework because the widespread use of the internet in every aspect of daily life has created an almost irreversible dependence on its technological benefits, and because the conceptual

underpinnings of existing legal frameworks are not readily adaptable to threats emerging in cyberspace

7.2. General Recommendations

There are two major areas that are in need of governmental attention at the moment:

1. development of comprehensive and clear policies on cyber security, and
2. development and adoption of relevant legislation supporting the policy that would enhance cyber security.

The considerations of the policy is of utmost importance and should include first and foremost long-term educational efforts on all levels of society including general education on cyber security matters, as well as professional education of law enforcement, judiciary and legislative authorities.

Also, an important component of a viable policy is promoting international discussion on the issues cyber security and its management on an international level. While international cooperation is necessary, each nation will have to develop, as a foundation, its own national cyber security strategy, authorities, and capabilities.

Within any given nation state, adequate cyber security will require effective coordination and cooperation among governmental entities on the national and sub-national levels as well as the private sector and civil society.

The questions arise in order to be into serious consideration:

- To what extent should cooperation of the private sector be legally compelled?
- What incentives or subsidies may promote cooperation?
- How far should governments go in regulating the private sector in the name of improving cyber security?
- What is the role of civil liability systems in addressing cyber-vulnerabilities?

As governments seek to develop their own national policies and structures for cybersecurity, questions include:

Which agency or ministry should have the lead?

- What should be the role of civilian agencies versus national security agencies?
- What should be the roles of law enforcement or national security agencies versus the roles of ministries for trade, commerce, or communications?

Nine years of legal vacuum in corporate security in the Republic of Macedonia disappear when the Macedonian Parliament passed the law that entrenched the private sector in this field.

8. MACEDONIAN LEGAL FRAMEWROK

The *"Security of property and personnel Act*" (also known as the "Act for Private security agencies") proclaimed the private security companies' actions as "*public interest actions*".

However, this as we have discussed above did not solve all of the problems. Beside mentality and inexperience public also was not ready to accept this radical shift.
Thus, regardless of costs and benefits of using private sector in the Republic of Macedonia by the law critical infrastructure is directly protected only by highly decentralized governmental institutions. Private security sector is only indirectly involved through providing physical security for the private commercial enterprises that own specific infrastructure.[109]
There is no legal document in Macedonia that contains summarized list of dedicated critical infrastructure. Instead, the network of laws regarding the CIP gravitate over the, Ministry of interior,
Ministry of defense, Ministry of transport and communication, Directorate for protection of classified information Crisis management center, Directorate for protection of classified information and Protection and rescue directorate.
Since there is no clear dedicated list of critical infrastructure further legal segmentation follows regarding the anticipated roles and service support for successful CIP. However, all of these documents include acts defining the responsibilities of the government authorities in case of emergencies as well as legislation dealing with issues (such as technical IT security for example).
International legislation further facilitates legal background for CIP in Macedonia. This is understandable since cyber-security and environmental protection are on the security agenda in most of the international organizations to whom Macedonia is party. One could observe this legislative in two directions.

1. First, obligations incorporated from Macedonian's membership of these organizations (or willingness to join). In this context further legislative support comes from the fact that almost all critical infrastructures rely on energy and telecommunications for support.
2. Second, most of the services that provide this support in Macedonia are owned or operated on a commercial basis (foreign private enterprises).

Consequently, all bilateral and multilateral agreements in this regards have to be considered.
Since these corporations in Macedonia run their security based on Macedonian private security agencies from legal point of view, one should also take into account the Act for security of property and personnel.
In sum, Macedonian legislation for CIP does not centralize responsibility only in one governmental authority. It consists of both, provisions that directly locate responsibility and the leading role of specific agency and provisions that imply responsibility (*regarding the bilateral business agreements and corporate security).*

The Macedonian legal system is consists of several legal documents that regulate the security protection, as follows:

- Security of property and personnel Act, following the Macedonian Constitution, in article 2 proclaims the private security agencies work as "public interest" 80/99.from 12. from1999.),
- Law on Internal Affairs" (The Official Gazette of R.M no.92/09),

- Law of Defense" (The Official Gazette of R.M no.8/92), and "Law for changes and addition of Law of Defense" (The Official Gazette of R.M no.5/03, 06 and 08),
- Law of Security in railway traffic" ("The Official Gazette of RM", No. 40/07),
- Law of transport of dangerous materials" ("The Official Gazette of RM", No. 92/07),
- Law of Security in railway system" ("The Official Gazette of RM", No.48/10),
- The law of public transportation in ground traffic ("The Official Gazette of RM", No.114/09, No. 83/10, No. 140/10),
- The law of Internal sailing ("The Official Gazette of RM", No. 55/07, No.26/09, No. 22/10),
- The law of electronic communications ("The Official Gazette of RM", No.14/07,
- No.55/07, No.98/08, No .83/10 No.48/10),
- The law of air traffic, ("The Official Gazette of RM", No.24/07, No.103/08, No.67/10)
- Law on Crisis Management" ("The Official Gazette of RM" No. 29/05)
- The law of classified information, ("The Official Gazette of RM", No.9/04)
- The Law on Rescue and Protection" ("Official Gazette of RM", No. 36/04),
- This include data protection, damage to data, fraudulent use of a compute, the handling of electronic signatures, etc.
- The law of classified information, ("The Official Gazette of RM", No.9/04).

Many International organizations are dealing with this challenge and have taken steps to raise awareness, establish international partnerships, and agree on common rules and practices.
European Union (EU), the Forum of Incident Response and Security Teams (FIRST), the G8 Group, NATO, the OECD, the United Nations (UN), and the World Bank Group.
Speaking in terms of Penal code act CIP's regulations have also preventive role. Nevertheless, it could be argued that legal basis for CIP in Macedonia more or less, draws the organizational structure of governmental authorities involved in this process.

9. CONCLUSION

The Cyber security protection and implementing of legal framework is extremely important issue.
The protection of modern information technology is an important factor for the stability of national and international relations and security in general. Appropriate legal protection is therefore needed**.**

The effective legal regulation presumes creation of the viable policy that can adequately address the substance of the problem and the technical complexity on various levels, including legislative interventions in the form of criminalization and harmonization, international cooperation, collaboration with the private sector, professional educational and capacity building in terms of technical support and assistance.

Many countries, especially developing countries, do not have 6criminal laws that specifically address cybercrime. Neither do they have adequate capacity to enforce the laws. The developing countries still have a legal gap in terms of cyber threats and their prevention.

Risks of cyber manifest on various levels, as national ас њелл ас international.

Collectively, these concerns are describes by the common umbrella concept of cyber security. The legal framework and adequate regulations and implementation are a necessary tool to protect Cyber threats.

10. SHORTCUTS AND IDIOMS

- **Cyberattack:** An offensive act against computer systems, networks, or infrastructure.
- **Cybercrime:** Computer-facilitated crimes, though frequently can be used to refer to all forms of technology-enabled crimes.
- **Cyberespionage:** The practice and theft of confidential information from an individual or organisation.
- **Cybersecurity:** The discipline and practice of preventing and mitigating attacks on computer systems and networks.
- **Cyberthreat:** A potential threat targeting computer systems and technology, typically from the internet.
- **Cyberwarfare:** Internet-based conflict to attack computer systems to disrupt or destroy. Usually in reference to nation states but can also refer to companies, terrorist or political groups, or activists.
- **DoS/DDoS:** Denial of Service/ Distributed Denial of Service. A common attack involving thousands of devices accessing a site simultaneously and continually to overload its ability to serve web pages.
- **Hacker/Hacking:**While originally in reference to a programmer 'hacking at code', it's now become mainstream to represent individuals who maliciously breach ('hack into') computers and related systems.
- **ICT:** Information and Communications Technology. Overarching term encompassing all forms of computing and telecommunications technology inclusive of hardware, software, and networks.
- **Internet of Things.** An evolving definition of the wide-variety of internet-connected devices ranging from sensors to smartphones.
- **Internet security:** A general term referring to the security of internet related technologies, such as web browsers, but also that of the underlying operating system or networks.
- **Malware:**Catch-all term to refer to any type of malicious software, typically used interference to viruses, ransom ware, spyware and similar.

- **Phishing:** Deceptive attempt, usually over email, to trick users into handing over personally identifiable or critical information (such as passwords or credit card numbers). A form of social engineering.
- **Ransomware:** Malware used to hold an individual or organisation to ransom, typically by encrypting files or an entire hard drive and demanding payment to 'unlock' the data. Also known as Crypto ware.
- **Social engineering:** The practice of manipulating human beings to gain access to data or computer systems.
- **Spear-phishing:** Highly-targeted form of phishing towards an individual or business, often utilising social engineering techniques to appear to be from a trusted source.
- **Spyware:** Covert software designed to steal data or monitor people and systems for cybercriminals, organisations, or nation states.
- **Threat actor:** an individual or entity that has the potential to impact, or has already impacted the security of an organisation.
- **White Hat:** Programmers who 'hack' into systems to test their capabilities, and report vulnerabilities to authorities to be fixed.

BIBLIOGRAPHY

- DEMOS,The Business of Resilience Corporate security for the 21st century, Rachel Briggs and Charlie Edwards, 2006,
- Cyber security, Threats Challenges Opportunities ACS, November 2016,
- Derek Manky, Fortinet Global Security Strategist5 https://www.acs.org.au/content/dam/acs/acspublications/ACS_Cybersecurity_Guide.pdf,
- Rodney Gedda, Senior Analyst, Telsyte, 53, 2016
- McAfee Labs Threats Predictions,15,2016,
- Estimated worth of the cyber security industry by 2023,
- Rodney Gedda, Senior Analyst, Telsyte 53
- Josh Lifton, CEO of Crowd Supply 55,
- What Companies Need to Do Now 1 Thomas J. Smedinghoff,,2
- National Strategy to Secure Cyberspace, February 14, 2003, at p. 6, available at www.whitehouse.gov/pcipb.
- GLB Security Regulations, 12 C.F.R. Part 30 Appendix B, Part III.C;
- California Department of Consumer Affairs, Office of Privacy Protection, "Recommended Practices on Notification of Security Breach Involving Personal Information," October 10, 2003, available at www.privacy.ca.gov/recommendations/secbreach.pdf.
- Can legislation stop cybercrime? https://www.computerweekly.com/opinion/Can-legislation-stop-cyber-crimeStewart James

Вонр.проф. д-р Елизабета Стамевска
Доц. д-р Васко Стамевски

УЛОГАТА НА КОРПОРАТИВНОТО УПРАВУВАЊЕ ВО СИСТЕМОТ НА КОРПОРАТИВНА БЕЗБЕДНОСТ НА КОМПАНИИТЕ

АБСТРАКТ

Во системот за на корпоративната безбедност корпоративното управување има голема улога и во зависност од поставеноста на корпоративното управување се поставуваат корпоративните цели, кои, најчесто се движат кон реализација на јасна организациска структура, со прецизно дефинирани права и одговорности на членовите на органите на надзор и управување и на другите вработени во компанијата. Целите се поставуваат и во насока на имплементирање на ефикасни процедури за идентификување, мерење, следење и контрола на ризиците на кои е изложена компанијата, понатаму, ефикасни механизми на внатрешна контрола, транспарентност во работењето на компанијата во однос на сите заинтересирани субјекти, во согласност со прописите и со деловната политика, како и воспоставување на системи за надзор и контрола.
Во согласност со поставеноста а во насока на зголемување на корпоративната безбедност, корпоративното управување, предлага, организира и спроведува, дизајнирање на стратегии за внатрешна безбеност и надворешна безбедност, корпоративна заштита на деловната успешност, деловни тајни, предлага превентивни мерки за спречување на можни кризни ситуации и предлог мерки нивно решавање итн.

Клучни зборови: Корпоративно управување, Корпоративна безбедност, кризни состојби, деловна тајна, стратегија

Prof. Dr. Elizabeta Stamevska
Assoc. Dr. Vasko Stamevski

THE ROLE OF CORPORATE GOVERNANCE IN THE COMPANY CORPORATE SECURITY SYSTEM

ABSTRACT

In the corporate security system, corporate governance plays a major role and, depending on the corporate governance set, corporate goals are set, which, most often, move towards the realization of a clear organizational structure, with precisely defined rights and responsibilities of the members of the supervisory and management bodies and other employees of the company. The goals are set in the direction of implementing efficient procedures for identifying, measuring, monitoring and controlling the risks to which the company is exposed, and further effective

internal control mechanisms, transparency in the operations of the company in relation to all stakeholders, in accordance with regulations and business policy, as well as the establishment of surveillance and control systems.
In accordance with the set up and in the direction of increasing corporate security, corporate governance proposes, organizes and implements, designs strategies for internal security and external security, corporate protection of business success, business secrets, proposes preventive measures to prevent possible crisis situations and proposal measures to solve them, etc.

Key words: corporate governance, corporate security, crisis, business secret, strategy

Улогата на корпоративното управување во системот на корпоративната безбедност на компаниите

Вовед

Корпоративното управување во современото општество, не може да финкционира, доколку, нема обезбедено соодветна заштита или механизам, преку кој, ризиците со кои се среќава при секојдневното работење, не се сведат на минимум. Оттука, и поставените цели на корпоратривното управување се во насока на имплементирање на ефикасни процедури за идентификување, мерење, следење и контрола на ризиците на кои е изложена компанијата, понатаму, ефикасни механизми на внатрешна контрола, транспарентност во работењето на компанијата во однос на сите заинтересирани субјекти, во согласност со прописите и со деловната политика, како и воспоставување на системи за надзор и контрола.

Корпоративната безбедност во смисла на сеопфатна заштита на стопанисувањето на стопанските субјекти – корпорациите, претставува, комплекесен систем од задачи, мерки и активности, преку кои треба ризикот да се сведе на минимално ниво. Заштитата на деловното работење од можни загрозувања од страна на надворешни и внатрешни фактори, е еден од основните приоритети на секоја корпорација.Успешен и ефикасно поставен систем на корпоративна заштита, ја штити корпорацијата од ризици и формира основа за донесување на важни деловни одлуки во насока на зголемување на нејзината успешност.

Корпоративно управување
Поим

Корпоративното управување ја опфаќа структурата, преку која се одредуваат целите на компанијата, а истовремено претставува и есенцијален елемент во подобрувањето на нивната економска ефикасност, раст, како и зголемување на довербата кај инвеститорите. Концептот на успешно корпоративно управување веќе подолго време сè повеќе станува преокупација на првите луѓе на компаниите. Компанијата, како човечка организација треба да биде

високо кооперативна, за успешно да се развива и да се оствари синергија меѓу нејзините составни делови.[110]

Некои дефиниции го ограничуваат значењето на корпоративното управување само на односите во самата компанија како и неговото значење за релевантната општествена рамка, а додека други автори се фокусираат на финансиските аспекти на корпоративното управување. Еден генерален заклучок е дека, под корпоративно управување се подразбира систем според којшто се управуваат и контролираат компаниите. Корпоративното управување вклучува сет на односи помеѓу менаџментот на компанијата, нејзиниот одбор, акционерите и другите засегнати лица. Корпоративното управување, исто така обезбедува организациона структура пред која што се утврдуваат целите на компанијата, а воедно се определуваат и начините за остварување на овие цели, како и следењето на префомансите на компанијата. Доброто корпоративно управување треба да обезбеди соодветни стимуланси за да се остварат целите што се во интерес на компанијата и акционерите и треба да го олесни ефикасниот мониторинг, со што ќе ги охрабри компаниите ефикасно да ги користат своите ресурси. Компаниите кои се посветени на воведување и примена на управувачки практики засновани на интегритет, практики кои се во интерес на сите засегнати лица, вклучувајки ги акционерите, вработени, клиентите, добавувачите, потенцијалните инвеститори и општествената средина во која компанијата ја врши својата дејност.

Корпоративни цели

Корпоративното управување претставува топ тема во светски размери, која што посебно доби на својата актуелност со избивањето на финансиските скандали и кризи, кои во последниве дваесет години попримија неочекувани размери. Актуелните случувања и отсуството на квалитетно корпоративно управување го потврдуваат неговото значење и важност за компаниите за целиот финансиски и економски систем, во поширока смисла.

Многу истражувања одат во прилог на поврзаноста меѓу управувањето и перформансите на компаниите, кои се во меѓусебна интеракција. Неспорно, доброто корпоративното управување позитивно влијание врз перформансите на фирмите.[111]

Органите на управување се мошне значајни чинители за решавање на проблемите поврзани со корпоративното управување. Составот на органите на управување, како персоналниот, така и бројниот, има многу силна рефлексија врз процесот на донесување одлуки. Особено, присуството на независни членови претставува катализатор на доброто корпоративно управување.

[110] Стамевска, Е.„Корпоративно управување“, Скопје, 2014, стр.18
[111] Belkhir, M., Board Structure, Ownership Structure, and Firm Performance: Evidence from Banking, EFMA, Madrid Meetings, 2006.

Доброто корпоративно управување значи можност за креирање на добри иницијативи од страна на работоводниот орган, во функција на ефикасно користење на човечките и останатите ресурси и следење и остварување на поставените цели. Оттука и системот на корпоративното управување во компаниите е насочен кон реализација на следниве корпоративни цели:

- Јасна организациска структура, со прецизно дефинирани права и одговорности на членовите на органите на надзор и управување и на другите вработени во компанијата;
- Ефикасни процедури за идентификување, мерење, следење и контрола на ризиците на кои е изложена компанијата;
- Ефикасни механизми на внатрешна контрола, кои, меѓу другото, вклучуваат детални административни и сметководствени процедури на компанијата;
- Транспарентност во работењето на компанијата во однос на сите заинтересирани субјекти, во согласност со прописите и со деловната политика;
- Системи за надзор и контрола.

Всушност, доброто корпоративно управување се јавува во улога на мултипликатор на кредибилитетот на компаниите, ја зголемува пристапноста до средствата за финансирање, ја намалува цената на капиталот и ги подобрува оперативните перформанси.[112]

Корпоративното управување ја опфаќа организацијата на вкупното работење на компанијата, на начин да се заштитат интересите и правата на сите негови партиципиенти, а најмногу на акционерите, преку користење на низа механизми. Тоа не е прашање на избор, туку се наметнува како обврска на деловните субјекти да го имплементираат во своето работење. Тоа не е активност која еднократно се одвива, туку е динамичен, жив и континуиран процес, кој може во голема мера да влијае на кризите кои се јавуваат во деловното работење на компаниите.

Кризите, било каде и да се појават, ретко доаѓаат сами и брзо се прошируваат. Повеќето видови на кризи не се поединечни настани, туку во најголемиот број случаи се појавуваат како комбинација од нив, што го прави идентификувањето на вистинскиот извор на кризата мошне тешко. Без оглед на правната рамка или сопственичката структура, секоја криза има негативен одраз на компаниите и претставува своевиден тест за системот на нивното корпоративно управување. Во кризни ситуации слабостите и судирите во компанијата многу појасно се покажуваат и оние кои не се подготвени се соочат со последиците од тоа стануваат казнети.[113]

Современиот концепт на работење во компаниите, во услови на пазарна економија, не може да се замисли без адекватен пристап и управување со ризикот, кој е основен предуслов за успешно работење на секоја компанија.

[112] Стамевска, Е.„Корпоративно управување“, Скопје, 2014, стр.169
[113] Исто, 174

Компаниите треба да обезбедат адекватно ниво на сопствени средства, во зависност од видот и обемот на финансиските активности и висината на ризиците, кои произлегуваат од извршувањето на активностите. Со општи акти и интерни процедури, тие треба да ги пропишат критериумите, начинот и методите на управување со ризици, како и оценката на адекватноста на капиталот, согласно со степенот на ризичност.

Стратегија за управување со ризиците

Управувањето со ризиците треба да се заснова врз стратегијата за управување со ризици. Главните цели на стратегијата за управување се насочени кон:

- Воспоставување мапа на ризици, која ќе ги идентификува сите значајни ризици со кои се соочува компанијата, за да помогне во остварувањето на стратегијата, преку проактивно управување со нив;
- Рангирање на сите ризици, од аспект на веројатноста на случување и очекуваното влијание на компанијата;
- Дефинирање на јасни улоги, одговорности и надлежности за управување со ризиците;
- Обезбедување усогласеност со најдобрите практики на корпоративно управување, овозможувајќи во годишниот финансиски извештај да се објави соодветна информација за процесот на управување со ризиците. Како дополнување потребно е финансиските извештаи да вклучуваат и резиме на процесот за ревизија за ефективноста на системот на внатрешна контрола;
- Подигање на свеста за принципите и бенефициите, кои произлегуваат од процесот за управување со ризиците и обезбедување посветеност на вработените кон принципите за контрола на ризиците.

За да се направи да се управува со ризиците , потребно е да се дрфинира поимот ризик а потоа и да се направи проценка на ризиците. Отука, одредени автори сметаат дека ризик претставува „ситуација во која постиои можност за отстапување во однос на посакуваниот резултат“ [114], а за други ризик претставува „комплексна особина со која се опишува веројатност од настанување на штетни последици и очекувана големина на последици од тие настани за сиот систем и за време на утврдената должина на временскиот интервал или за време на одредена мисија“.[115] Сепак, може да се заокружи дека ризикот не е ништо друго, освен, неможност да се предвиди резултатот од некои идни настани и случувања со висок процент на сигурност.

[114] Vaugan Emmet, Risk Menagement, John Wiley &Sons, Inc, New York, 1996 p.23

[115] Вукичевиќ, Д. Видовиќ, Д., „Могучности оптимизације улагања у превентиву и интерес осигурувајучих комапнија за та улагања“, Превентивно инжињерство, год III , Превинг, Београд 1996, стр. 5

Бенефиции од стратегијата за управување со ризиците

Доколку процесот на управување со ризиците е ефикасно испланиран и спроведен, согласно спецификите на компанијата, придобивките се повеќекратни, а се однесуваат на:

- Постоење на свест за различното влијание на определени ризици, при планирањето за користење на ресурсите во компанијата;
- Согледување на потребата од респонзивност и лоцирање на одговорноста;
- Олеснување на процесот на стартешко и оперативно планирање и донесување одлуки;
- Помош при идентификација на нови развојни можности;
- Повисок степен на консензуалност во донесувањето на стратешките одлуки од страна на органите на компанијата.

Сепак, имајќи ја предвид разликата меѓу компаниите, од аспект на нивната големина и комплексност, потребен е адекватен пристап, во кој ќе се понудат повеќе опции, достапни на компаниите, во зависност од нивните потреби и подготвеноста за инвестирање во пософистицирани системи за проценка на ризикот, бидејќи секако не е можно да се примени рамка, која би била идентична и подеднакво ефикасна и применлива за сите нив. [116]

Корпоративна безбедност
Поим, цели и задачи

Широк е поимот на корпоративната безбедност и неговото дефинирање е тема за дебатирање на безбедносната теорија и практика, при што, присутни се голем број суштински разлики во поимното определување на овој облик на безбедсност а со самото тоа и во поглед на нејзината содржина. Голем е бројот на дефиниции и толкувања за определени сфаќања во оваа сфера, но сепак може да се заклучи дека еден репрезентативен број на автори содржините на корпоративната безбедност некогаш во целост ги изедначуваат со содржините на приватната безбедност. Во таа смисла карактеристична дефиницијата е според која „приватната (корпоративна) безбедност е планска, организирана и врз основа на закон формирана самостојна или заедничка дејност и функција на организациите, приватни и(ли) професионални агенции, насочени кон сопствена заштита или заштита на други, како и заштита на соодветни лица, простори, објекти, работењаили дејности, а кои не се покриени со ексклузивна заштита од страна на државните органи".[117] Корпоративната безбедност е нов концепт во областа на безбедноста кој се грижи за работите поврзани со безбедноста во компаниите и којшто едноставно го дефинираат како заштита на имотот и работењето на компаниите

[116] Елизабета С., Корпоративно управување, Скопје, 2014, стр.252 - 254
[117] Стаиќ, Љ.„Правна рамка на приватната безбедност„ Зборник на трудови на Правниот факултет во Нови Сад, бр. 1-2/2008, стр.383

Гледајќи ги изнесените размислувања и ставови на голем број автори за корпоративната безбедност може да се заклучи дека има недостаток од конзистентна и воедначена дефиниција за овој поим, што го прави дефинирањето на овој термин е исклучително тешко. Општиот впечаток е дека полето на корпоративната безбедност е доста значајно и суштинско во работата на самата корпорација.

Самиот поим на корпоративната безбедност не може да се изедначува со поимот приватно обезбедување и неговите сегменти, туку е посебен сегмент на безбедноста [118] и претставува дејност што ја сочинуваат збир на мерки, постапки и активности кои се преземаат со цел за идентификување на ризикот и негово менаџирање, превентивно дејствување и заштита од ризикот, менаџирање со последиците од ризиците, зголемување на отпорноста на претпријатијата и обезбедување на нивен опстанок и успех.[119]

Во утврдувањето и дефинирањето на целите, задачите, принципите и критериумите за корпоративна безбедност во одредена компанија, покрај клучната улога на врвниот менаџмент на корпорацијата, влијание има и опкружувањето на компанијата, што ја доведува во врска функцијата на целта на планирањето на корпоративната безбедност, и работата на менаџерите за безбедност кои изработуваатсоодветни планови на корпорацијата. На тој начин се воспоставува системска врска помеѓу функцијата на секторот за безбедност во корпорацијата и нејзиното опкружување, што укажува на нужноста од постоење на системски пристап при изработката на плановите во корпоративната безбедност. Во таа смисла, како цели на корпоративната безбедност можат да се одредат:

- превентивно дејствување насочено кон елиминација на сите ризици;
- загрозувачките фактори кои можат да влијаат на деловните активности и остварување деловен успех на корпорацијата; сведување на загрозувачките дејства на најмала можна мера;
- деловно функционирање во услови на криза, како и надминување на кризата и повторно нормално работење.

За сето да се тоа оствари, потребно е да се воспостави нормативно, организациски и функционален конзистентен систем на безбедност кој ќе овозможи посигурна и поефикасна заштита на лицата, имотот и работењето на корпорацијата.

---

[118]Според насоките од Европската унија, корпоративна безбедност во корпорациите се дефинира како интегрална безбедност, која во себе опфаќа работи од безбедноста и заштитата , што пак вклучува собирање на информации, безбедносни процени и процени на ризик, информатичка заштита, кризен менаџмент, заштита од пожари, експлозии и хаварии, заштита на безбедноста и здравјето на работа и друго (види повеќе: Бакрески, О. и др. „Корпорациски безбедносен систем“, Скопје 2012 стр. 50)

[119]Повеќе кај: Gerald L. Kovacich & Edward Halibozek The Manager's Handbook for Corporate Security: Establishing and Managing a Successful Assets Protection Program Hardcover ISBN-13: 978-0750674874

Функции на корпоративната безбедност

Корпоративната безбедност во континутет е интегрирана сите постоечки процеси на корпоративното управување, така што, таа ги штити и овозможува нормалното одвивање на сите процеси во самата корпорација. Таа преку своето функционирање ги отстранува сите новосоздадени безбедносни проблеми и на вработените им создава безбедносни услови за работа. Оттука, корпоративната безбедност работи на создавање планови и спроведување мерки чија цел е: заштита на корисникот науслуги, заштита на вработените во деловната организација, заштита на имотот во сопственост на деловните организации, заштита на информациите и на репутацијата на деловната организација од материјални штети, криминални дејности итн. Со тоа корпорацискатa безбедност е составен дел на процесот со кој се управуваат деловните ризици внатре во деловниот субјект.[120]

Во насока на дообјаснување на поимит и фукциите на корпоративната безбедност современите европски држави направиле сопствен концепт на корпоративна безбедност при што неговите функции опфаќаат: административна безбедност (процедури и политика во областа на информатичката заштита); физичка и техничка безбедност (машини, постројки и објекти); безбедност на имотот и надворешни партнерства и лична безбедност (заштита на лица и заштита при работа); заштита од пожари; работа во вонредни ситуации; информатичка безбедност; безбедност на менаџерот; безбедност на различни деловни случувања и настани; безбедност на договорени работи со државни структури; истраги (програма за заштита од криминалитет); програма за едукација и развој на безбедносната култура на вработените идр.

Сите параметри кои се однесуваат на корпоративната безбедност, што по правило треба да биде канализирана преку посебна организациската единица за корпоративна безбедност, која ќе се занимава со неколку основни дејности. За почеток нејзината активност ќе се однесува на собирање информации и процена на ризикот, при што, нејзината активност ќе биде собирање на релевантни информации од областа на безбедноста и заштитата, чие што влијание ќе се рефлектира врз безбедноста и заштитата и врз основа на тоа ќе биде изработена проценка на ризикот. Понатаму оваа организациона единица треба да подготвува и организира заштита при вонредни состојби кои моќат да го загрозат функционирањето на корпорацијата, при што, подготвува и реализира превентивни мерки и планови са спречување на тие можни ситуации.

Исто така, овие единици имаат задача да подготваат планови и елаборати за обезбедување и заштита на виталните интереси и ги спроведува истите. Како една од клучните активности на корпоративната безбедност е превенирањето на кризини состојби и поединечни инциденти како и адекватната реакција за решавање на истите. Овде посебно место зема анализа на информациите и

[120] Бакрески, О. и др. „Корпорациски безбедносен систем“, Скопје 2012 стр. 117

координирање на активностите со лицата во организацијата и во државните институции за да се предвидат можните напади врз организацијата, односно како да се направат превентивните процедури. Од друга страна таа мора да посвети максимално внимание за враќање на организацијата во нормална работна состојба по инцидентни и акцидентни состојби, во координасција со сите надлежни институиции и органи. [121]

Заклучок

Корпоративното управување, во рамките на својата поставеност а во насока на зголемување на корпоративната безбедност, предлага, организира и спроведува, дизајнирање на стратегии за внатрешна безбеност и надворешна безбедност, корпоративна заштита на деловната успешност, деловни тајни, предлага превентивни мерки за спречување на можни кризни ситуации и предлог мерки нивно решавање итн.

Како основна задача на корпоративната безбедност е создавање клима, преку која сите членови на компанијата – корпорацијата, ќе дадат придонес кон корпоративното обезбедување преку секојдневните активности. Корпоративната безбедност е таа која ќе му обезбеди на препријатието, да преземе ризик и да се носи со тој рзик, а не да го одвраќа од него, што ја класифицира на правата линија во отворање на нови бизниси.

Безбедноста постојано се менува и еволуира, затоа портфолиото на активностио кои корпоративната безбедност ќе ги има, ќе се менува и адаптира и таа за разлика од класичниот пристап на безбедност во компаниите, како основна цел ја има резилиентноста на претпријатито - корпорацијата.

Исто така, корпоративната безбеднот се прелева преку стратешкиот и оперативниот дел на компанијата за разлика од различните оддели, кои може да припаѓаат или во стратешкиот или во оперативниот дел од корпорацијата.

Треба да се спомене и фактот што самата моќ на корпоративната безбедност не извира од знењето исклучиво на безбедноста. Таа извира од капацитетот на корпоративното управување да ја разбере, логиката на бизнисот, вештините да се прилагодат на потребите, динамиките на пазарот во контекст на фирмата, како и способноста за менаџирање и комуникација, сето тоа во контекст на корпоративната бебзедност.

Соодветен систем на корпоративно управување треба да има сеопфатен пристап и знаење, како да ги процени динамиките на пазарот, политичкото и безбедносно опкружување, сопствените и капацитетите на конкуренцијатаа и во огласност со тоа да организира континуитет на бизнис процесот. Овие пристапи и знаења се основни детерминанти за тоа, како и на кој начин корпоративното управување ќе ги планира мерките и активностите, кои се

[121] Повеќе кај: Veic T.,, Korporativna sigurnost", Posta, glediste, II br. 3 Zagreb, 2007, str. 41 - 42

однесуваат на ефикасно функционирање на системот на корпоративна безбедност.

Библиографија

1. Belkhir, M., Board Structure, Ownership Structure, and Firm Performance: Evidence from Banking, EFMA, Madrid Meetings, 2006.
2. Бакрески, О. и др. „Корпорациски безбедносен систем“, Скопје, 2012
3. L. Kovacich & Edward Halibozek The Manager's Handbook for Corporate Security: Establishing and Managing a Successful Assets Protection Program Hardcover ISBN-13: 978-0750674874
4. Стамевска, Е.„Корпоративно управување“, Скопје, 2014
5. Стаиќ, Љ.„Правна рамка на приватната безбедност„ Зборник на трудови на Правниот факултет во Нови Сад, бр. 1-2/2008
6. Veic T.,, Korporativna sigurnost”, Posta, glediste, II br. 3 Zagreb, 2007
7. Vaugan Emmet, Risk Menagement, John Wiley &Sons, Inc, New York, 1996
8. Вукичевиќ, Д. Видовиќ, Д., „Могучности оптимизације улагања у превентиву и интерес осигурувајучих комапнија за та улагања“, Превентивно инжињерство, год III , Превинг, Београд 1996

Aleksandar Nacev PhD
Executive Director
Center for Security Research

POLICIES AND PROCEDURES FOR INDUSTRIAL SECURITY

Abstract

The term industrial security means the provision of security procedures and measures required to achieve the relevant levels of protection of classified information exchanged between the state and companies. It involves the introduction of a security system which effectively prevents the unauthorised disclosure, destruction, misappropriation, modification or any other misuse of classified information, equipment, facilities, or any kind of property the state wishes to protect. Industrial security is a multidisciplinary area integrating elements of personal, physical, technical, documentation and IT security. In order to achieve a relevant level of protection of classified information, organisational, administrative and other procedures are required to provide for comprehensive and integrated security. In its broader sense, industrial security can also be understood as the ability of the state to strike an adequate balance between protecting its own economic, political and security interests and, at the same time, promote economic growth.

Key words: classified information, industrial security, contracts, facility security clearance, MISWG

Introduction

Due to the fact that it is just developed recently it is hard to find the appropriate definition of industrial security in literature. The closest one we could find are on the Internet and it is described as the portion of internal security which refers to the protection of industrial installations, resources, utilities, materials, and classified information essential to protection from loss or damage[122]. In its narrowest sense, the term industrial security means the provision of security procedures and measures required to achieve the relevant levels of protection of classified information exchanged between the state and companies. It involves the introduction of a security system which effectively prevents the unauthorised disclosure, destruction, misappropriation, modification or any other misuse of classified information, equipment, facilities, or any kind of property the state wishes to protect. Industrial security is a multidisciplinary area integrating elements of personal, physical, technical, documentation and IT security. In order to achieve a relevant level of protection of classified information, organisational, administrative

[122] Classified information is any information determined to require protection against unauthorized access or use and which has been so designated by a security classification. - Law on Classified Information (Official Gazette of the Republic of Macedonia, no. 9/2004), Article 5

and other procedures are required to provide for comprehensive and integrated security. In its broader sense, industrial security can also be understood as the ability of the state to strike an adequate balance between protecting its own economic, political and security interests and, at the same time, promote economic growth.

Facility security clearances

A company may be given access to classified information owned by the state if it obtains appropriate facility security clearance. The request for the facility security clearance shall have attached the following papers:

- application for entering the commercial register;
- court decision for registration;
- paper containing the name and seat of the founder and the total amount of the capital of the founder and each of the investors;
- power of attorney of the subject for registering in the legal transactions;
- names of the persons authorized for representation and the extent of their authority, and for the foreigners also the papers subscribed in the Law on Companies;
-report and opinion on the business success ("bonitée") issued by the Central Registry;
-confirmation from a relevant court that bankruptcy proceedings or liquidation procedure has not been opened;
-confirmation from a relevant court that no security measure for prohibition from practicing a profession has been delivered; and
-certificate from the Public Revenue Authority for paid taxes and other public allowances[123].

Facility security clearance means an administrative determination that a company fulfils the conditions for the safe handling of classified information of the lowest classification level up to the same classification level as the clearance being granted. To meet the minimum security standards, the following measures and activities must be met:

- Protection from misplacing or compromising of classified information contained in industrial agreements. The legal entity will have to establish a security system within the facility where the contract is to be executed. In case of noticed security risk, the competent bodies and persons shall immediately be informed in order to take measures to prevent the risk and to remove the possible negative consequences;

- Issuing of security clearances to legal entities and natural persons that produce, use or have contact with industry related classified information. Before taking part in the contract, the persons involved as lawyers, experts, consultants or in a similar capacity, which will use classified information, need to have a relevant personnel

[123] Decree on Industrial security of classified information, 07.03.2005, Republic of Macedonia, article 12

security clearance (PSC) commensurate to the classification level of the information used in the contracts;

- Protection from misplacing or compromising of classified information in consortia and mixed enterprises with foreign legal entities and natural persons;

- Ensure protection during transportation of classified information. Transportation of classified information outside the security zones, from one building to another or abroad, shall be carried out by transporters that meet the legal requirements for this type of transportation. This is done to ensure the security of classified information at all stages during the transportation and under all circumstances from the point of origin to the ultimate destination; and

- Establishing procedures for visits of legal entities and natural persons from other countries to facilities and industrial associations where classified material is produced, processed and kept. These visits shall be accomplished on the basis of the obligations stemming from the agreements and upon an invitation by the competent authorities and visitors shall be given access only to the classified information and materials related to the purpose of the visit.

When taking measures and activities for industrial security, particular attention shall be paid to:

- the level of classification;

- the scope and shape of the classification level; and

- the threat assessment for the security of classified information and materials[124].

A company in possession of facility security clearance also has an opportunity to sign commercial contracts with companies from other countries, the implementation of which requires access to classified information; the precondition is, however, that state has signed a security agreement with the country in question and that the agreement is in force. Bilateral cooperation and interstate agreements on the mutual protection of classified information are among the most important tasks of the national security authority. It is also important to encourage companies to acquire facility security clearances.

By being granted such clearances for access to foreign classified information, companies may also get the opportunity to participate in international tenders, meaning both those from foreign countries and international organisations (i.e. NATO). Owing to the constantly changing global security environment, industrial security has become one of the most rapidly developing and intensive areas of operation and cooperation between national security authorities; it is also an area in which every change can be observed immediately. Flexibility and the adaptability of everyone involved are therefore two extremely important elements. The competent authorities at the national and international levels have entered into various forms of

[124] Decree on Industrial security of classified information, 07.03.2005, Republic of Macedonia, article 1

cooperation in order to coordinate their activities, resolve open issues and adopt guidelines relating to industrial security.

Important tool for every state to encourage the companies to gain facility security clearance and to promote the security standards in the economic sector is the so called industrial security manual. It is a ready and simple reference which tells managers in the companies what they must know about state government security standards and procedures and how to ensure that their organization meets these security requirements. Usually the industrial security manual prescribes the procedures to be applied by state-based organizations, for the safeguarding of government information and assets, provided to or produced by private organizations. Procedures are also provided for the same activities related to allied foreign governments.

National and international solutions concerning the industrial security

At the national level, the appreciated solution could be in the establishment of Inter-Ministerial Project Group for Industrial Security, which could consists of representatives from different governmental entities who are involved in the industrial security process. The main tasks of such group could be to introduce uniform procedures and applicable standards to be used by every authority issuing facility security clearances to organisations, to examine and submit proposals for solutions in new critical situations related to industrial security and to prepare annual reports on industrial security. The Inter-Ministerial Project Group may also establish a subgroup to deal with more specific areas within its tasks; the subgroup shall be obliged to report to the inter-ministerial project group.

At the international level, the most important authorities are the European Union and NATO working committees and bodies developing security policies in this area, and the Multinational Industrial Security Working Group (MISWG). The group was established in 1985 in response to the finding that the applicable incompatible security requirements of the individual states in the area of industrial cooperation had become an impediment. The MISWG meets once a year at closed meetings attended by senior industrial security officials from all of NATO countries (with the exception of Iceland), Australia, Finland, Israel, New Zealand, Sweden and Switzerland, and representatives of Macedonia, NATO and the European Commission who have observer status. The MISWG's decisions are adopted in the form of legally non-binding documents, which means that member states decide whether to transpose them into their national legislation. When joining the MISWG, states nevertheless informally undertake to comply with its decisions to the greatest extent possible. Viewed together with the number of countries participating in the MISWG, this represents an important indicator of the global industrial security trends; the MISWG documents also provide an important basis for drafting binding international regulations and national laws, facilitate their swift drafting and adoption and diminish bureaucratic barriers.

Conclusion

Today, specific knowledge is required for the identification of different types of threats and risk management. We also have to underline the importance of security training programmes in order to improve the level of protection of classified information and to encourage people to raise their security awareness. The programmes are intended for key management personnel and the persons responsible for security in companies which possess facility security clearances. The main purpose of the training is not only to strengthen ties between the state and the economic sector, which is crucial in the area of protection of classified information, but also to make the concept of protecting vital state interests more understandable to those entities that come across classified information in their working processes. The training participants should also be better aware of the need to protect their own knowledge, innovations and ideas. In this way, national security authority directly contributes to protecting the competitiveness of the economy, while indirectly also contributing to faster economic growth and development.

Bibliography

1. EU Council Decision 2001/264/EC – Security Regulations Of The Council Of The European Union, 19 March 2001
2. Multinational Industrial Security Working Group. MISWG Document Number 7, 1 November 2007 (Amended 1 March 2013)
3. NATO Security Committee AC/35-D/2002-REV3. NATO Security Committee Directive on the Security of Information, 06.12.2006
4. Pfeifer, W. Joseph. *Network Fusion: Information and Intelligence Sharing for a Networked World*, Homeland Security Affairs, Vol.8, US, 2012
5. Republic of Macedonia. Decree on Industrial security of classified information, 07.03.2005
6. Republic of Macedonia. Law on Classified Information (Official Gazette of the Republic of Macedonia, no. 9/2004)
7. Republic of Slovenia. Classified Information Act (official consolidated text) (ZTP-UPB2), (Official Gazette of the Republic of Slovenia, no. 87/01, 08. 11. 2001)
8. Republic of Slovenia. Decree on the method and procedure of assessing the conditions for issuing the facility security clearance, 19.07.2007

Mr Branka Mijić
Fakultet za kriminalistiku, kriminologiju i sigurnosne studije
Sarajevo, Bosna i Hercegovina

INFORMACIJSKI RAT

SAŽETAK

Informacijski rat (eng. Information Warfare - IW) je koncept koji uključuje korištenje i upravljanje informacijsko-komunikacijskim tehnologijama (ICT) u borbenom prostoru u postizanju konkurentske prednosti nad protivnicima. Informativni rat može uključivati prikupljanje taktičkih informacija, uvjerenje da su vlastiti podaci valjani, širenje propagande ili dezinformacije kako bi demoralizirali ili manipulirali neprijateljem i javnošću, potkopavajući kvalitetu suprotstavljene informacije o sili i uskraćivanju informacija - mogućnosti prikupljanja suprotstavljenim snagama. Informacijski rat je usko povezan s psihološkim ratovima.
Američki vojni fokus usredotočuje se na tehnologiju i stoga se širi u područja elektroničkog ratovanja, cyberwarfare, informacijskog osiguranja i operacija računalne mreže, napada i obrane. Većina ostatka svijeta koristi mnogo širi pojam „Informacijske operacije“ koji, iako se koriste tehnologijom, usredotočuju se na više aspekte korištenja informacija vezanih uz čovjeka, uključujući (između ostalog) analizu društvene mreže, analizu odluka i ljudskih aspekata zapovijedanja i kontrole.

Ovaj rad predstavljat će analizu informacijskih ratova u suvremenom dobu, kada je tehnološki razvoj na svom vrhuncu. U radu će biti obrađeni način informacijskog ratovanja, te mogućnosti zaštite od istog.

Ključne riječi: informacijski rat, informacijsko – komunikacijske tehnologije, propaganda, cyberwarfare.

SUMARY

Information Warfare (IW) is a concept that involves the use and management of information and communication technologies (ICT) in the combat space in achieving competitive advantage over opponents. The information war may include the gathering of tactical information, the conviction that their own data is valid, propaganda dissemination or disinformation, to demoralize or manipulate the enemy and the public, undermining the quality of the opposing information about force and deprivation of information-the possibility of collecting opposing forces. The information war is closely related to psychological wars.
The US military focus focuses on technology and is therefore expanding into areas of electronic warfare, cyberwarfare, information security and computer network operations, attacks and defenses. Most of the rest of the world uses a much wider concept of "Information Operations", though utilized by technology, focusing on multiple aspects of using human-related information, including (inter alia) social network analysis, decision-making and human aspects of command and control.

UVOD

Jedna od najčešćih pojava u razvoju ljudskog roda, gotovo kao njegova zakonitost, jeste rat. Odavno, a i danas je to očigledno, sporna pitanja između država, društvenih grupa i drugih organiziranih ljudskih zajednica, osim na bojnom polju, prenose se i rješavaju u drugim sferama: političkoj, medijskoj, naučnoj, kulturnoj, sportskoj, informativnoj, informatičkoj, ekonomskoj, sferi međunarodnog prava, komunikativnoj sferi, itd. Iako ciljevi i oblici sukoba ostaju isti, promjene se događaju proširenjem sfera i primjenom novih metoda i sredstava.

Jedna od karakteristika suvremenog rata jeste i disproporcija sukobljenih (zaraćenih) strana, u svim segmentima koje rat kao društvenu pojavu karakteriziraju, kao što su: ciljevi, snage (podrazumijeva se i sredstva), prostor, vrijeme, način vođenja operacija i sl. Neravnoteža snaga je, po pravilu, ono čemu se stremi u oružanim sukobima. Drugim riječima, to znači da se rat vodi između strana koje se veoma razlikuju po količini moći kojom raspolažu. Takvi ratovi nazivaju se i asimetričnim ratovima. Na jednoj strani je moć izražena u količini žive sile, borbenim sustavima sa njihovim borbenim i vatrenim mogućnostima, ekonomskim i privrednim potencijalima, kontroli medija za masovno komuniciranje, širokoj podršci (i u globalnim razmjerima), a, sa druge strane, ograničen broj ratnika (po pravilu bez uniforme) sa selektivnim izborom oružja i drugih sredstava, ali odlučnih u svojim namjerama.
Može se reći da će budući ratovi imati najmanje dvije forme: tradicionalnu, ali veoma usavršenu formu, koja se oslanja na visokoprecizno oružje, koje može da djeluje sa velike distance, uključujući i svemir, i formu rata koja se upravo rađa i koja će biti jedinstvena. Iako su danas još uvijek prisutne teškoće u sagledavanju skupa aktivnosti koje konstituiraju ovu novu formu rata i iako je teško sagledati i označiti sve aspekte ove forme budućeg ratovanja, sigurno je da će informaciona tehnologija oblikovati ovu formu, a da će bojište biti u domenu koji neki nazivaju cyber prostor, a drugi nacionalna informaciona struktura.

DEFINIRANJE INFORMACIJSKOG RATA

Tanka je nit između tradicionalnog rata i informacijskog (cyber) rata. Tradicionalni rat je uništavajući i pogibeljan po čitavu jednu sredinu u fizičkom smislu, dok je cyber rat više pogibeljan za određeni prostor u duhovnom smislu. Interesantno je što ovi ratovi počinju iznenada i završe, ali i ponovo se pokrenu i nitko ne zna kada bi mogao završiti. Informacijski rat (IW) je koncept koji uključuje korištenje i upravljanje informacijsko-komunikacijskim tehnologijama (ICT) u borbenom prostoru u postizanju konkurentske prednosti nad protivnicima, utječući na njegove informacije, procese koji se temelje na informacijama, informacijske sustave i na računalne mreže, dok se istodobno brane vlastite informacije, procesi i informacijski sustavi. Informativni rat može uključivati prikupljanje taktičkih informacija, uvjerenje da su vlastiti podaci valjani, širenje propagande ili dezinformacije kako bi demoralizirali ili manipulirali neprijateljem i javnošću, potkopavajući kvalitetu suprotstavljene informacije o sili i uskraćivanju informacija - mogućnosti prikupljanja

suprotstavljenim snagama. Informacijski rat je usko povezan s psihološkim ratovima.[125]
Inovacija naprednijih i autonomnih ICT-a potaknula je novu revoluciju u vojnim poslovima, koja obuhvaća uporabu ICT-a u cyber prostoru i fizičkom bojištu kako bi se borili protiv njihovih protivnika. Tri najčešća revolucija u vojnim poslovima dolaze u obliku kibernetičkih napada, autonomnih robota i upravljanja komunikacijom (Rid, 2007).

U području virtualnog prostora postoje dva primarna oružja: mrežni centrički rat i C4ISR, što označava integrirano zapovijedanje, kontrolu, komunikacije, računala, inteligencija, nadzor i izviđanje. Nadalje, napadi na cyber prostor koji je pokrenula jedna nacija protiv druge nacije imaju temeljni cilj dobivanja informacijske superiornosti nad napadnutom stranom, što uključuje narušavanje ili negiranje sposobnosti žrtve da prikuplja i distribuira informacije.
Stvarnu pojavu koja je ilustrirala opasni potencijal cyber napada tijekom 2007. godine, kada je napad izraelske snage srušio navodni nuklearni reaktor u Siriji koji se gradi putem suradnje između Sirije i Sjeverne Koreje. U pratnji napada bio je kibernetski napad na sirijsku zračnu obranu, što je Siriju ostavilo slijepom za obranu.
Primjer temeljitijeg napada na naciju unutar cyber prostora je napad DDOS (Distributed Denial of Service) koji se koristi za ometanje mreža ili web stranica dok ne izgube primarnu funkcionalnost.
Imamo primjer kibernetskog rata, takozvani Prvi mrežni rat (eng. Web War 1), u kojem su 2007. u Estoniji DDOS-om napadani serveri estonske vlade, ministarstava, medija, banaka i tvrtki, što je rezultiralo isključivanjem tih subjekata s Interneta na određeno vrijeme, te vrlo sličan ruski napad na servere kojim su se koristila brojna vladina tijela, mediji i poslovni subjekti Gruzije, a koji je tekao istovremeno s bojnim djelovanje ruskih snaga spram gruzijskih.[126]
Mada informacioni rat nije novina, zahvaljujući cayber tehnologijama on postaje jeftiniji, brži i efikasniji, teže ga je otkriti i lakše ga je negirati. Trenutno u svijetu imamo nekoliko cyber ratova, u većini imaju političku pozadinu.
Ako pogledamo rezultate, Ruski informacioni rat dijelom je bio uspješan, jer je na neki način uticao na američke izbor 2016.godine, ali je i propao ako ga promatramo iz ugla meke sile. Po rejtingu londonske kompanije Portland Consultancy, koja rangira 30 zemalja po snazi meke moći (Soft Power 30), Rusija zauzima 27. mjesto. Ruski informacioni rat je postao smetnja predsjedniku SAD jer je naglo smanjila meku silu Rusije u Americi. Postoji mišljene da je najbolji odgovor na “rijeke laži” najbolje ne pokušavati da se na tu laž odgovori, već da treba preventivno djelovati protiv samog procesa, a to pokazuje pobjeda Makrona. Također, postoje sumnje i o njenoj umiješanosti u hakerske napade na servere izbornog štaba predsjednika Francuske Makrona, to nas ne može čuditi ako se sjetimo kako predsjednik Putin (nepravilno) svata meku silu (meka sila, kompleks instrumenata i metoda za

[125] Primjerice, američki vojni fokus usredotočuje se na tehnologiju i stoga se širi u područja elektroničkog ratovanja, cyberwarfare, informacijskog osiguranja i operacija računalne mreže, napada i obrane. Većina ostatka svijeta koristi mnogo širi pojam "Informacijske operacije" koji, iako se koriste tehnologijom, usredotočuju se više na aspekte korištenja informacija vezanih uz čovjeka, uključujući (između mnogih drugih) analizu društvene mreže, analizu odluka i ljudskih aspekata zapovijedanja i kontrole.
[126] DDOS (eng. Distributed Denial-of-service) – napad kojim se sprječava pristup računalom sustavu koristeći preopterećivanje računalne mreže slanjem mnogostrukih zahtjeva prema poslužitelju, tako da se zaustavi legitimni promet prema tim poslužiteljima.

dostizanje spoljnopolitičkih ciljeva bez prijemne oružja, a na račun informacionih i drugih izvora djelovanja).
Kao što je implicirano, internetski napadi ne utječu samo na napad na vojnu stranku nego na cijelo stanovništvo te nacije. Budući da se više aspekata svakodnevnog života integrira u mreže u kibernetičkom prostoru, civilno stanovništvo može potencijalno negativno utjecati tijekom rata. Na primjer, ako je neka zemlja odlučila napasti druge mrežne poslužitelje električne energije na određenom području kako bi poremetila komunikaciju, civili i tvrtke u tom području također bi se morali nositi s prekidima napajanja, što bi moglo potencijalno dovesti do ekonomskih poremećaja.
Štoviše, fizičke ICT se također provode u najnoviju revoluciju u vojnim poslovima uvođenjem novih, autonomnijih robota (tj. - bespilotnih dronova) na bojno polje za obavljanje dužnosti poput patroliranja granica i napada ciljeva na zemlji. Ljudi s udaljenih lokacija pilotiraju mnoge bespilotne dronove, međutim, neki od naprednijih robota, kao što je Northrop Grumman X-47B, mogu samostalno odlučivati. Unatoč pilotiranju dronovima s udaljenih lokacija, dio pilota još uvijek pati od stresnih čimbenika tradicionalnijeg ratovanja.[127]
Suvremene ICT također su donijele napredak u upravljanju komunikacijom među vojnim snagama. Komunikacija je vitalni aspekt rata za bilo koju uključenu stranu, a provođenjem novih ICT-a kao što su uređaji s podacima, vojne snage sada mogu brže širiti informacije nego ikad prije. Na primjer, neke vojske sada koriste uporabu iPhona za prijenos podataka i informacija koje su prikupili dronovi na istom području.
Termin informativni rat u osnovi označava nedovoljno uobličen koncept suvremenog načina sukobljavanja u kome informacije postaju ključni resurs i predstavljaju glavno oružje koje suprotstavljene strane koriste za ostvarivanje premoći i pobjede u ratu, radi ostvarivanja konkretnih državnih interesa ili interesa nadnacionalnih vojno-političkih saveza. Pojedini stručnjaci smatraju da informativni rat obuhvata aktivnosti koje čine sadržaje medijskog, informatičkog i elektroničkog rata. Informativni rat ima široku primjenu na vojnom planu, ali se ispoljava i u oblasti ekonomije i politike (Volkov, 2001).
Polazeći od činjenice da u informativnom ratu informacija predstavlja strategijsko sredstvo, mogu se razlikovati tri vida ratovanja: borba za informaciju, zaštita informacije i rat putem informacije, što bi značilo: saznati, spriječiti drugog da dođe do saznanja i navesti druge da dođu do lažnog saznanja. U ovom trećem aspektu riječ je o dezinformaciji i utjecaju na mišljenje i stavove (Waltzm 1998).
Rat za informaciju zasniva se na iskorištavanju dostupnih informacija bez obzira na to da li potiču iz otvorenih ili povjerljivih izvora. To znači da se mogu koristiti podaci iz svih raspoloživih izvora – iz medija, štampanih i elektronskih, sa interneta, informacije prikupljene prisluškivanjem elektronskih emisija, kanala veze, upada u informacijski sustav protivnika, ali i dobivene klasičnim obavještajnim postupcima. Pri tom, veoma je bitno da dotok informacija bude stalan, što podrazumijeva i znatne ljudske i tehničke resurse, radi njihove uspješne obrade (Kurmon i Ribnikar, 2003).

Za informacijsko ratovanje, ne treba bojno polje, već se sve odvija u cyberspace-u. Na cyberspace može utjecati bilo koja grupa koja posjeduje računala koji se mogu

[127] Prema NPR-u, istraživanje provedeno od strane Pentagona u 2011. godini pokazalo je da je 29% pilota dronova podvrgnuto visokoj razini stresa. Nadalje, približno 17% pilota ispitanih u studiji također pokazuju znakove posttraumatskog stresnog poremećaja.

povezati u postojeće računalne mreže. Internetski napadi neke skupine mogu biti usmjereni na namjerno ubacivanje dezinformacija na neke internetske forume,enciklopedije, blogove i web stranice sličnog karaktera ili mogu biti strogo usmjereni prema mrežnoj sabotaži tj. internetskom terorizmu.

ORUŽJE INFORMACIJSKOG RATA

Prikupljanje i transport informacija

Prikupljanje informacija je ključni dio informacijskog ratovanja jer informacijska revolucija podrazumijeva uspon načina ratovanja u kojemu strana koja zna više uživa presudne prednosti. U današnje doba, razvoj tehnologije doveo je do različitih metoda upravljanja informacijama: prikupljanja, skladištenja, obrade, korištenja i razmjene informacija. Ideja je da što više informacija ima, to je veća njegova situacijska svijest, što dovodi do boljih planova bitaka i boljih ishoda. Nedavno je poznavanje položaja i prijateljskih snaga bio veliki zadatak. Preciznost pozicioniranja tehnologija kao što je navigacija temeljena na Global Positioning System (GPS) je uvelike ublažila te probleme. Poznavanje položaja neprijatelja također je omogućeno do stupnja zapošljavanja tehnologija upoznavanja i nadzora. Funkcije upoznavanja i nadzora kreću se prema korištenju senzora iz spektara poput infracrvenog, ultraljubičastog, mirisnog, auditivnog, vizualnog, seizmičkog, itd., i spajanju podataka iz njih da bi se formulirala cjelovita slika. U ratu s informacijama prikupljanje informacija je mnogo manje opasno i veoma kompletno jer se te tehnologije mogu koristiti za infiltriranje situacija i prikupljanje točnih informacija uz minimalan gubitak (Ventre, 2016).
U današnje doba više nije dovoljno biti informacijski stručnjak koji prikuplja, evaluira i diseminira informacije, nego treba biti informacijski strateg koji postavlja smjer strategije putem kojega se dolazi do cilja (Vojković, Štambuk-Sunjić 2006).
Prikupljanje velike količine sveobuhvatnih informacija svakako je dobra praksa, ali prikupljene informacije su malo vrijedne ako se informacije nalaze u skladištu, neiskorištene. Kao takav, sposobnost prijenosa informacija u ruke onih kojima je to potrebno pravodobno je još jedan bitan aspekt informacijskog ratovanja. Alati koji se koriste u ovoj oblasti nisu baš oružje, već civilne tehnologije korištene u vojnim situacijama. Najvažniji od tih alata su komunikacijska infrastruktura, sastavljena od mreža računala, usmjerivača, telefonskih linija, svjetlovodnih kabela, telefona, televizora, radija i drugih tehnologija i protokola prijenosa podataka. Bez tih tehnologija, sposobnost prijenosa informacija u stvarnom vremenu potrebnom današnjim standardima bila bi nemoguća (Ventre, 2016).
Iako je nešto izvan dosega ove rasprave, zanimljivo je u ovom trenutku uvesti pojam „mreža“ u vojnom vokabularu. Stotinama godina vojska se oslonila na hijerarhije, a ne mreže, za širenje informacija. Civilni napredak u komunikacijskoj tehnologiji uslijedio je, međutim, umrežene paradigme, što ima potencijal da ozbiljno promijeni način na koji se zapovijed i kontrola vrši u vojnim krugovima. Premještanje u umrežene strukture može zahtijevati decentralizaciju zapovijedanja i kontrole, ali decentralizacija je samo dio slike, a nova tehnologija može pružiti i veću vrhunsku sliku, središnje razumijevanje velike slike koja poboljšava upravljanje složenosti. Iz toga vidimo da čak i naizgled osnovna promjena u tehnologiji

prijenosa informacija ima potencijal da informacijsko ratno doba informacija bude drugačija od onoga što je to bilo prije.

Manipuliranje informacijama

Informacijska manipulacija u kontekstu informacijskog ratovanja je promjena informacija s namjerom narušavanja protivničke slike stvarnosti. To se može učiniti pomoću brojnih tehnologija, uključujući računalni softver za uređivanje teksta, grafike, video, audio i drugih oblika uređivanja informacija. Dizajn manipuliranih podataka obično se obavlja ručno, tako da zapovjednici imaju kontrolu nad onim što se prikazuje neprijatelju, no spomenute tehnologije obično se koriste za brži proces fizičke manipulacije nakon što se odlučuje o sadržaju.

Svrha informacijskog ratovanja je steći prednosti koje se mogu koristiti i za slučaju "vrućeg" sukoba, ali i u "hladnoj" fazi konfrontacije. Cilj je utjecati na svijest osobe i tako promijeniti njeno ponašanje, sustav vrijednosti, moral, a što je najvažnije - na sposobnost pružanja otpora. u procesu informacijskog ratovanja suprotna strana prikazuje u najcrnjem svjetlu, a vojni neprijatelj se dehumanizira. Koriste se mnoge neprovjerene statistike i reference koje ukazuju na "razmišljanje većine".

Neke se činjenice zanemaruju, dok se druge predstavljaju suprotno istini. "Curenje informacija" je izumljeno kako bi se dobila slika veće vjerodostojnosti. Koriste se mišljenja "stručnjaka" i poziva se na razne eksperte, jer u očima običnih gledatelja oni imaju "duboko znanje" o temi o kojoj se raspravlja.

Smetnje i degradacija informacija

Konačni aspekti informacijskog ratovanja, su poremećaj, degradacija i poricanje. Sve tri tehnike su sredstvo za isti opći cilj - sprečavanje neprijatelja da dobije potpune, točne informacije. Zbog sličnosti, mnoga su istog oružja korištena za postizanje jednog ili više ciljeva. Neka od popularnijih oružja korištenih za ovakve vrste informacijskog ratovanja su podvala, ometanje i preopterećenje.

Odbacivanje je tehnika koja se koristi za degradiranje kvalitete informacija koje se šalju neprijatelju. Neprijateljski tok informacija ometan je uvođenjem „varalice“ ili lažne poruke u taj tok. Tehnika funkcionira jer omogućuje da se pruže lažne informacije ciljanim sustavima prikupljanja konkurenata kako bi se ta organizacija potaknula na pogrešne odluke na temelju ove neispravne informacije (Ventre, 2016).

Drugi način je uvođenje buke u frekvenciju koju upotrebljavaju. Pozadinska buka otežava neprijatelju da odvoji stvarnu poruku od buke. Ovo je osobito korisna tehnika ako neprijatelj koristi oblike bežične komunikacije, budući da se te frekvencije mogu iskoristiti bez potrebe da se zapravo spoje u fizičku mrežu kabela.

Zastoj je tehnika koja se koristi i koja uključuje presretanje signala poslanih između dvije komunikacijske veze ili između senzora i veze. Signal je presrnut, zatim „zaglavljen“ ili zaustavljen od daljnjeg napretka prema namjenskom odredištu. U većini slučajeva isti je signal pohranjen od strane lovca kao obavještajne informacije i koristi se za utvrđivanje neprijateljskog gledanja na vlastiti položaj.

Konačno, preopterećenje je tehnika koja se koristi za odbijanje informacija neprijatelju u vojnim i civilnim okruženjima. Slanjem volumena podataka neprijateljskom komunikacijskom sustavu koji je prevelik da bi se mogao nositi,

jedan uzrokuje pad ili tešku degradaciju sposobnosti sustava da dostavi informacije. Sustav je toliko zauzet da se bavi preopterećenjem, nije u mogućnosti dostaviti bitne informacije onima kojima je to potrebno.

ZAŠTITA U INFORMACIJSKOM RATU

Zaštita od prikupljanja i prijenosa informacija

Dostupne protumjere za obranu od prikupljanja informacija su, dakle, ista oružja koja su ranije definirana za uporabu u zaštiti, smetnjama, degradacijama i napadima uskraćivanja. Naime, upotreba šifriranja, spoofinga, uvođenja buke, ometanja i preopterećenja osobito su korisna za zaštitu informacija od neprijatelja.
Budući da je informacijski transport u velikoj mjeri ovisan o infrastrukturi, najučinkovitija protumjera sprečavanja prijenosa je uništavanje neprijateljske infrastrukture. Ovaj protusmjer zahtijeva znanje kako komunicira druga strana. S tim znanjem, ova obrana može biti relativno jednostavna. Ako je neprijateljska arhitektura npr. žičana lako se identificira i onemogućava. Kao i zapovjedni centri, komunikacijski sustavi mogu biti oštećeni napadima na generatore, stanice i cjevovode za opskrbu gorivom. Ako je arhitektura elektromagnetna, često ključni čvorovi su vidljivi. Ako se sateliti koriste za prijenos i signalizaciju, tada komunikacijske linije mogu biti zaglavljene.

Zaštita informacija

Zaštita informacija, u suštini, predstavlja specifične mjere i postupke kojima se neovlaštena lica sprečavaju da pristupe informacijama, koje imaju izuzetan značaj za vojsku, obranu, ili državu uopće. Taj vid ratovanja oslanja se na sigurnost informativnih sistema, odnosno na funkcioniranje specijalnih ofanzivnih i defanzivnih uređaja. Također, podrazumijeva i informativne protumjere – primjenu tehnike namijenjene osobnoj zaštiti od mogućih manipulacija informacijama.
Jedan od najčešće dogovorenih aspekata informacijskog ratovanja je potreba da se minimizira količina informacija kojoj protivnik ima pristup. Veliki dio toga štiti informacije od druge strane. Oružje koje se koristi za zaštitu sigurnosti podataka spada u dvije klase. Prve su one tehnologije koje fizički štite vitalne podatke, računala i mehanizme transporta, uključujući bombe i metke za zaštitu od metaka i mehanizme za sprečavanje upada, poput bravica i skeniranja otiska prsta. Drugo, a možda i još važnije, su tehnologije koje sprečavaju neprijatelja. To svakako uključuje osnovne tehnologije računalne sigurnosti kao što su lozinke, kao i sofisticirane tehnologije poput enkripcije. Svrstavanjem vlastitih poruka i onih s druge strane, svaka strana provodi bitan čin informacijskog ratovanja, štiteći vlastiti pogled na stvarnost, a ponižavajući onu s druge strane (Ventre, 2011).
Kako bi se suprotstavili neprijateljskim pokušaji vlastitih informacija, mora se biti u mogućnosti da se zaokruže njihovi zaštitni mehanizmi. Nažalost, nedavna povećanja sofisticiranosti kriptografije učinila su zaštitu veoma teškom. Kombiniranje tehnologija kao što je trostruki digitalni šifrirani standard (DES) za komunikaciju poruka pomoću privatnih ključeva i šifriranje javnog ključa (PKE) za donošenje privatnih ključeva pomoću javnih ključeva vjerojatno će preplaviti najbolje računalo za enkripciju kodova. Ono što to znači za one koji se žele suprotstaviti zaštiti informacija jest da će njihovi napori naposljetku postati uzaludni.

Do tada, pokušaji prekidanja kodova pomoću snažnih računala najvjerojatnije će dati najbolje rezultate.

Zaštita od manipuliranja informacijama
Jednom kada neprijatelj ima informacije, malo tko može učiniti kako bi spriječio njihovo manipuliranje. U svjetlu toga, zaista postoje samo dvije protumjere koje se mogu koristiti za ove vrste napada. Prije svega, može se raditi na sprečavanju neprijatelja da presretne informacije. Tehnike za informacijsku zaštitu ovdje su najučinkovitije jer zadržavaju neprijatelja ili od pristupanja ili od razumijevanja informacije.
Drugi, a možda i ključni, način u obrani od manipuliranja podacima jest sprečavanje ponovnog uvođenja izmijenjenih podataka u tok stvarnih informacija. Srećom, postoji nekoliko tehnika za to, od kojih je najčešća redundancija. Prikupljanjem iste informacije iz višestrukih, redundantnih izvora, povećava vjerojatnost da će se dobiti točne informacije. Čak i ako je neprijatelj uspio pokvariti te podatke na jednoj komunikacijskoj liniji, lako će se otkriti loši podaci jer se razlikuju od slike koju oslikavaju ostali izvori.

Zaštita od smetnji i degradacije informacija
Obrana od poremećaja, degradacije i uskraćivanja informacija zahtijeva korištenje već spomenutih protumjera. Bilo koje oružje za ugradnju ove vrste napada zahtijeva pristup neprijateljskim komunikacijskim kanalima, tako mehanizmi za zaštitu informacija i suvišni kanali mogu biti učinkoviti u održavanju nekih linija komunikacije na koje ne utječu potencijalni napadači.

ZAKLJUČAK

Suvremene sukobe karakterizira primjena različitih ne oružanih modaliteta ratovanja. Brojnost koncepata sukoba u komunikativnoj sferi, ne oružanih formi ratovanja u odnosu na oblike primjene oružane sile u suvremenim sukobima, i stupanj učešća najviših vojnih rukovodilaca u njihovoj realizaciji, ukazuju na bitno izmijenjenu strukturu snaga upotrijebljenih u agresiji, te na totalitet i konstantnost suvremenih konflikata. U tim sukobima najčešće se može zapaziti disproporcija u snagama, informatičkoj opremljenosti i obučenosti sastava za primjenu modernih tehnologija u okviru ratnih aktivnosti.
Dakle, suvremeni razvoj informacionih tehnologija (zastupljenost računalne tehnologije u borbenim sustavima, kompleksnost suvremenih upravljačkih sustava, ovisnost drugih oblasti od informatičkih sredstava, osjetljivost informatičke infrastrukture i ovisnost vojne i ekonomske moći od informacijskog potencijala) bitno mijenja vojne sustave i koncepte operacija u osnovnom obliku. Naime, u suvremenim sukobima prevladavaju koncepti ratovanja zasnovani na informacijama, koji se realiziraju u sferi komunikacije (u oblastima medija, odnosa sa javnošću, informiranja, informativnog osiguranja, itd.).

S tim u vezi može se zaključiti da je došlo do porasta značaja informacija za uspjeh u ratu, povećanja stupnja utjecaja medija na formiranje javnog mišljenja i podrške za rješavanje spornih pitanja ratom, te značaja informatičke opremljenosti i obučenosti sastava oružanih snaga razvijenih zemalja za primjenu modernih tehnologija u sklopu ratnih aktivnosti.

LITERATURA

1. Kurmon, B. i Ribnikar, D. (2003). Asimetrični ratovi, sukobi juče i danas, terorizam i nove pretnje. Beograd: NIC „Vojska“.
2. Rid, T. (2007). War and Media Operations: The US Military and the Press from Vietnam to Iraq. London: Routledge (2007) (ISBN 0415416590).
3. Ventre, D. (2011). Cyberwar and Information Warfare. New York: Wiley.
4. Ventre, D. (2016). Information Warfare. New York: Wiley.
5. Volkov, V. (2001). Dezinformacija, od trojanskog konja do interneta. Beograd: Naš dom.
6. Waltz, E. (1998). Information Warfare Principles and Operations. Norwood: Artech House.

Časopisi:
1. Goran Vojković i Marija Štambuk-Sunjić s Pravnog fakulteta u Splitu u članku „Konvencija o kibernetičkom kriminalu i Kazneni zakon Republike Hrvatske“, Zbornik radova Pravnog fakulteta u Splitu, Vol.43 No.1, Split, 2006.

Др Роза Гурмешевић, доктор правних наука
(на Правном факултету Универзитета у Београду)
Email: rozagurmesevik@yahoo.com
Моб. тел: 070/967-544
Република Македонија

Људска права и неједнакости у условима дигитализације и експанзије интернета

Апстракт
У последњих неколико година сведоци смо неминовних промена у свету које су резултат економског, политичког и културног процеса глобализације и дигитализације. Све већа глобализација тржишта има своје позитивне и негативне стране. Најновијим економским, безбедносно-информационим и научно-технолошким достигнућима отварају се могућности за нове врсте пословања, комуникације, сарадње и размене; постављају се нови критеријуми и стандарди у организацијској структури компанија и проналазе се нова техничка и технолошка решења у складу са новонасталим условима. Ове промене захтевају учинковито, модерно и одлучно деловање у складу са новонасталим условима.
Промене изазване глобализацијским трендовима и дигитализацијом утичу и на заштиту и унапређење људских права у готово свим областима живота. Експанзијом информационих и комуникационих технологија долази до замагљивања границе између приватног и пословног живота и све веће неједнакости између радика са ниским приходима и оних који се налазе на врху лествице тржишта. У области рада и запошљавања извесна је поларизација тржишта, као и феномен „дигиталне дискриминације“, која укључује дискриминацију на основу расе, пола, узраста итд. Људска права у дигиталном добу исправљена су пред великим изазовима (нпр. право на приватност). Искуства говоре да модерне компаније, организације и институције имају значајне могућности за промоцију и унапређење људских права не само у пословном, већ и у приватном животу.

Кључне речи: дигитализација, неједнакост, људска права, право на приватност, дигитална дискриминација

Dr Roza Gurmešević, Doctor of the Science of Law
(at the Faculty of Law, University of Belgrade)
Email: rozagurmesevik@yahoo.com
Cell phone: 070/967-544
Republic of Macedonia

Human Rights and Inequalities in Terms of Digitization and Expansion of the Internet

Abstract
In recent years we have witnessed the inevitable changes in the world as a result of economic, political and cultural processes of globalization and digitization. The

increasing globalization of markets has its positive and negative sides. The latest economic, information security, scientific and technological developments open up opportunities for new types of business, communication, cooperation and exchange; set new criteria and standards in the organizational structure of the company and find new technical and technological solutions in accordance with the new conditions. These changes require an effective, modern and resolute action in line with global trends.
The changes caused by globalization trends and digitization affect the protection and promotion of human rights in almost all areas of life. Expansion of information and communication technologies leads to the blurring of boundaries between work and private life, and the growing inequality between workers with low incomes and those who are at the top of the market. In the field of labor and employment is a certain polarization of the market, as well as the phenomenon of „digital discrimination“, which includes discrimination based on race, sex, age etc. Human rights in the digital age are facing great challenges (e.g. the right to privacy). Experience shows that modern companies, organizations and institutions have significant opportunities for promotion and advancement of human rights not only in business but also in private life.

Key words: digitization, inequality, human rights, the right to privacy, digital discrimination

Глобализација и дигитализација и њихов утицај на концепт људских права

Глобализација и дигитализација су неизбежни процеси данашњице. Експанзијом ових процеса који са собом носе читав низ феномена у готово свим сферама друштва, као што су економска, политичка, технолошка, социјална или културна, неизбежне су промене како у економији и трговини појединих држава, тако и у читавом друштву, укључујући концепт заштите људских права. Наше политичке, социјалне и правне институције још увек нису у кораку са импликацијама транзиције која је резултат и одговор на дигитализацију и глобализацију друштва. Научно-технолошки развој и иновације у последње две деценије, посебно у облику персоналних рачунара и интернета, променили су концепт радних места у многим сферама живота (образовање, здравство, трговина, банкарство, ауто индустрија итд.), а у најбрже растућим економијама света довели су до побољшања ефикасности пословања и развоја нових индустрија заснованих на дигиталној технологији. Да би се таква дигитална интеграција постигла и у мање развијеним земљама, потребни су додатни напори за даљи развој како на националном и регионалном, тако и на европском и светском нивоу. То укључује свеобухватне реформе постојећег система, а нарочито реформе јавне администрације, дефинирање дигиталних стратегија и политика и усвајање свеобухватног законодавства које ће бити у стању да прати глобалне трендове и истовремено штити људска права. У том контексту, посебну важност у мање развијеним земљама заузима оспособљавање стручне радне снаге за рад у дигиталном добу и успостављање механизама и инструмената за успешно спровођење процеса дигитализације. Истраживања која се тичу

унапређења дигиталних вештина указују да је Европи потребно преко 300 милиона радних места у области информационих технологија. Према томе, дигитализација представља користан процес и предуслов за економски раст и развој иновативности у многим државама, а посебно у земљама западног Балкана. Њихова способност да користе савремене технологије и активни ангажман у процесу дигитализације може допринети борби против сиромаштва и незапослености, унапређењу положаја националних мањина (нпр. право на језик) и добросуседских односа, као и побољшању квалитета живота свих грађана. Чињеница је да се данас регион суочава са бројним изазовима који успоравају напредак у овој области (све више младих напушта регион, корупција, финансијски проблеми, повреда људских права итд.). Један од корака за њихово превазилажење је унапређење регионалне сарадње, јачање унутрашњег дигиталног тржишта и комуникација, као и развој руралних подручја и побољшање њихове повезаности. Имајући у виду да дигитализација доводи и до укидања појединих занимања и радних места, потребно је обезбедити поверење грађана и пословних субјеката, као и учинковито и свеобухватно разумевање овог процеса.

Дигитализација је уско повезана са глобализацијом. Захваљујући развоју науке, технологије, демократије, тржишне економије, убрзању саобраћајних средстава и информатичке револуције многе земље, а нарочито у Европи након Другог светског рата, су започеле процес међусобног побезивања, трговинске размене и умножавања међуљудских односа како би превазишле потешкоће људског друштва. И сам концепт људских права је у том контексту превазишао националне и културне границе. Исход тог процеса је етаблирање нових институција и скретање пажње на већ постојеће међународне институције (Уједињене нације, Међународна организација рада, Светска здравствена организација, Европска заједница за угљен и челик, Европска економска зајединца, касније Европска унија). Зато нас не чуди када многи теоретичари корене глобализације проналазе у Европи, иако се сам појам глобализације значајније појављује тек шездесетих година 20. века. Данас се о глобализацији увелико говори са различитих аспеката: економског, политичко-правног, културног итд. То нам говори да је у питању комплексан појам који укључујчуе готово све врсте људских активности (економске, политичке, технолошке, психолошке, социјалне, културне), као и идеје, норме и обичаје ван државних граница. Имајући у виду такав опсег деловања, једни глобализацију критикују, док је други фаворизују. Заговорници сматрају да глобализација подразумева напредак земље јер иста покреће раст и економију. Стога, да би поједине земље осетиле благодете глобализације оне морају исту прихватити. С друге стране, критичари сматрају да глобализација не утиче подједнако на све људе јер је довела до повећања јаза између богатих и сиромашних и више људи који живе у крајњем сиромаштву, искључености и социјалној неједнакости. Другим речима, они сматрају да глобализација фаворизује само богате државе.

Незаобилазна тема дебате о глобализацији и дигитализацији са правно-политичког аспекта су људска права. Будући да се друштво данас суочава са дубоким, готово тектонским, променама изазваним брзим ширењем дигиталне комуникационе инфраструктуре и технологије, заштита људских права у 21. веку ће зависити од способности држава да јасно утврде како ће примењивати

трајне принципе људских права у дигиталном контексту. Дигиталном технологијом дошло је до трансформације средстава којима се истовремено остварују и крше људска права. Многи теоретичари сматрају да је интернет, као ново и све моћније средство за комуникацију која не познаје територијалне границе, постао незаменљив алат за остваривање целог низа људских права. Не само што је погодан за информисање, комуникацију, преглед и преузимање разних садржаја, већ и за ширење идеја, мисли, ставова, формирање јавног мњења и подизање свести о основним људским правима. Ипак, готово сваки дан, наилазимо на примере кршења људских права и утицаја дигиталне технологије на остваривање концепта људских права (дигитална дискриминација[128], повреда права на приватност, забрана популарних друштвених мрежа и сајтова, нпр. Твитера и Јутјуба у Турској; смртна казна за постављање на Фејсбуку у Ирану; пресуда Суда правде Европске уније о „праву на заборав" у случају Гугл против Шпаније (енг. *Google vs. Spain*) од 13. маја 2014. године[129] итд.). Ово нам говори да је заштита људских права у дигиталном контексту „дошла до одређене критичне тачке." Да би се такво стање променило потребно је да сваки актер, а нарочито владе које својим деловањем утичу на прокламацију и уживање људских права, заступа политике о поновном истицању међународног оквира за људска права као централног стуба у области безбедности, развоја и слободе у дигиталном контексту. Захваљујући процесу глобализације у таквим условима расте и својеврсна међународна одговорност држава не само за повреду људских права својих грађана, већ и за њихову прокламацију и поштовање.

Право на приватност у дигиталном добу

Право на приватност је комплексан појам који је временом еволуирао и добио различите облике и вредности. То је изазвало потешкоће међу ауторима када је у питању његова дефиниција. У најопштијем смислу речи „приватност подразумева легитимни захтев појединца да утврди у којој мери жели да себе дели и комуницира са другима. То значи да сваки појединац има право да се повуче или да учествује у заједници када је то потребно, као и право да контролише ширење информација о себи."[130] Луис Брандиес (енг. *Louis D. Brandies*) је назвао право на приватност „*право да се буде остављен на*

[128]Дигитална дискриминација је облик дискриминације који још увек није јасно дефинисан и истражен у академским круговима. У најопштијем смислу речи „дигитална дискриминација" подразумева представљање дискриминаторног садржаја и дискриминаторних ставова дигиталним средствима. Према томе није у питању нека нова врста дискриминације, већ нови начин изражавања и ширења дискриминаторног садржаја и постојеће дискриминације. Ипак, у питању је шири појам који, услед развоја технологије, укључује и неке нове аспекте дискриминације и насиља на интернету, као што су нпр. сајбер малтретирање и сајбер ухођење. Било да је изражена отворено или у скривеној форми често је тешко спречити ширење дискриминаторног садржаја новим технологијама. Један од корака за сузбијање ове врсте дискриминације је промоција позитивних ставова између „реалне" и „дигиталне" заједнице, промоција позитивних акција, као и доношење и имплементација постојећих закона који се тичу забране дискриминације, говора мржње, злочина из мржње, сајбер малтретирања, сајбер ухођења и сл.

[129] У овом случају Суд правде ЕУ је признао право појединаца да од популарног интернет претраживача „Гугла" (енг. *Google)* затраже да њихови подаци о личности буду избрисани из резултата претраге. Ова пресуда је изазвала доста полемике у јавности. У медијима се писало о њеној контроверзности, с обзиром да иста подрива слободу изражавања и информисања и захтева од „Гугла" да помаже људима да са интернета нестану ствари који им се не свиђају. Овом пресудом се успоставља ново право под називом „право на заборав" (енг. *right to be forgotten*).

[130] Breckenridge, A.C.: The Right to Privacy, University of Nebraska Press, Lincoln, 1970, p.1.

миру.“[131] Поставља се питање да ли желимо да увек будемо остављени на миру? То је свакако немогуће будући да живимо у заједници са другима и имамо потребу да комуницирамо и учествујемо у тој заједници. Овај аспект приватности иде руку под руку са надлежностима носиоца извршне власти - влада које, с једне стране, имају највећу моћ да контролишу нашу приватност док, с друге стране, оне то раде с намером да нас заштите. У том контексту важно је напоменути да је право на приватност неопходно у смислу заштите од друштва у којем владе имају потпуну контролу над људским животом. То укључује сфере живота које су од посебног значаја за нашу слободу и индивидуалност. Ствари које многи од нас сматрају приватним укључују наше мисли, наше разговоре са другима, наше интимне везе, наше личне ствари итд.[132] Међутим, с обзиром да се разликујемо и да долазимо из различитих културних средина, разликују се и наша уверења о вредностима које сматрамо приватним и које желимо заштитити од других. Услед развоја науке и технологије не само што су се променили ставови о приватности, већ је и само право на приватност исправљено пред многим изазовима.

Брзим напретком информационо-комуникационих технологија дошло је до драматичног побољшања комуникација и размене информација широм света. Док савремене технологије, с једне стране доприносе побољшању квалитета живота и уживања људских права, с друге стране, оне су осетљиве на електронски надзор и прислушкивање. Високи комесар за људска права је у својим изјавама 2013. и 2014. године упозорио да такав надзор прети појединим људским правима, укључујући право на приватност и слободу изражавања и удруживања, и инхибира слободно функциконисање активног цивилног друштва. У том контексту усвајање Резолуције 68/167 Генералне скупштине Уједињених нација о праву на приватност у дигиталном добу у децембру 2013. године је од кључног значаја за заштиту права на приватност у светлу нових изазова. Изразивши дубоку забринутост због негативног утицаја надзора комуникација и прислушкивања на људским правима, Генерална скупштина је том приликом позвала све државе да: а) поштују и штите право на приватност у дигиталној комуникацији; б) преиспитају своје поступке, праксу и законе који се односе на надзор комуникација, прислушкивање и прикупљање личних података; и в) осигурају пуну и ефикасну имплементацију својих обавеза према међународном праву о људским правима.

Имајући у виду да се све више и више лични подаци прикупљају, обрађују и споделују, у новембру 2016. године Генерална скупштина Уједињених нација је усвојила нову резолуцију о праву на приватност у дигиталном добу која изражава забринутост због продаје или вишеструких поновних продаја личних података, што се често догађа без слободног, експлицитног и информисаног пристанка појединца. Она позива на јачање превенције и заштите од таквих повреда, и позива државе да развију превентивне мере, санкције и правне лекове. Ова резолуција више него експлицитно се осврће на улогу приватног сектора, позивајући државе да успоставе (или одрже) ефикасне санкције и правне лекове које ће спречи приватни сектор да врши повреде и злоупотребе

[131] Garrett, B.: Individual Rights and Civic Responsibility, The Right to Privacy, The Rosen Publishing Group, New York, 2001, p. 6.
[132] Op.cit., p.7.

права на приватност. То је у складу са обавезама држава према „Водећим принципима Уједињених нација о пословању и људским правима“, који захтевају од држава да штите од злоупотреба од стране предузећа у оквиру својих територија или надлежности. Резолуција посебно позива државе да се уздрже од захтева предузећа да предузму незаконите кораке који повређују право на приватност. Што се тиче предузећа, она подсећа на одговорност приватног сектора да поштује људска права, и нарочито их позива да информишу своје кориснике о политици предузећа која може утицати на њихово право на приватност. У резолуцији се наводи да повреде и злоупотребе права на приватност више утичу на појединце, а посебно на жене, децу и рањиве и маргинализоване заједнице. Она повезује право на приватност са остваривањем права на слободу изражавања, као и учешће у политичком, економском, социјалном и културном животу, што изазива све већу идентификацију сигурности и надзора од стране влада и корпорација. Иако је у периоду од прве до друге резолуције дошло до значајних позитивних промена (оснивање специјалног известиоца за право на приватност) потребни су додатни напори за спровођење резолуције која није обавезујућа. Њена примена ће зависити и од озбиљности држава да схвате своје обавезе према међународном праву о људским правима и да побољшају своје законе и праксу у погледу њихове надзорне праксе.

Један од корака за заштиту људских права у дигиталном контексту је глобална подршка и поштовање критика специјалног известиоца за право на приватност у дигиталном добу. Специјални известилац је независни експерт за међународно право људских права именован од стране Савета Уједињених нација за људска права у јулу 2015. године на период од три године. Стварање овог хитно потребног међународног мандата је у складу са Резолуцијом о праву на приватност у дигиталном добу коју је Генерална скупштина Уједињених нација усвојила 18. децембра 2013. године. Главна идеја стварања специјалног известиоца је уследила након уочавања изазова који произилазе из нових технологија и последица неконтролисаног масовног надзора, укључујући и ерозију темељне слободе изражавања, окупљања и удруживања. У таквим условима сасвим је сигурно да ће ситуације у којима се прати све оно што желимо рећи или урадити негативно утицати на слободу грађана да у потпуности уживају своја права. Успостављањем специјалног известиоца Уједињене нације су значајније приступиле решавању проблема заштите права на приватност, укључујући и право на заштиту података о личности, и то са аспекта дигиталног доба и утицаја нових технологија на њих. У циљу јачања заштите и спречавања даљих повреда људских права која су тесно повезана са правом на приватност у дигиталном добу, очекује се да специјални известилац да суштински допринос развоју кохерентног приступа међусобном односу приватности, слободе изражавања и других људских права.

Специјални известилац је мандат добио Резолуцијом 28/16 Савета за људска права, у чијем уквиру спадају следећа овлашћења: а) да прикупља релевантне информације, укључујући међународне и националне оквире, националне праксе и искуства, да проучава трендове, развој и изазове у вези са правом на приватност и да даје препоруке како би се осигурала њихова промоција и заштита, укључујући и изазове који произлазе из нових

технологија; б) да тражи, прима и реагује на информације, избегавајући дуплирање, од држава, Уједињених нација и њених агенција, програма и фондова, регионалних механизама за заштиту људских права, националних институција за људска права, организација цивилног друштва, приватног сектора, укључујући и привредна предузећа, и било које друге релевантне актере или стране; в) да утврди могуће препреке за промоцију и заштиту права на приватност, да идентификује, размењује и промовише принципе и најбоље праксе на националном, регионалном и међународном нивоу, као и да подноси предлоге и препоруке Савету за људска права у том смислу, укључујући и одређене изазове који настају у дигиталном добу; г) да учествује и доприноси релевантним међународним конференцијама и догађајима са циљем промовисања систематског и кохерентног приступа питањима која произилазе из његовог мандата; д) да подиже свест о важности промовисања и заштите права на приватност, укључујући и одређене изазове који су настали у дигиталном добу, као и о значају омогућавања права на делотворан правни лек појединцима чије право на приватност је нарушено, у складу са међународним обавезама људских права; ђ) да интегрише родну равноправност током рада мандата; е) да извештава о наводним повредама, где год да се десе, права на приватност, као што је наведено у члану 12 Универзалне декларације о људским правима и члану 17 Међународног пакта о грађанским и политичким правима, укључујући и у вези са изазовима који произилазе из нових технологија, и да скрене пажњу Савету и Високом комесару Уједињених нација за људска права на ситуације које нарочито озбиљно забрињавају; ж) да подноси годишњи извештај Савету за људска права и Генералној скупштини, почевши од тридесет прве односно седамдесет прве седнице.[133]

Право на приватност је несумњиво повезано са правом на заштиту података о личности, будући да промоцијом нових технологија, ова заштита постаје дигитална. О њиховој повезаности сведочи и судска пракса Европског суда за људска права и Суда правде Европске уније. Заштита података о личности је шири појам који поред заштиту права на приватност, обуквата и право на слободу изражавања, слободу веросиповести и мишљења, слободан проток информација и право на недискриминацију. Међународно правна регулатива о заштити приватности и заштити података о личности је подигнута и на новоу комунитарног права Европске уније.[134] Европска унија посебно уређује заштиту података о личности на интернету, док Суд правде Европске уније игра активну улогу у тумачењу постојећих законских норми (нпр. успостављање права на заборав).

Да би се постигао развој и напредак у овој области, а нарочито да би се побољшала промоција људских права у дигиталном контексту, која првенствено укључује поштовање људског достојанства, потребно је да се у

---

[133] Special Rapporteur on the right to privacy, http://www.ohchr.org/EN/Issues/Privacy/SR/Pages/SRPrivacyIndex.aspx (5 April 2018).

[134] Најзначајнији инструменти ЕУ који регулишу право на приватност и право на заштиту података о личности су: Повеља ЕУ о основним правима (члан 8); Директива број 95/46/ЕЦ Европског парламента и Савета о заштити појединаца у вези са обрадом података о личности и слободном протоку таквих података од 24. октобра 1995. године; Регулатива број 45/2001 о заштити појединаца у погледу обраде података о личности од стране институција и тела Заједнице и о слободном протоку таквих података од 18. децембра 2000. године; Директива број 2002/58/ЕЦ Европског парламента и Савета о обради података о личности и заштити приватности у подручју електронских комуникација од 12. јула 2002. године;

процесу стварања механизама за управљање интернетом и савременим технологијама укључе сви актери, почев од влада, државника, креатора политика, приватног сектора, технолога, инжењера, привредника, па све до невладиног сектора и организација цивилног друштва које су посвећене промоцији и заштити људских права. Заштита људских права и владавине права у дигиталном контексту је од суштинског значаја не само за заштиту националне, већ и међународне безбедности.

ЗАКЉУЧАК:

Растући и непредвидив тренд промена у односима између информационо-комуникационих технологија и свеукупног друштва снажно утиче на цео спектар људских права, а поготово на заштиту права на приватност и слободу изражавања у дигиталном добу. У условима када су људска комуникација и пословање попримили нове, дигиталне облике потребно је да сви нивои друштва, почев од државног врха, влада, предузећа, академске заједнице, организација цивилног друштва па до сваког грађанина, критички размотре питање људских права која су предмет злоупотреба у дигиталном добу као један од националних изазова. Начин на који ће владе, надлежне институције и предузећа (у јавном, а поготово у приватном сектору) одговорити на изазове које са собом носе процеси глобализације и дигитализације, снажно ће утицати на животе многих корисника информационо-комуникационих технологија у различитим сферама живота. У складу са међународним и домаћим стандардима заштите људских права владе су дужне да поштују, штите, промовишу и остварују људска права. То, између осталог, подразумева адекватну примену и усклађивање националне легисталиве са међународним стандардима о заштити приватности и слободе изражавања, као и одговорност компанија да, у условима дигиталне трансформације, поштују слободу изражавања и право на приватност сваког појединца. Дигитална сигурност, у најопштијем смислу речи, захтева дијалог између компанија у смислу проналажења одговарајућег приступа за спровођење њихових активности у складу са захтевима за заштиту људских права, дебате које окупљају више заинтересованих страна, адекватну едукацију на свим нивоима друштва, подизање свести о праву на приватност и могућим повредама људских права у дигиталном добу, одговарајуће и ефикасне инструменте и механизме за заштиту људских права на међународном, регионалном, националном и локалном нивоу (нпр. глобалне, регионалне и националне иницијативе о управљању интеренетом, форуми, тела) итд.

м-р Стефан Димоски
Европски Универзитет Република Македонија
Факултет за детективи и криминалистика
Република Македонија
e-mail: stedimmk2@yahoo.com

ПОЛИЦИЈАТА И ПРИВАТНОТО ОБЕЗБЕДУВАЊЕ VIS-A-VIS МЕДИУМИТЕ

Апстракт
Глобалните процеси кон крајот на XX и почетокот на XXI век, предизвикаа брз развој на науката, техниката и технологијата. Светот доживеа огромни и значајни општествено-политички, економско-социјални, техничко-технолошки, културни и цивилизациски промени и извонредно брз мулти - димензионален интеграциски прогрес. Интензивната глобализација на човештвото му донесе глобализацијата на пазарот, воспоставување целосно нов информациско-комуникациски систем, дигитални трансформации, нагласена транспарентност но и потреба од силен концепт на корпоративно управување како основа за одржлив економски развој. Во ерата на глобализацијата и компјутеризацијата, на интеракциските процеси, информатичката технологија и новите медиумско-комуникациски технологии, се создаде една сосема нова безбедносна реалност во меѓународни рамки и универзалност на безбедносните предизвици и ризици. Новото безбедносно опкружување, светот го соочи со низа нови форми на организиран криминал, корпоративен и компјутерски криминал, тероризам, екстремизам и други сложени разновидни закани по светската сигурност. Глобализацијата со своето силно стратегиско влијание врз безбедносните системи, ги постави безбедносните прашања и нивното решавање како врвен приоритет што е од суштинска важност за ефикасна безбедност и ефективно справување со опасностите по светскиот мир.
Во светот но и во Република Македонија, медиумите како социјални феномени, доживеаја значителни системски потреси и промени а суштинско значење доби корпоративното управување и потребата од силна корпоративна безбедност на компаниите. Во новите демократските општества, полицијата добива нова позиција и е круцијален легитимен фактор во справувањето со новите безбедносни проблеми и заштитата на личната сигурност на граѓаните и нивните материјални добра. Покрај тоа, интерес на секоја демократска држава е системски да ја уреди работата и во приватниот сектор за обезбедување односно на приватните правни субјекти кои пружаат услуги во сферата на безбедноста. Во развиените демократии, тоа се прави пред се, да се заштитат човековите права и слободи но и да се унапреди севкупната сигурност и безбедност на државата, стопанските субјекти и секако сигурноста на граѓаните. Преку своите законски механизми, демократските држави треба да креираат функционален систем во кој, тие ќе можат да ги искористат капацитетите на субјектите во приватното обезбедување со цел да ја унапредат севкупната безбедносна состојба во државата.

Клучни зборови: глобализација,корпоративно упраавување, интеракциски процеси, нови форми на организиран криминал, полиција, приватен сектор во обезбедување.

1.Вовед и поимно определување

Во речничко-енциклопедиската литература, под поимот медиум, се подразбира секое средство за комуницирање преку кое може да се пренесува порака или информација од комуникаторот до реципиентот без оглед на тоа дали во улога на комуникатори, односно реципиенти, се јавуваат поединци или групи, како актери на комуникативната практика. Поимот масовен медиум претставува средство за масовно комуницирање со чие посредство се остварува дифузија на пораката, информацијата од изворот кон неброената маса реципиенти, односно масовната публика. Во масовните медиуми ги вбројуваме: печатот, радиото, филмот, телевизијата, интернетот. Секој од овие медиуми има свои специфични техничко-технолошки својства и е функционално оспособен да ги дифузира, за него, приспособените пораки. Медиумите, како субјекти што имаат силна јавна општествена функција, постојано, во фокусот на својот интерес ја имаат полицијата како најдиректно одговорен орган на државната управа, за јавната безбедност. Со својата моќ за информирање и креирање на јавното мислење, медиумите се мост кон јавноста и субјект за контрола врз работата на полицијата.

Оценувајќи ја полицијата како посебно организирана државна служба за заштита на јавниот ред и поредок и на внатрешната безбедност, денес повеќе автори ја посочуваат дефиницијата на Б.Милосављевиќ, според која, полицијата е „ сложен систем од професионален тип, организиран заради одржување на јавниот ред и поредок во општеството, кој, за таа цел има законски овластувања и потребни средства, вклучувајќи ги и средствата за принуда“. ***(фуснота: Милосављевиќ Б. Историски осврт на полициското работење)**

За полициската организација во граѓанските општества, од огромна важност е јасното дефинирање и практикување на стратегиската определба за функционирање во согласност со националните и меѓународните закони, за континуирани демократски промени и реформи во сопствените редови, почитување на човековите права и слободи и еднаквост на сите пред законите. Полициското работење претставува круцијален сегмент од севкупната полициска организација и интегрален дел од целокупниот безбедносен систем на една општествена заедница. Полициското работење треба да ја покаже способноста на полицијата за справување со сите облици и форми на криминалитет, да покаже дека полициската организација ефикасно работи, ефективно го контролира и сузбива криминалот.

Според членот 1 од Европскиот кодекс за полициска етика од 2001 година, основните задачи на полицијата во едно демократско општество, раководено со владеењето на правото, се:

- Да го одржува јавниот ред и мир и поредокот во општеството;

- Да ги штити и почитува фундаменталните права и слободи на поединецот; особено како што се содржани во Европската конвенција за човекови права;

- Да го спречува и да се бори против криминалот;

- Да го открива криминалот;

- Да обезбедува помош и услужни функции на јавноста *(**за фуснота*Полициско работење во мултиетничка средина-Прирачник, Скопје,2003)**

Според членот 3 од Законот за полиција, основна функција на Полицијата е заштита и почитување на основните слободи и права на човекот и граѓанинот гарантирани со Уставот на Република Македонија, законите и ратификуваните меѓународни договори,заштита на правниотпоредок, спречување и откривање на казниви дела, преземање мерки за гонење на сторителите на тие дела, како и одржување на јавниот ред и мир во општеството.

(*фуснота Службен весник на Република Македонија број 114 од 03.11.2006 година и Указ за прогласување на Законот Бр. 07-3954/1 од 30 октомври 2006 година,Скопје.

Задачите на полицијата, практично значат работа во корист на граѓаните и нивната севкупна безбедност.

Во корист на граѓаните е фокусирана и работата на приватното обезбедување како дејност од јавен интерес, кое го опфаќа давањето на услуги, односно вршењето на работи на заштита на лица, имот и работење со физичка и техничка заштита, кога тие работи не се во исклучива надлежност на надлежните органи. Според Законот за приватно обезбедување (Објавено во Сл.Веснк на Република Македонија, бр.166 од 26.12.2012 година), приватното обезбедување е дејност од јавен интерес и со овој закон се уредуваат условите за вршење на приватно обезбедување; вршењето на приватното обезбедување;приватното обезбедување за сопствени потреби;задолжителното приватно обезбедување;овластувањата на работниците за приватно обезбедување; работната облека и ознаката на работниците за приватно обезбедување; формирањето, овластувањата и финансирањето на Комората на Република Македонија за приватно обезбедување; евиденциите, заштитата на податоците и информациите, надзорот, овластувањето за подзаконски прописи и прекршочните одредби..

Правните лица кои имаат дозвола за приватно обезбедување преземаат мерки и активности утврдени со овој закон заради спречување и откривање на штетни појави и противправни дејствија кои ги загрозуваат телесниот интегритет и достоинството на личноста и имотот што се обезбедува

.(*фуснота Закон за приватно обезбедување - Сл.Веснк на Република Македонија, бр.166 од 26.12.2012 година)

Услугите на приватното обезбедување не спаѓаат во полициски и безбедносни работи коишто ги вршат органите на државната управа. Моментно, во Република Македонија, во областа на приватното обезбедување

работаат околу четири илјади службеници-работници на приватно обезбедување.

Тие, како дел од приватниот безбедносен сектор на Република Македонија, во извршувањето на своите задачи за обезбедување поголема сигурност на правните и физичките лица, реално се соочуваат со низа нерешени состојби пред се во делот со нормативната регулација на законот односно дорегулацијата на јавните овластувања на работниците за приватно обезбедување.

2.Медиумите како интегрална компонента на полициската работа и приватното обезбедување

Медиумите (лат.media-средство) или средствата за пренесување на информациите, во демократските граѓански општества го претставуваат „четвртиот степен“ на власта. Тие имаат „привилегија“ да допрат до огромна маса луѓе ширум светот, и со секавична брзина да информираат, изнесуваат факти за одредени состојби и од субјектите во заедницата да пренесуваат ставови и мислења. Тие се креатори на јавното мислење и на социјалната реалност во заедницата.Медиумите, како средства за масовно комуницирање се мост помеѓу општествените субјекти и јавноста во целина. Во современите граѓански општества, медиумите го трансформираат светот во едно „големо село“ и се вистински чувари на демократијата, носители на демократските, цивилизациските и прогресивните вредности. Медиумите силно влијаат врз формирањето на позициите и ставовите на граѓаните односно врз јавното мислење кон најразлични прашања и состојби во општествено-политичкиот, економскиот, социјалниот, и секако во безбедносниот сегмент од функционирањето на општествената заедница.Медиумите се една од инстанците на слободното граѓанско општество за неформална надворешна контрола над полициското работење.Оттука, за полицијата како исклучително значајна безбедносна институција, ставовите на јавноста имаат витална улога во процесот на легитимирање на полицијата и зачувување на нејзиниот авторитет пред општествената јавност. Медиумите го анализираат и коментираат полицискиот правен и стручен капацитет односно севкупната полициска работа со што можат, полицијата во јавноста да ја претстават како легитимна и одговорна полициска организација - заштитник на човековите права и слободи или како насилна, недемократска, затворена, отуѓена, непрофесионална и нехумана институција која ги ограничува и гуши човековите демократски права и слободи.

На тој начин, медиумите го креираат општиот јавен впечаток за поставеноста на полицијата во општествената заедница, го градат нејзиниот имиџ и влијаат врз перцепцијата кај граѓаните за придобивање или отфрлање на почитта и довербата на јавноста кон полицијата и кон нејзините припадници. Медиумите имаат можности, на јавноста да и покажат дали и колку полицијата дејствува законски, етички, ефикасно и ефективно.

Во својата работа медиумите се потпираат врз основното начело на демократското општество, имено, начелото на јавност и потребата, но и правото на граѓаните да бидат навремено и објективно информирани за сите настани и појави во заедницата, вклучително и за оние кои се поврзани со криминалитетот односно имаат безбедносен карактер. Во овој контекст има потреба да укажеме на опасноста од информации кои можат понекогаш да „поттикнуваат“ на криминалитет, а кои се многу присутни во средствата за масовно комуницирање со цел да се постигне одредена сензационалност на веста.*(Јордан Спасески,Пере Аслимоски, Дефендологија, Педагошки факултет Битола, Охрид 2002, стр.283)

3.Полицијата и приватното обезбедување-партнерство и компатибилност

4.Потреби, значење и придобивки од приватното обезбедување во корпоративната безбедност

5.Медиумите, полицијата и приватното обезбедување-комуникациско интеракциски релации

6.Заклучок

7.Користена литература

Тони Наумовски, Д-р
Штабен офицер во Генералштабот на Армијата на Република Македонија
Министерство за одбрана
toninaumovski@yahoo.com;
Ненад Танески, Доцент Д-р
Раководител на Катедрата за Воени науки и вештини во Воената Академија
Министерство за одбрана
nenoreal@yahoo.com;
Методија Дојчиновски, Вонреден професор Д-р
Раководител на Катедрата за Безбедност, управување со кризи, заштита и спасување во Воената Академија,
Министерство за одбрана
metodija.dojcinovski@morm. gov.mk

Поддршка на критичните бизнис функции со користење на Инфраструктура со јавен клуч (PKI)

Апстракт:

Зголемениот тренд од глобална размена на информации помеѓу работодавецот, вработените и деловните партнери ги зголеми заканите по доверли-воста, интегритетот и достапноста на чувствителните деловни податоци. Тоа бара развој на методи кои ќе обезбедат зголемена безбедност на информа-циите за критичните бизнис функции на компанијата. Прашањето е: Како да се докаже идентитетот во „онлајн“ светот? Како што личните карти го докажуваат идентитетот во „офлајн“ светот, еден од начините за докажување на идентитетот во „онлајн“ светот е Инфраструктурата со јавен клуч (PKI). Воспоставувањето на безбеден PKI им помага на компаниите да обезбедат основни безбедносни контроли за критичните бизнис функции. Овој труд се однесува на аспектите на воспоставување на PKI и треба да се смета како студија која ги нагласува ефективните контроли во инфромацискатa безбедност, во однос на чувствителните информации.

Клучни зборови: Инфраструктура со јавен клуч (PKI), информациска безбедност, организација, бизнис функции, политики.

Supporting Critical Business Functions by using Public Key Infrastructure (PKI)

Abstract:

The increasing trend for global information exchange amongst employer, employees, and business partners increased threats to the confidentiality, integrity and availability of sensitive business data. That requires developing methods which will provide increased information security for the company’s critical business functions. The question is: how to prove identity in the online world? As personal ID cards prove identity in the offline world, one of the ways to prove identity in the online world is Public Key Infrastructure (PKI). Establishing of secure PKI helps companies to provide basic security controls to the critical business functions. The

paper is intended to cover the aspects of establishing PKI and should be viewed as a study which highlights the effective information security controls over sensitive information.

Key words: Public Key Infrastructure (PKI), information security, organization, business functions, policies.

Introduction

Information sharing is a one of the critical business functions. During this process there are more and more threats that harm confidentiality, integrity and availability of sensitive business data. The increasing of the threats highly requires developing methods which should provide security to the process of company's/companies' information exchange. One of the approaches related to secure information exchange is Public Key Infrastructure (PKI). Secure information exchange over insecure networks is critical when conducting online sensitive business data and PKI can protect and provide basic security controls during the information exchange.

Business requirements and PKI

PKI is a technology and a set of practices and policies that is highly recommended during information sharing and exchange. PKI offers authentication, confidentiality, integrity, access control as well as non-repudiation. These security controls are critical for the business process. Each PKI solution is unique, and supports the distribution, management, expiration, rollover, backup, and revoking Public/Private Keys. PKI is asymmetric cryptography technology that enables the creation of verified communication between the Public Key and the identity of the correspondent Private Key owner. Public key algorithms, also called asymmetric algorithms, have the property of having a different encryption key for encryption and decryption. The decryption key cannot be calculated from the encryption key and the encryption key can be made public (Paganini, 2017). The encryption key is Public Key and the decryption key is Private Key (Figure 1).

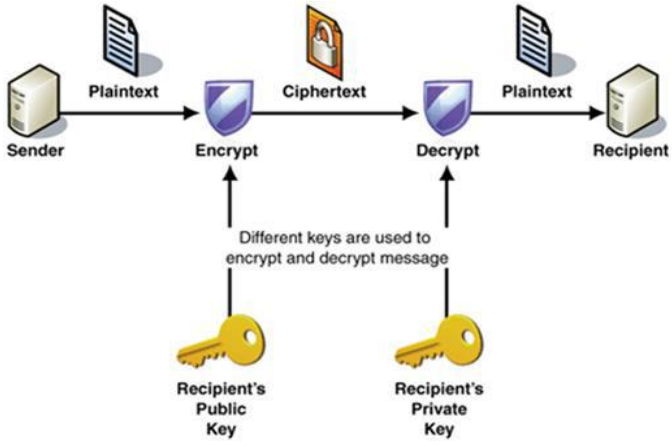


Figure 1: Public key encryption

The main advantage of public key cryptography is the fact that the public key can be made publicly available without compromising on security, as long as the sender keeps the corresponding Private Key secure (Balakrishnan, 2003:5). In general, PKI is a provider of solutions for the following high-level business requirements: *authentication, data encryption and data integrity*. Authentication can be defined as a means of identification. PKI offers this through Digital Certificates. Digital Certificates are sometimes also referred to as X.509 certificates or simply as certificates. Think of a certificate as a virtual ID card (Posey, 2005). Posey simply explain the virtuality. According to Posey, people, in the real world, use ID cards such as driver's license, passport, or employee ID badge to prove their identity and a certificate does the same basic thing in the electronic world, but with one big difference. Certificates are not just issued to people (users, administrators, etc.). Certificates can also be issued to computers, software packages, or to just about anything else that you may need to prove the identity of. Encryption example is given in the article of SANS Institute: A Business Perspective on PKI: Why Many PKI Implementations Fail, and Success Factors To Consider. The most common use of Public/Private keys is for encrypting email messages between people. If Ann wants to encrypt a message for Clark:

- Clark would make his Public Key available (as an attachment to an email sent to Ann, through a directory or a public key exchange site accessible to both Ann and Clark, etc.).
- Ann would compose and address the email message and signal the email software to encrypt the message (usually by clicking on a icon or selecting the action from the Toolbar).
- The email software would use Clark's Public encryption Key, which is stored with his information in Ann's email address book or available in a shared area, to encrypt the message.
- Ann sends the encrypted message to Clark.
- Clark's email software receives the message and automatically tries to decrypt it using Clark's Private encryption Key, or through a dialog box, offers to decrypt the message.
- If the email message was really encrypted using Clark's Public Key, then Clark's Private Key will decrypt the message so Clark can read it.

The concept of data integrity reveals any changes to files, programs, transmissions and the Public Key Infrastructure provide integrity, which is ensured by message hashing.

It is not possible to prevent attacks, but it is possible to reduce them and to implement controls that make the compromise much more difficult. PKI helps to secure companies and critical business functions.

PKI function, operation and managing

Public Key Infrastructure (PKI) is a popular encryption and authentication approach used by both small businesses and large enterprises (Lawton, 2015). PKI infrastructure is comprised of listed main components: Digital Certificates; Public and Private Keys; Certificate Authority (CA) and Registration Authorities (RA). The

framework of a PKI consists of security and operational policies, security services, and interoperability protocols supporting the use of public key cryptography for the management of keys and certificates. The generation, distribution, and management of Public Keys and associated certificates normally occur through the use of Certification Authorities (CA), Registration Authorities (RA), and directory services, which can be used to establish a hierarchy or chain of trust (Weise, 2001). In the article of cryptography part 5: The Mathematical Algorithms of Asymmetric Cryptography and an Introduction to Public Key Infrastructure, available on the INFOSEC INSTITUTE web site, are explained the basic premises of PKI. It is clearly noted that the PKI is to help create, organize, store, and distribute as well as maintain the Public Keys. In PKI infrastructure, both of the Public and Private Keys are referred to as Digital Signature. They are created by a separate entity known as the Certificate Authority (CA), not by the sending and the receiving parties. The Digital Certificate consists of both the Public key and the Private Key, issued by the relevant CA. This is also the entity that verified Digital Certificate. The Digital Certificates are typically kept in the company's central server. The databases that collect and distribute the Digital Certificates from the CA are the LDAP or X.500 directories. Another term is the Registration Authority (RA) that usually exists in big Multinational Corporation. RA handles and processes the requests for the required Digital Certificates and then transmits those requests to the CA where are created the required Digital Certificates. To summarize, the Public Key Infrastructure (PKI), as a specialized form of asymmetric cryptography, offers a higher level of security not only by using the Public Key/Private Key combination but also by making use of the CA. CA is trusted, third party governing body of PKI, where all Public Keys/Private Keys are created and verified. This is important to ensure the integrity amongst the Digital Certificates, related to the communication process for both, the sending and the receiving parties. Another mechanism of security is RA which confirms the identities of the sending and receiving parties that are requesting the Public Key/Private Key combinations. The parties must be uniquely identifiable within each CA and the verification process provides that information (Figure 2).

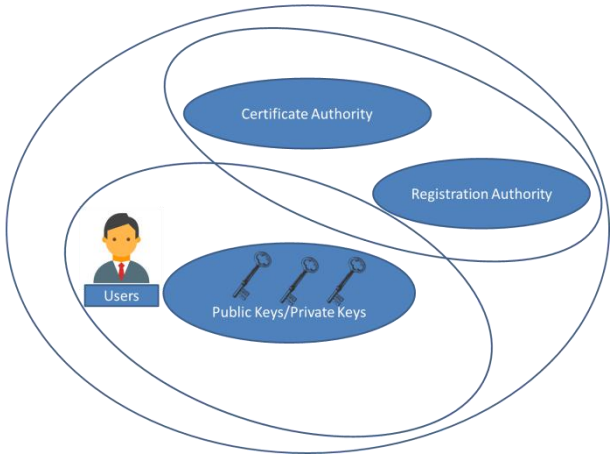


Figure 2: Public key infrastructure

Mentioned, related to function and operation of CA and RA is tightly connected with various policies and rules. The Certificate Authority must provide for adequate protection of the Private Key that it uses to sign certificates. The machine that CA runs on must be protected from network and physical intrusions (Patriciu and Serb, 2000). Attacks against company computer infrastructure have existed as long as technologies development. Also, with the globalization, increases the numbers of companies in all parts of the world significantly changed companies acting and the threats manifestation and perception. Besides education, strong password polices and as well as installing updates to the company computer system is important to ensure that devices only communicate with other trusted devices. Maintaining the trust is an integral component for implementing a PKI. To facilitate trust PKI must be managed with policies, standards and procedures. Through a risk assessment, it is possible to reduce the attacks and implementation of required PKI policies, standards and procedures makes the compromise much more difficult.

A Public Key Infrastructure uses the basic Public-Private key-pair relationship to build not only many of its services provides but also the trusted infrastructure that provides the services (Lareau, 2002). Brown (2001) explains the PKI 'Questions of trust'. Brown states that besides being a technology based on Public/Private Keys and Digital certificates, PKI is also a trust network which operates at several levels. They are:

- trust between organizations and their PKI service providers (Certificate Authorities for example),
- between companies and their trading partners, and
- among individual employees.

According to Microsoft (Microsoft IT Showcase Article: Managing Public Key Infrastructure in the Enterprise, June 2014) many organizations deploy a Public Key Infrastructure (PKI) to support critical business functions, such as strong authentication of users for remote access or for helping to protect access to sensitive data. It is noted that attacking a PKI infrastructure is typically not the end goal of attackers, and compromising a PKI can provide attackers with credentials that they can use to gain further access. Security of the systems and processes that compose a PKI is an important consideration in the design and deployment of a PKI, and the solution that is recommended by Microsoft is as follows: Planning a CA Hierarchy (consider long-term business goals); Providing Physical Controls (identify the key physical security controls); Establishing Processes (establishing repeatable processes); Providing Technical Controls (deploy strong technical controls to protect the PKI from unauthorized access); Planning Certificate Algorithms and Usages (ensure that is selected the strongest cryptographic algorithms); Storing and Managing Keys and Artifacts (primary security control in a PKI is how Private Keys are stored and managed); and Monitoring (key component of any PKI security plan is ongoing monitoring of the infrastructure and supporting processes); Developing a Compromise Response (it's vital to have a plan of action in the event of a PKI compromise).

The listed recommendations are a brief look at Microsoft PKI best practices. Details are given in the Microsoft IT Showcase Article: Managing Public Key Infrastructure in the Enterprise, June 2014.

Conclusion

The purpose of a PKI is to manage keys and certificates by establishing and maintaining a trustworthy company networking environment. In other words, PKI facilitate the secure electronic transfer of information and its use is across a wide variety of applications. It is a set of policies, standards and procedures related to authentication, encryption and non-repudiation that all operating within a chain of trust. It is necessary to develop a strong process that ensures that the PKI is run with oversight from the proper teams within companies and ensure its secure operating and proper managing.

References

1. Balakrishnan, T.: Current Status of Public Key Infrastructures. Report, 2003.pp.1-61. https://minerva.leeds.ac.uk/bbcswebdav/orgs/SCH_Computing/MSCProj/reports/0203/balakrishnan.pdf
2. Brown, K.J.: PKI and Information Security Awareness: Opportunity and Obligation. SANS Institute InfoSec Reading Room. (2001). https://www.sans.org/reading-room/whitepapers/vpns/pki-information-security-awareness-opportunity-obligation-750
3. Lareau, P.: PKI Basics - A Business Perspective, PKI Forum's Business Working Group. April 2002. http://www.oasis-pki.org/pdfs/PKI_Basics-A_business_perspective.pdf
4. Lawton, S.: Introduction To Public Key Infrastructure (PKI). tom'sIT PRO real-world business technology. MARCH 17, 2015. http://www.tomsitpro.com/articles/public-key-infrastructure-introduction,2-884.html
5. Microsoft IT Showcase Article: Managing Public Key Infrastructure in the Enterprise, June 2014.https://msdn.microsoft.com/en-us/library/dn756431.aspx
6. Paganini, P: Cryptology for Business and Organizations on the 21st century. Security Affairs. April 27, 2017.http://securityaffairs.co/wordpress/58459/security/cryptology-businesses-cyber-security.html
7. Patriciu, V.V. and Serb, A.: Design Aspects in a Public Key Infrastructure for Network Applications Security. Report: New Information Processing Techniques for Military System. Defense Technical Information Center. 2000. http://www.dtic.mil/dtic/tr/fulltext/u2/p010879.pdf
8. Posey, B.: A beginner's guide to Public Key Infrastructure. TechRepublic September 15, 2005. https://www.techrepublic.com/article/a-beginners-guide-to-public-key-infrastructure/
9. SANS institute: A Business Perspective on PKI: Why Many PKI Implementations Fail, and Success Factors To Consider. SANS Institute InfoSec Reading Room. (2001) pp 1-9. https://www.sans.org/reading-room/whitepapers/vpns/business-perspective-pki-pki-implementations-fail-success-factors-728
10. INFOSEC INSTITUTE: The Mathematical Algorithms of Asymmetric Cryptography and an Introduction to Public Key Infrastructure.http://resources.infosecinstitute.com/mathematical-algorithms-asymmetric-cryptography-introduction-public-key-infrastructure/#article
11. Weise, J.: Public Key Infrastructure Overview. SunPSSM Global Security Practice Sun BluePrints™ OnLine. August 2001. https://pdfs.semanticscholar.org/6439/5a36e7eedfdf60f885ad013ac125dc6e37de.pdf

Стефанија Агротова, м-р
Факултет за Детективи и криминалистика – ЕУРМ, Македонија
stefanija.agrotova@eurm.edu.mk
Славески Стојан, проф д-р
Факултет за Детективи и криминалистика – ЕУРМ, Македонија
slaveski.stojan@eurm.edu.мk

Корпоративната безбедност и заштита на тајноста на податоците

КРАТОК ИЗВАДОК:

Корпоративната безбедност е резултат на новата општествена реалност и особено од сознанието дека и нашата држава има потреба од истражување во оваа област. Дијапазонот на активности на корпоративната безбедноста ја прави да биде комплексна, а во ерата на интернетот активностите на секоја организација се загрозени. Факт е дека податоците од интернетот се достапни за секого но кражбата на истите или измамата може да биде сериозен проблем. Оттука се извлекува прашањето во врска со секојдневната заштита на податоците со кои работат самите компании. Што и како се превзема како мерка за заштита на податоците? Колку се инофрмирани самите вработени за заштита на податоците? Овој труд ќе ни даде одговор на овие и други прашања со кои секојдневно се соочуваат организациите. Ќе биде разгледана и регулативата во нашата држава како и почитувањето на истата

Клучни зборови: загрозени, тајни податоци, заштита, корпоративна, безбедност

Absract:

The corporate security is a result of the new social reality and especially from the knowledge that our country also needs research in this area. The range of corporate security activities makes it complex, and in the era of online activities of any organization are threatened. The fact is that online data is available to everyone, but their deprivation or fraud can be a serious problem. This raises the issue of day-to-day data protection by the companies themselves. What and how is it taken as a measure of data protection? How many employees have been tamed to protect the data? This paper will give us an answer to these and other questions that organizations face every day. The regulations in our country will be reviewed as well as respecting it

Keywords: threatened, secret data, protection, corporate, security

Вовед

Веќе две децении европските држави, американските, како и дел од азиските државни институции развиваат и нудат програми од областа на корпоративната безбедност како одговор на потребите од сé поприсутната приватизација на безбедносниот сектор во национални и во глобални рамки, каде корпоративната безбедност денеска регулира голем дел од животот и од

бизнисот во многу држави во светот. Бројни примери потврдуваат дека оваа дејност има широк дијапазон активности, а тоа ја прави комплексна, разновидна и привлечна. Оттука, нема дилема дека корпоративната безбедност игра една од поважните улоги во остварување на безбедноста на податоците. Исто така би сакале да потенцираме дека ефикасноста во справување со одредени специфични ризици и закани придонесе за подигнување на свеста кај поединците и кај фирмите за корисната функција и за реалната потреба од дополнителна превенција и заштита на тајноста на податоците и заеднички добра, бизниси и имот од различни безбедносни закани. Во тој контекст, согледувајќи ги новите реалности преку овој научен труд ќе придонесеме за поадекватно и за попродлабочено разбирање на сета сложена и противречна општествена стварност. Тоа е истовремено и процес на континуирано култивирање за значењето на новата безбедносна парадигма.

Важноста од нормативна рамка за заштита на податоците

Функционирањето на општеството во современиот свет се базира на меѓусебно поврзани национални и меѓународни информатички инфраструктури. Постоечкиот глобален тренд за интеграција на комуникациските и информатичките технологии, доведува до зголемување на нивната ефикасност од една страна и нивната ранливост од друга страна. Можноста за неуспех на сегменти на системот подразбира опасност од прекинување на перформансите на системот како целина. Постојаното зголемување на важноста на информациите ги прави комуникациските и информативните системи незаменливи и, во исто време, соодветни цели за напад од страна на поединци, групи и држави, чија цел е прекин на нормалниот ритам на животот и општеството. Тоа е причината поради која е неопходно да се дефинира заедничка и сеопфатна политика и нормативна рамка за заштита на податоците во корпациите. Во Република Македонија, експертите од оваа области се децидни, не постојат прецизни одредби за безбедноста на информациите од чувствителен карактер.

Последици од неовластено откривање на податоците

Информациските инфраструктури и услугите што ги поддржуваат корпорациите се соочуваат со зголемување на безбедносните закани. Неовластеното откривање, корупција, кражба, нарушување или негирање на информатичките технологии имаат потенцијал да влијаат врз јавниот и приватниот сектор и општеството во целина. Една од целите на секое современо општество е да го промовира развојот на културата на безбедност во општеството. Некои информациски системи се критични бидејќи нивното нарушување или уништување би имало сериозно влијание врз безбедноста, економската или ефективното функционирање на корпорациите. Значи податоците кои се од големо значење за корпорациите треба да се чуваат во тајност, бидејќи нивното откривање на јавноста би можело да ја загрози работата. Од друга страна, корпорациите треба да им овозможат на граѓаните

слободен пристап до сите други информации. Транспарентноста е особено важен фактор за успехот на реформите во корпорациите.[135] Оттука, многу е тешко да се смени пристапот сѐ додека системот не се отвори до јавен надзор. Кога се комбинираат со нови луѓе и практики, транспарентноста го зголемува јавниот интерес во начинот на кој се управува со информациите. Затоа, корпоративната безбедност е фокусирана на процесите и состојбите во определена компанија, односно е приспособена да одговори на структуралните ризици за компанијата, преку примена на определени модели на симулација за спроведување на најдобрата безбедносна практика во компанијата. Суштината е во тоа дека во деловните субјекти мора да ги обединат сите работи врзани за безбедноста и заштитата на податоците. Во согласност со насоките од Европската унија, во таквите субјекти се инсистира на интегрална безбедност, која во себе ги опфаќа работите од обезбедување во најширока смисла (security) и работите врзани за заштитата (safety).[136] Заради ваквата комплексност во теориското дискурс за прашањата од корпорациската безбедност се смета дека се едни од најтешките, затоа што се врзани за управувањето со сите безбедносни процеси во корпорацијата, но ова не значи дека создавањето ваков систем само по себе ќе значи и соодветен придонес за поефикасна заштита на корпорациите од загрозувања кои се насочени кон безбедноста на имотот и кон работењето на компаниите. Сепак, нема дилема дека заштитата на податоците на корпорациите мора да биде врвен приоритет за корпорациската безбедност на компанијата која мора да биде исклучително добро организирана, имајќи ги предвид мотивите на сопствениците на имотот и капиталот да го заштитат и да ги сочуваат по секоја цена.

Препораки за заштита на тајноста на податоците

Нарушувањето на безбедноста на информациите претставува безбедносен ризик за корпорациите. Поради фактот на постоење на различни видови инофрмации, имаме и различни видви на пристап на заштита на истите. Како самите корпорации можат да допринесат за намалување на ризикот од оддавање на информациите важни за корпорацијата? Постојат различни видови на активни мерки кои можат да се воспостават и применат во самите корпорации меѓу кои: следење на активности на вработените, набљудување на нивната работа со податоците, постојани опсервации и проверки како и реакција од неовластена активност. Генерално потребно е да се истакне безбедносната свест на оние кои ракуваат со тие информации, тука се вклучуваат и постојаните обуки на вработените (доколку се неопходни). Незнаењето и ненамерата за откривањето на информацијата, не ги ослободува вработените од злоупотребата на истите.

Во одредени корпорации посебно е актуелно работењето со интернет информациите, оттука е важно да се почитуваат безбедносните основни

[135] Во Република Македонија овој дел е регулиран со Законот за пристап до информации од јавен карактер сл.Весник13/06, Заради непочитување во оваа област се воспоставува незвависна Комисија за заштита на правото за слободен пристап до информации од јавен карактер.
[136] CONVENTION of 26.7.95 on the establishment of a European Police Office (Europol Convention)

концепти (доверливост, интегритет и достапност).[137] Компјутерот остава многу траги, во таков случај, потребно е воведување на Кодекс на однесување при користење на информатичка-комуникациска технологија на работното место. Препораките во овој дел се однесуваат и на унапредување на преносот на податоци во мрежи, организирање на податоците, законска употреба на компјутерски програми како и воведување и/или напредување на канцелариски пакет.

Затоа, секоја корпорација потребно е да работи на (security awareness) подигнување на безбедносната свест на вработените како важен превентивен пристап при заштита на податоците.

Користена литература

1. Armour, John and Joseph A McCahery (Eds.). (2006). After Enron: Improving Corporate Law and Modernizing Securities Regulation in Europe and the US. Oxford: Hart Publishing.
2. Бакрески. О.: Помеѓу заштитата на националниот интерес и транспарентноста во работата на институциите: Акуелно состојби и предлози за подобрување, Скопје 2017
3. Прирачник информатичка и комуникациска технологија, USAID, 2006 Скопје
4. Hadji –Janev. M., Slaveski, S.: Corporate security and critical infrastructure protection in the Republic of Macedonia, http://sd.fzf.ukim.edu.mk
5. CONVENTION 108 on the Protection of Individuals with regard to Automatic Processing of Personal Data (Council of Europe, 1981)
6. ADDITIONAL PROTOCOL to the Convention 108
7. CONVENTION of 26.7.95 on the establishment of a European Police Office (Europol Convention)
8. Закон за пристап до информации од јавен карактер сл.Весник13/06

[137] Кога овластено лице чита и копира информација, резултатот епознат како загуба на *доверливоста*. За неколку вида информации доверливоста е многу важен атрибут. Примерите на ваквиот вид информации вклучуваат медицински и осигурителни записи, лични податоци на граѓаните, податоци добиени преку истражување,одредени инвестициски планови, итн. Во одредени средини може да постои законска обврска за заштита на приватноста на единката (банки и кредитни компании, болници, лекарски ординации, лаборатории за медицински испитувања, психолошки ординации итн.). Интегритет - кога е достапна на небезбедна мрежа, информацијата може да биде изменета. Кога една информација е изменета на неочекувани начини, резултатот е познат како загуба на *интегритетот*. Тоа значи дека податоците претрпуваат неовластени модификации, како резултат на човечки грешки или намерни активности. Интегритетот е важен кај финансиските податоци, во контролата на воздушниот сообраќај или во сметководството. Достапност на информациите може да се избришат или да станат недостапни. Резултатот од тоа е познат како недостапност. Тоа значи дека лицата овластени за пристап до информацијата не се во состојба да дојдат до неа. Достапноста е честопати најважниот атрибут на услужнитекомпании, кои зависат од информациите (планирање на воздушниот сообраќај, онлајн информативни системи итн.).

Проф. д-р Лидија Наумовска
Европски Универзитет Република Македонија
е-маил: lidija.naumovska@eurm.edu.mk

Улогата на електронските платформи и човечкото однесување во прооцесот на планирање распореди за работа

Апстракт
Во процесот на планирање како менаџерска функција, во подготовка на распоред за работа во компаниите во последно време се користат компјутери кои нудат многу добри алатки, со кои може да се оценат и проверат многу алтернативи и променливи варијабли. Сепак, распоредот, исто така, е организациски процес каде што човечките планери вршат различни активности, како што се: собирање на информации и толкување, комуникација, решавање на загатки и преговарање со различни засегнати страни.
Постојат многу задачи и активности кои ги вршат планерите при создавање на распореди, тие соработуваат и ја координираат нивната работа и улогата на компјутерска поддршка во овој процес. Распоредот го одредува времето на активности и одредува, на пример, кои луѓе работат на бараната проблематика, кога се купуваат суровините, во кој момент ќе започне производството, кога треба да се изврши нарачка на материјалите, кога да се испорачаат готовите производи, кои возила се на распоред, кои луѓе се подготвени да излезат во пресрет на задачата.

Клучни зборови: *планирање, распореди, организациско однесување, софтверски платформи;*

Планирање

Планирањето е комплексен процес кој вклучува серии на разни елементи кои се преплетуваат во разни периоди од работењето на секоја компанија. Има најмалку три типови на планирање: **стратешко, тактично и операционо планирање**.
Стратешкото планирање е поставување на главен план кој ја одредува судбината на фирмата.
Тактичкото планирање е потребно за да се поддржи стратешкиот план, како што е на пример, одредување на корпоративната безбедност на компанијата. Со негова помош, се преведуваат стратешките планови во специфични цели и планови кои се најпристапни и најприфатливи за организационата единка.
Третиот тип на планирање е ориентиран кон операциите кои се вршат од ден за ден, односно оперативното планирање во компанијата и бизнисот. Ова планирање идентификува посебни или специфични процедури и акции, потребни за успешно раководење на бизнисот од страна на пониските нивоа во организацијата.
Планерот мора да ја дефинира моменталната ситуација во компанијата, да ги постави целите, да ги предвиди бариерите и пречките, да состави планови за

акција со цел да ги постигне целите, за да развие буџет, да ги имплементира плановите и да ја контролира нивната примена[138].
Секое делување од страна на планерот треба да биде осмислено и целосно подготвено. Планерот треба да ги исполни следните услови:

- ❖ Да има претходно составен план
- ❖ Поставување на крајни рокови
- ❖ Организација на работниот простор
- ❖ Надградување на личната технолија
- ❖ Зачувување на личните проблеми за во слободно време
- ❖ Психички-интензивни наутро, трудо-интензивни попладне.
- ❖ Делегирање
- ❖ Планерот мора ефикасно и делотворно да функционира

Ефекасно и делотворно функционирање

Тоа што е заедничко на сите делотворни луѓе се **постапките** кои ги прават ефикасни. А тие постапки се исти, без оглед на тоа дали работат во компанија за производство, полиција, војска, агенција за обезбедување, во државна администрација или се декани на факултети.
Постојат пет основни постапки кои се потребни за човекот да стане делотворен.

- Систематски да го мери и користи **времето**.
- Да се концентрира на **резултатите**, а не на методите и средствата кои се користат при тоа.
- Делотворните луѓе (раководители) се развиваат на **нивните предности** и предностите на нивните колеги или надредени, а никако не, на нивните слабости.
- Поставува **приоритети**.
- Донесува **делотворни одлуки**.
- Можеби ништо друго не ги **карактеризира** така добро делотворните раководители како нивната **суптилна и константна грижа која му ја посветуваат на времето.**

Време (Time managment)
Времето е најскапоцениот ресурс на делотворниот менаџер. Тоа е незаменливо и не може да се сочува, туку може само да биде пресметано од активностите со помала вредност, кон активности со поголема вредност, бидејќи сите активности бараат време.
Моментот кога менаџерот ќе размислува за активностите кои ги презема и ќе мисли на своето време, пред да го потроши, ќе почне да го подобрува неговиот тајм менаџмент.
Вработените имаат толку многу обврски, а толку малку време за својот приватен живот, па затоа често се чувствуваат дека се пренатрупани со одговорности и активности. Затоа, може да се случи набрзо да се изгуби

[138] Т.Кралев, Л.Наумовска, *Менаџмент*, Европски Универзитет РМ, Скопје, 2008г.,

контролата и човекот да се чувствува дека животот да го управува него, а не тој го управува него.
Значи, време е да се застане и да се размисли што правиме. Мора да се преиспитаат сите активности од аспект на тоа што нам ни е навистина важно. Потребно е да се организира животот ефикасно, со цел да се постигне рамнотежа и хармонија. Преземањето акција, без претходно размислување е причина за сите неуспеси[139].
Главна алатка за ефикасно користење на времето и правилна распределба на ресурсите е изработка на распоред за работа, особено во компании каде се ба-ра постојано присуство на вработени, работа во три смени, празници и ивикенди.

Распореди

Распоредот опфаќа распределба на ресурси за различни задачи и активности (Leung 2004; Pinedo 2012). Ова вклучува одлуки за приоритетите, тајмингот, распределба на персоналот, распределба на машините, возилата. Повеќето луѓе ќе го препознаат резултатот од процесот на планирање, кој вклучува, на пример, Гантови дијаграми, листи за испраќање и распоред на персоналот. Планирањето е обично класифицирано како комплексен проблем. Дури и малите проблеми со закажување на клиенти, имаат огромен број на алтернативи за избор.
Компјутерите нудат многу добри алатки, со кои може да се оценат и проверат многу алтернативи за кратко време. Сепак, распоредот, исто така, е организациски процес каде што човечките планери вршат различни активности, како што се: собирање на информации и толкување, комуникација, решавање на загатки и преговарање со различни засегнати страни.
Постојат многу задачи и активности кои ги вршат планерите при создавање на распореди, тие соработуваат и ја координираат нивната работа и улогата на компјутерска поддршка во овој процес. Распоредот го одредува времето на активности и одредува, на пример, кои луѓе работат на бараната проблематика, кога се купуваат суровините, во кој момент ќе започне производството, кога треба да се изврши нарачка на материјалите, кога да се испорачаат готовите производи.

Зошто проблемите со правење распоред се тешки?

Компјутерите можат да споредуваат илјадници алтернативни распореди во секунда и да ги идентификуваат прекршувањата на ограничувањата во графиците, кои се премногу големи за да ги разберат човечките распореди.
Пет основни својства на информации го прават невозможно испитувањето на сите можни решенија за планирање.
1.Првиот е поврзан со нумеричката комплексност, бидејќи секогаш треба да се приближат алгоритмите за решавање во разумно време (Pinedo 2012). Приближувањето значи дека е пронајдено решение, но не е нужно оптимално

[139] Isto, kako 1.

решение. Ова резултира со компромис помеѓу брзината и квалитет на решение.

2. Вториот е временскиот диспаритет на информациите. Понекогаш, треба да се донесе одлука, пред да бидат достапни сите потребни влезни информации. На пример, времето на набавка на суровина на производителот, може да биде подолго од времето на добивање понуда на клиентот. Резултатот е дека понудата и побарувачката треба да бидат раздвоени.

3.Третиот е информациска несигурност или неточност. На пример, за некој рецепт во фабрика за лекови, може да се наведе дека компонентите треба да се мешаат две минути, но ова може да биде просечно време. Вистинското време може да зависи од квалитетот на суровината, температурата, влажноста и сл. Затоа, за распоредот е важно да се знаат карактеристиките на процесот (дали има неизвесност или нема). Алгоритмите за распоред можат да земат предвид комбинирање на различни несигурни податоци и пресметување на најлошо и најдобро сценарио.

4. Четвртиот е толкување на информациите во социјален контекст. Ова претставува суптилна и збунувачка ситуација, која најдобро може да се објасни преку следниот пример. Во текот на ноќта, во трета смена во работата на една фабрика, се расипува една машина. Потребна е итна поправка во 4:00 часот изутрина, па затоа клиентот мораше да биде информиран дека нарачката ќе биде испратена подоцна. Но, сигурно работникот нема да го извести клиентот, туку ќе чека да дојде неговиот шеф и тој да го информира. Од друга страна некој треба да го информира магиционерот, транспортерот итн. Корисникот ќе ја следи официјалната рута, што ќе доведе до метеж и незадоволен клиент. Овие околности се многу специфични за времето на расипување на машината или возилото и специфичниот клиент. Овој вид на информации често е поврзан со време, динамичен е, и се решава врз основа на лични односи и чувства, што го прави невозможно квантифицирањето, формализирањето и воведување во формални постапки или употреба на алгоритми при планирање.

5. Петтата - нецелосни информации. Одлуките се донесуваат со најдобри претпоставки што влијаат на тоа каде е лицето, кој е квалитетот на извршената работа, и колку е завршена.

За да се надминат овие проблеми, се користат следниве механизми за справување со овие сложености.

Првиот е, поделба на распоредните задачи усогласени со временскиот хоризонт, или когнитив на обемот на работа. За да се намали сложеноста и да се ублажи диференцијалноста на времето, компаниите традиционално користеле хиерархиско донесување одлуки.

Вториот механизам е алгоритми за планирање. Со алгоритми кои ги следат претходно специфицираните чекори за креирање на распоредот, многу брзо може да се споредат повеќекратни променливи на распоредот, со кои може да се пресметаат овие сложени несигурности и тоа многу подобро отколку што можат луѓето.

Третиот е човечкиот фактор. Првите два механизми можат да бидат дизајнирани и формално структурирани во секојдневните процеси. Сепак, недостапно е користењето на осетливи информации во дизајнот. Ова резултира со потреба за човечки планери за да ги регулираат и да го обработуваат протокот на

информации, што не може да се прецизира. Фактот што човечките планери играат улога во процесот на планирање, подразбира дека другите механизми (хиерархија, поделба на задачата, алгоритми), треба да ја инкорпорираат оваа улога, а тоа е местото каде што се одвиваат операциите во однесувањето.

Примери за сложени распореди:

Распоред за производство, распоред за транспорт на средствата, планирање на проекти, временски диспаритет; (време за купување суровини и материјали, кое е подолго од времето на испорака).
Логистичките компании имаат потреба од распореди за камиони и возачи, пред да биде позната нарачката за транспорт. Кој производ ќе се товара во кој камион? Со која брзина се движат камионите, дали има сообраќаен метеж?
Луѓето често работат во повеќе проекти истовремено; тие имаат потреба да ги резервираат капацитетите уште пред да започнат активностите.
Брзина и поле на хемиски реакции (при транспорт на хемиски средства, отрови, разни хемикалии изложени на топлина, притисок, храна со ладилници).
Одговорност за исполнување обврски поврзани со време (состаноци, договор за време на испорака.

Пренесување на тајни информации.

Одржување на точните распореди, флексибилност на време од страна на клиентите, опции, можности. Информациската непристапност и толкувањето, бараат од човечките распореди да бидат вклучени во процесот на планирање[140].
Индивидуално планирање на ефикасноста на задачата и когнитивните модели на планирање, покажуваат како се однесува решавањето на проблемите, планирањето и обработката на информациите. Неколку пристапи во распоредот биле инспирирани
од начинот на кој луѓето решаваат проблеми во приватниот живот, како што се: правење шопинг листа, планирање на одмор или играње шах. Овој модел е земен за толкување на начинот на кој се контролира обработката на човековата информација и ги снабдува обрасците со суштински врски помеѓу знаење, евалуација и акција.
За да се справат со сложеноста, луѓето применуваат: хиерархија на апстракција, хеуристика, скрипти и опортунистичко планирање. Постојат сличности и разлики помеѓу планирањето за себе наспроти планирање за другите.
На пример, според Хејс-Рот, изборот на стратегијата за планирање, зависи од три варијабли: проблематичните карактеристики, експертиза и индивидуални разлики.
Fransoo и Wiers (2006) [141]покажаа дека комплексноста на планерите и активностите се зголемуваат со сложеноста и бројот на спроведени акции. Ова наоѓањето е прилично интуитивно, но е во спротивност со разумот што води

[140] https://www.researchgate.net, The imlpications of fit between planning environments and manufacturing planning and control methods, Patrick Jonsson, Aug 2003
[141] https://www.researchgate.netScheduling the scheduling task: a time-management perspective on scheduling, Jose Larco, Jan Fransoo and Vincent Wiers (2007)

до сложеност и ментално преоптоварување и на тој начин, потпирање на рутински одлуки. Иако временскиот притисок резултира во зголемување на перцепираниот обем на работа, операторите работат со константно ниво на напор и намалување на бројот на закажани задачи. Експертите користат повисоко ниво на апстракција и повеќе расудување, од врвот надолу. Индивидуалните разлики доведуваат до разлики во стратегии и ставови за задачи со проблематична структура.

Покрај тоа, овие промени со текот на времето се зголемуваат. Иако планирањето може да биде олеснето со софтверски платформи, беа пронајдени неколку недостатоци: комплетен комбиниран детален распоред, кој беше преголем за да се ревидира од страна на луѓето (нумеричка комплексност), и затоа беше преземен авторитетот на локалните менаџери.

Во овој труд, направено е подробно истражување, и од сите софтверски алатки за изработка и управување со распореди кои се на располагање, главно се користат конвенционалните уредувачи за текст (како што е MS Word) или пак тие за табеларно работење (пр. MS Excel). Специјализираните cloud решенија за оваа намена најчесто се со плаќање на лиценци, но постои една софтверска платформа, која е многу добро рангирана а во исто време нуди и бесплатен пакет, доколку се користи за потребните интерни рамки во една организација (пример EYPM или слично). Сервисот се вика Sling и може да се најде на следната адреса: https://getsling.com/[142]

Пример во деск итражувањето е Сиетлската полиција 911 Центар, која е примарна одговорна точка за јавна безбедност (ПСАП) за итни повици поставени во градот Сиетл. Повиците за пожар или медицински одговор се доставуваат до Центарот за аларм во Сиетл. Центарот се справува со околу 900.000 повици годишно и е работи 24 часа дневно, 365 дена годишно.

Обработка на повици

Кога ќе го повикате 911, диспечер за полициски комуникации, го проценува вашиот повик и одредува кој тип на одговор е потребен. Тие ги внесуваат информациите за повик во системот за компјутерски информации, (CAD) кој го насочува повикот до соодветниот сектор за распоредување.

Испраќање

Друг диспечер од полициска комуникација, исто така познат како радио диспечер, комуницира со првите реагирачи во оваа област. Кога повикот е внесен во CAD системот, радио диспечерот веднаш се известува за дојдовен повик и ги испраќа расположивите ресурси. Радио диспечерот одржува контакт со единици на теренот и го координира одговорот на специјалните единици како K.9., S.W.A.T, воздушна поддршка за меѓусебна помош и детективи.

Мисијата на полицискиот оддел е брзо и професионално да одговори на сите барања за услуга за градот; да обезбеди професионално испраќање, известување и комуникациски услуги за Секторот; и да го олесни известувањето за помали инциденти преку телефонски и онлајн системи.

Приоритетите на полицискиот оддел се:

[142] https://getsling.com/

1. Итни случаи - Примарниот фокус е брзо да се одговори на итните барања за сервисирање, без оглед на тоа како тие се примени, правилно да се прикажат барањата на граѓаните, да се насочат кон правилниот центар за испраќање и ефикасно да испратат ресурси за решавање на итни случаи.
2. Известувања на одделот за комуникации - вториот приоритет е да се оперираат странични и комуникациски системи кои овозможуваат да се известат службениците од одделот за специфични информации за мисијата на база на 24/7/365 и да се извести јавноста за одредени состојби.
3. Не итни случаи - третиот приоритет е да се одговори на итните повици и да се упатат повици за испраќање, доколку е соодветно.
4. Извештаи – четвртиот приоритет е да се земат соодветните полициски извештаи преку телефон или упатување до системот за онлајн известување.
Пет совети за креирање на работна распоред за полициска служба[143]

Заклучок:

Без соодветна тимска комуникација, работниот распоред за деловното планирање, особено во компании 24/7/365, брзо се распаѓа. Без разлика дали менаџерот е одговорен за помагање на цела единица која мора да работи беспрекорно или е вклучен во локален оддел кој има тим од 10 вработени, тешкотиите во распоредувањето може да предизвикаат големи проблеми.
За среќа, постојат правила во менаџментот за користење на времето и ресурсите што можат да се преземеат за да се направи распоредот што поедноставно и посигурно.
Исто така постојат повеќе софтверски платформи и сервиси со кои планирањето на распоред станува автоматско и лесно, сепак со посебно внимание за човечките ресурси кои не се машини.

Литература:

1. Т.Кралев, Л.Наумовска, *Менаџмент*, Европски Универзитет РМ, Скопје, 2008г.,
2. Л. Наумовска, *Менаџмент на човечки ресурси*, Европски Универзитет РМ, Скопје, 2008г.,
3. https://getsling.com/
4.https:// crewapp.com/ Posted on September 8, 2017 by Kristin Proctor
5. https://www.researchgate.net, The imlpications of fit between planning environments and manufacturing planning and control methods, Patrick Jonsson, Aug 2003
6.https://www.researchgate.netScheduling the scheduling task: a time-management perspective on scheduling, Jose Larco, Jan Fransoo and Vincent Wiers (2007)

[143] https:// crewapp.com/ Posted on September 8, 2017 by Kristin Proctor

Д-р Зоран Крстевски
Е-маил: zkastrofilozof@yahoo.com

ЕТИЧКИТЕ АСПЕКТИ НА КОРПОРАТИВНАТА ОДГОВОРНОСТ

АПСТРАКТ
Етичко-економските прашања предизвикуваат исклучително големо интересирање, а етиката во економијата понуди некои од најмодерните етички согледби и норми за современото човештво. Деловната етика се наметна како мошне значајна гранка на економијата, која на деловните луѓе им наложи обврска да донесуваат одлуки кои според целите и вредностите се добри за целокупното општество.
Се прави разлика помеѓу традиционалната и современата деловна етика, каде во првата јасно се гледа разграничувањето помеѓу класичните категории како што се среќата и моралната одговорност, доброто и злото, слободата, додека во современата сфера на деловната етика е припоена клучната етичка категорија – корпоративна одговорност.
Општествено одговорен начин на однесување е претпоставка на однесување на секоја компанија, која се обврзува на почитување и полна примена на етичките принципи, норми и уверувања. Концептот на општествената одговорност денес најчесто се поврзува со поимите на корпоративната одржливост и корпоративното граѓанство. За концептот на корпоративната одговорност се врзуваат повеќе поими: етичко работење, корпоративно граѓанство, корпоративен одржлив развој, а во последно време е се повеќе присутен терминот корпоративно општествени перформанси.

Клучни зборови: деловна етика, економија, корпорации, одговорност, безбедност.

ABSTRACT
Ethical-economic issues cause extremely great interest, and ethics in the economy offers some of the most modern ethical insights and policies of modern humanity. Business ethics has been imposed as a very important branch of the economy, which gave obligation to business people to make decisions that, according to the goals and values, are good for the entire society.
A distinction has been made between traditional and contemporary business ethics. The traditional ethics makes clear distinction between classical categories such as happiness and moral responsibility, good and evil, as well as freedom, while the corporate responsibility is the key ethical category which has been attached to the contemporary sphere of business ethics.
A socially responsible mode of behavior is the premise of every company's behavior, which commits itself to respect and fully apply ethical principles, policies and beliefs. The concept of corporate responsibility encompasses many terms like ethical work, corporate citizenship, corporate sustainable development, and lately the term corporate social performance has been increasingly used.

Key words: business ethics, economy, corporate, responsibility, security.

ВОВЕД

Во економијата е главен стремежот кон успех и заработувачка. Меѓутоа, погрешни се мислењата дека тоа води кон негирање или заборавање на моралните принципи, односно дека успех може да се постигне само со отфрлање на етиката, т.е. дека во деловниот свет треба да се постапува без почитување на моралот и со измама. Тоа не е точно, современите погледи на моралот инсистираат токму на големото значење на строгата етичност во економските односи. Деловноста претставува основна грижа за успешно спроведување на економијата, таа е амбиција добро да се води економијата и да се постигне успех. Во нејзиниот домен спаѓаат: економичност, дух на бизнисот, посветеност и добро водење на економската дејност.
Етиката во економијата се однесува на моралните принципи, вреднување и однесување во разни области. Тука спаѓа една општа етика на односите во деловниот свет и меѓу деловните партнери. Има и низа посебни етики: етика на трудот; етика на конкуренцијата; етика на квалитетот на производството и на производите (да бидат многу добри и соодветно ефтини, да не се повредува средината, да не се возбудуваат моралните чувства на заедницата, да не се прави штета на моралниот развиток на децата и др.); етика на односите во приозводството; етика на раководењето во економијата; етика на маркетингот; етика на рекламата и сл. Економијата и економската етика, во чиј домен спаѓа и деловната етика се во центарот на современата етичка ренесанса на човештвото – кое препорачува постојана активност, унапредување на знаењата, учење, вложување, ефективност и мотивација за поголем напредок на општеството, компаниите и сите чинители на работните процеси.

1. Деловна етика

Деловната етика не е нешто ново. Таа е срцевина на економската мисла и дејност откако човекот ги произведува условите на својот живот. Денес интензивирањето на улогата и значењето на деловната етика се случува во време на глобализацијата и брзиот развој на технологијата, како и се поизразената економска и еколошка криза.
Деловната етика се однесува на моралните принципи, вреднување и однесување на полето на остварувањето на примарните задачи во економијата, како што се пронаоѓање на добра област за дејствување и вложување; заживување; добро искористување и ширење на капацитетите; добро водење на компанијата, што резултира со остварување заработувачка, придонес за општеството и задоволни вработени, клиенти (потрошувачи). Во доменот на деловната етика присутно е прашањето: дали може ли да се воспостави одредена врска помеѓу моралното работење и моралното однесување? Дали секое морално работење нужно станува и помалку успешно работење? Одговорот на овие прашања е дека деловните луѓе имаат обврска да донесуваат одлуки кои според целите и вредностите ќе бидат добри не само за компанијата, туку и за целокупното општество. „Деловната етика настојува да го одвои доброто од лошото во работењето и според

нејзините критериуми се одредува правилното морално однесување во бизнис релациите“[144].
Деловната етика претставува целина на прифатливи форми на работење во компанијата и таа е одредена од следниве учесници: Клиенти (потрошувачи); други учесници на пазарното работење; законски прописи; интересни групации; јавно мислење; лични морални вредности и начела на секој поединец посебно. Тежнението кон материјално богатство и тенденцијата за бескруполозно експлоататирање на сепостоечкото, станаа силна движечка сила во современиот начин на живеење, потиснувајќи ги хуманиот императив и вредност на деловната етика и етиката воопшто.
Имено, пазарните правила и строгата ориентираност кон профитот отворија многу прашања како што се: Дали постои експлоатација на работната сила во земјите во развој, а која пред се има за резултат намалување на трошоците на работењето и зголемување на продуктивноста? Дали продажбата на производи кои го нарушуваат здравјето, како што се цигарите, спаѓаат во етичко работење? Дали маркетиншкото таргетирање на деца е етички дозволено работење? Која е улогата на деловната етика, тогаш кога се бара дупка во законот со цел да се избегне плаќање данок? Последно што етиката во овие и слични ситуации смее да си дозволи е да не постои корпоративна одговорност и со тоа да се загрозат слободата и правата на луѓето.

2. Корпоративна одговорност

Етичка одговорност подразбира доброволно усогласување на деловното работење со моралните и етички норми на заедницата. Тоа подразбира дека учесниците во трудот треба да го работат тоа што е морално правилно и праведно, без нанесување штета на општеството и другите. Во тој контекст, компаниите се должни да се придржуваат до пропишаните закони и етичките кодекси и во склад со истите да ги извршуваат своите деловни активности.
Авторката Вебер се занимавала со проучување на поврзаноста помеѓу општествената одговорност на претпријатието и деловните резултати, па истакнува 5 основни категории кои му носат корист на претпријатието[145]:
1) Зголемување на репутацијата на компанијата,
2) Мотивираност на вработените,
3) Намалување на целокупните трошоци во работењето,
4) Зголемување на приходите и раст на учеството на компанијата на пазарот,
5) Минимализација на ризикот во работењето што е поврзано со активностите на општествената одговорност на работењето.
Се смета дека глобалистичките трендови целосно ја редефинирале областа на одговорноста, поврзувајќи ја за корпоративните бизнис активности. Бидејќи токму корпорациите се главните носечки елементи во економијата, но и во неекономските дејности, тие се должни да ја преземат одговорноста за општествените, политичките, еколошките проблеми, како на национално, така и на меѓународно ниво. Се верува дека зачетник на теоријата за општествена

[144] Nevenka Popović Šević, Etički aspekti integrisanih marketinških komunikacija, Univerzitet Singidunum, Beograd, str.85.
[145] Manuela Weber, The business case for corporate social responsibility: A company - level measurement approach for CSR, European Management Journal, vol.26, No.4, pp. 247-261.

одговорност е Ендрју Карнеги, според него, принципот на доброчинство има за претпоставка побогатите членови на една заедница да им помогнат и да придонесат за оние кои се помалку среќни (болни, невработени, стари и сл.). Оваа етичка доктрина препорачува богатиот слој на заедницата да ги инвестира парите и за добродетел на преостанатиот дел од општеството. Врз потполно други основи се развива теоријата на познатиот економист Милтон Фридман. Теоријата на општествена одговорност во работењето, тој ја базира врз постулатите што овозможуваат максимализација на профитот, бидејќи според него „постои една и единствена одговорност кон стопанството – во името на зголемување на профитот постојано да се користат неговите ресурси и енергијата, но само под услов да се игра по правилата на отворената и слободна конкуренција, без измами, лаги и проневери и сл“[146].

Фридман го застапува ставот дека основна идеја на секое деловно работење е ефикасно производство, така што решенијата за социјалните проблеми треба да се побараат кај владините служби.

Најчести примери на етички проблеми во работењето се врзани со дилемата околу тврдиот курс во профитабилниот интерес на компанијата што поефективно да се наметне на пазарот од една страна, и за тоа што компанијата го смета за етичко работење, од друга страна.

Етичките проблематики во современите бизнис релации може да ги поделиме во четири групи:

1. Судир на интереси – присвојување одредени добра на компанијата поради сопствени интереси, подмитувања и примање мито во процесот на извршување на работните задачи, давање посебни услуги (оддавање информации со намера во името на личниот интерес да и се наштети на спротивната страна);
2. Чесност и отвореност: свесно и намерно нанесување штета на клиентите (потрошувачите), вработените, јавното мислење, конкуренцијата – користејќи се со двосмислено информирање, изнудување, присила или која било друга форма на работна дискриминација, се со цел да се сочува деловната позиција на пазарот;
3. Комуникација – тука вбројуваме давање лоши информации за карактерот/својството на одреден производ или услуги кои компанијата комерцијално ги пласира на пазарот, измамувачко рекламирање на производи и услуги, лажна продажба, непотполно давање информации за штетното дејство на одредени производи (најприсутно кај лековите и лековитите средства), измамувачки корпоративни комуникации/рекламирање кое е на штета на конкуренцијата.
4. Деловни односи – злоупотреба на деловниот авторитет, оддавање деловни тајни, оневозможување извршување на деловните задачи, присилување на другите на неморални дејствија (мобинг).

Од друга страна, моралната коректност произлегува од практикување на следниве фактори:

а) Добри етички навики чие почитување и придржување се смета за елементарна култура на работењето,

б) Кодифицирани законски и подзаконски акти и уредби и

[146] Milton Friedman, Kapitalizam i sloboda. Novi Sad: Global book, 1997, str. 213.

в) Етички кодекси на одредени професии.
Со имплементирање на етичките кодекси јасно се прецизираат правилата и нормите на однесување на вработените. Многу од овие норми се ставени во кодекси (кодекс на лекарите, на новинарите, на сметководителите итн), а многу од нив се обичајни норми, кои се пренесуваат од еден дејственик на друг и така траат од генерација во генерација. Воведувањето етички кодекс не е гаранција за автоматско воспоставување морално однесување во некоја организација или професија. Кодексот се смета само како прв чекор кон етички настојувања кои подразбираат и следни активности: транспарентност, квалитет, почитување на добрите деловни обичаи кон деловните партнери, пренесување на етичките начела за поефикасно работење, постојана реафирмација на етичкиот кодекс и последици кои ќе бидат во случај на негова непримена.

ЗАКЛУЧОК

Етиката претставува темел, врз кој цивилизираното општество е изградено. Барањето на „моралната економија“ е да покаже дека е рационално, корисно и продуктивно да се биде морален во извршувањето на работните задачи. Искуствата покажале дека поединец, претпријатие, бизнис сектор или општество, кое ги игнорира етичките норми и вредности, е осудено на неуспех, порано или подоцна. Доколку корпорациите сакаат здрава клима, во кои би можеле да работат профитабилно и во иднина, тогаш тие мораат да преземат конкретни напори што ќе осигураат долгорочна одржливост. Од долгорочен интерес на претпријатијата е да ја вклучат општествената одговорност и да се водат според етичките кодекси во своите деловни одлуки, практики и активности.
Појавата на неетичко корпоративно однесување автоматски ги зголемува трошоците на општествената заедница и ги намалува количините на нејзините богатства. Типичен пример за тоа се последиците од еколошко загадување или неетичкиот вид на огласување во разните медиуми, после кои активното граѓанство бара спроведување на повеќе регулации. Зголемената регулација понатаму претпоставува интензивен ангажман на државниот апарат со што се зголемуваат неговите трошоци. Затоа, од исклучителна важност е етичките аспекти да бидат составен дел на корпоративното работење.
Современите корпорации, помеѓу другото се должни да развијат и стратегии за редуцирање на корпоративните безбедностни ризици и закани. Овие цели се во функција на унапредување на безбедностните капацитети во деловното работење, подигнување на интегритетот на компаниите, развој на информационата безбедност, заштита на лични податоци и деловна тајна.
Како заклучок ќе ги наведеме и зборовите на еден од најзначајните современи етичари Питер Сингер: „Етиката не претставува некој идеален систем кој во теоријата е возвишен, додека во практиката е слабо присутен. Токму обратното: етичкиот суд кој во пракса не е добар мора и во теориска смисла да биде спорен, бидејќи вистинската смисла на етичкото судење е да го раководи практичното постапување“[147].

[147] Piter Singer, Prakticna etika, Beograd, Signature, 2000, str. 2.

Библиографија:

1. Димитријевић, Наташа. Пословна етика, друштвена одговорност и конкурентска предност предузећа. дис. Београд: Алфа БК универзитет, 2016.
2. Ferrel, O, G. Hirt, G. Business Ethics and Social Responsibility, Boston: Irwin Mc Graw-Hill, 2000.
3. Friedman, Milton. Kapitalizam i sloboda. Novi Sad: Global book, 1997.
4. Ratkovič, Njegovan. Poslovna etika, Novi Sad: Fakultet tehničkih nauka.
5. Singer, Piter. Prakticna etika, Beograd: Signature, 2000.
6. Singer, Piter. Uvod u etiku, Novi Sad: Izdavačka knižarnica Zorana Stojanoviča, biblioteka Levijatan.
7. Šević, Popović, Nevenka: Etički aspekti integrisanih marketinških komunikacija. dis. Beograd: Univerzitet Singidunum.
8. Темков, Кирил. Етиката днес. София: Университетско издателство „Св. Климент Охридски“, 2006.
9. Темков, Кирил.Етика. Скопје: Епоха, 1998.
10. Weber, Manuela. The business case for corporate social responsibility: European Management Journal.

Вонр.проф.д-р Фердинанд Оџаков
Лимонка Василева-Гоцевска

КОРЕНИТЕ НА ДЕТЕКТИВСКАТА ДЕЈНОСТ

АПСТРАКТ
Оваа професија ги влече своите корени од таканаречените „ловци на криминалци за парична награда„, кои се појавуваат во Англија кон крајот на 17-от век, а е регулирана со Законот за друмски разбојници, со кој е предвидена можност за распишување парични награди за гонење на криминалци. Подоцна оваа пракса била применета и на територијата на САД.
Англија е лидер и во формирањето на друштвата за приватно гонење, кои функционирале во 18-от и 19-от век, чија основна цел била нудење помош во пронаоѓање на осомничени, а се распишувале и награди за добивање информации кои помагале во расветлување на криминалните дејствија, карактеристични за тој период.
Историски гледано, на некој начин, на Ален Пинкертон (Allan Pinkerton) се гледа како на креатор на детективската дејност со основањето на Пинкертонова Национална Детективска Агенција. Агенцијата нудела лепеза на услуги, од тајни истраги, расветлувања на злосторства, до физичко обезбедување.
Својот најголем подем детективската дејност го бележи во почетокот на дваесеттиот век, како резултат на економскиот галопирачки раст на САД и создавањето на средната класа, како најчест корисник на услугите на приватните детективи.

THE ROOTS OF DETECTIVE OCCUPATION

APSTRACT
This profession pulls its roots from so-called "hunters of criminals for a monetary reward" that appeared in England towards the end of the 17th century, and was regulated by the Law on Road Robberies, which provided the possibility of announcing cash rewards for prosecution of criminals. Later this practice was applied to the territory of the United States.
England is also a leader in the establishment of private prosecution companies that operated in the 18th and 19th century, whose main purpose was to provide assistance in finding suspects, and awards were also issued to obtain information that helped in clarification of criminal activities, typically for that period.
Historically, in a way, Allan Pinkerton is seen as the founder of the detective occupation with the establishment of the Pinkerton National Detective Agency. The agency offered a range of services, from secret inquiries, to crimes' clarification, to physical security.
Detective occupation noted its greatest rise in the early twentieth century, as a result of the galloping economic growth of the United States and the creation of the middle class as the most common user of services of the private detectives.

ВОВЕД

Покрај конвенционалните државни безбедносни структури, во модерните општества се наметнуваат и приватни „актери“ за обезбедување, кои несомнено наметнуваат намалување на ингеренциите на полицијата во јавниот сектор. Безбедносните побарувања во современото општество стануваат се поголеми, а со тоа и трошоците за зголемување на јавната безбедност, кое како такво е дополнително оптоварување на државниот буџет. Како резултат на оваа појава, дел од работата на јавната безбедност неизбежно ќе се префрли во приватниот сектор за безбедност. Во денешни услови може да се каже дека епицентарот на активности на полицијата најчесто се репресивни, односно реакции следствени на криминални дејствија, опасни настани, а во јавниот сектор дејствува превентивно само во поопшта смисла.

Соработката на државниот и приватниот сектор мора да почива на правни и професионални аспекти. За примена на какви било средства за присилба, приватните безбедносни чинители се законски обврзани да ги информираат овластените полициски органи, но исто така и за извршување на наредби кои доаѓаат од овластените полицајци. Полицијата има надзорна функција над приватниот сектор за безбедност, што значи врши контрола над законитоста на нивната работата, како и усогласеноста со правните стандарди во оваа област. Државата индиректно се појавува како гаранција за приватната безбедносна сфера. Неминовно односите меѓу приватното обезбедување и полицијата најмногу зависат од индивидуалните перцепции и примена на стекнатите искуства. Во некои развиени држави преовладува мислењето дека државната полиција е одговорна за јавната безбедност на национално ниво, па оттука и ставот дека, обврска на државата е да обезбеди генерално високо ниво на безбедност, а со тоа не се дозволува приватниот сектор да стане нејзин конкурент. Приватното обезбедување е само додаток на национална безбедност, гарантирано од државата. Сепак, може да влијае глобално на безбедноста преку своите напори за надминување на разликите помеѓу приватниот и јавноста интерес на заедницата. Интеграција на приватниот безбедносен сектор во системот на национална безбедност може да ги намали ризиците од криминализација и злоупотреба. Транзиција, односно предавање на одредени ингеренции и обврски од државната полиција на приватни безбедносни актери, и одрекување од довчерашното традиционално загарантирано право на полицијта, секако поминува низ еден комплексен процес, следен со многу лични интерпретации и застапување интереси. Понатаму, имплементирање на закони, прописи, надлежности, особено во пост-авторитативните, пост-конфликтните и општествата во транзиција.

Од комплетна превентивна и репресивна улога во безбедносната рамка, полицијата веќе не е сама на теренот како единствен чинител во јавната безбедност. Тука се приватните актери, кои се јавуваат во улога на физичко обезбедување на имоти и лица, бизнис поддршка, детективски работи и други услуги во полето на приватното обезбедувања.

Во Р. Македонија, приватните агенции за обезбедување своите корени ги бележат од 1994 година. Дваесет и четири години подоцна може да се каже дека и покрај огромнот напредок на ова поле, голем број стручни трудови и имплементирање на Закони, сеуште се актуелни дебатирања за ингеренциите,

прифатеноста од народот и "интер" соработката помеѓу државните и приватните структури.

1. Појава, причини и дефинирање

Самиот трансфер на државната сопственост во приватна, растот на приватниот капитал, зголеменото чувство на несигурност кај граѓаните и неможноста на државните структури да ги заштитат можните цели на напади, се повеќе од причини за појава и развој на приватниот сектор за обезбедување. Во исто време, полицијата е оптоварена со широк спектар на интервенции и решавање на безбедносни проблеми со помало значење, со што се дефокусираат во однос на сузбивање на посериозни видови криминалци**.**

Историски гледано, приватизацијата на безбедноста како стар феномен е присутен низ различни форми. Како еден од „резултатите" на хиперглобализацијата, приватната безбедносна индустрија најнапред се јавува во развиениот Западен свет, а потоа и пошироко. Своја примена најде и дефиницијата на германскиот социолог Макс Вебер: „државата со монопол на употреба на сила за одржување на поредокот и заштитата на имотот и безбедноста на поединците и на групите"[148]. Освен во националните граници, приватниот безбедносен сектор стана видлив и значаен и во меѓународен контекст, па така развиените демократии му дадоа голем легитимитет, и како таков стана комплементарен елемент на националната безбедност.

Причинителите за тоа се бројни, но две може да се издвојат како клучни: Прво, главниот фокус е на јавниот безбедносен сектор, кој сè уште минува низ реформски процеси и доживува осцилации; и второ, како и за секој бизнис сектор, отворањето непријатни прашања понекогаш носи ризик од губење на угледот, кој пак е основа за стекнување нови клиенти[149].

Како што наведува Кесиќ[150] - во литературата се разликуваат два основни пристапа во дефинирањето на приватниот сектор на безбедноста, односно поширок и потесен. Според пошироко гледиште: „приватниот безбедносен сектор би можел да се дефинира како собир на организираните облици за дејствување на доброволно и комерцијално насочување на недржавните чинители, чија основна дејност вклучува спротивставување на криминалното однесување". Потесното гледиште пак, би можело да се дефинира како: „збир на правно втемелени дејности, од професионалниот тип, надвор од рамките на надлежностите на државните органи, кои што се организирани поради давање одредени услуги заради лична заштита и имотна сигурност на граѓаните и собирање информации по барање".

2. Глобална организациска структура

Дефиницијата со која организацијата како систем од луѓе и средства кои се поврзани со цел да остварат некои заеднички цели, упатува на „процес на дефинирање на работите кои е неопходно да се реализираат, како и формирање на структура каква што е потребна за остварување на задачите со

---

[148] Max Weber, " Politics as a Vocation"-(1918), defines the state as a "**human community** that (successfully) claims the monopoly of the legitimate use of physical force within a given territory."

[149] Б. Ванковска State-Building and Privatisation of Security in Macedonia, Скопје 2016

[150] З. Кесиќ, Приватни сектор у контроли криминалитета, Београд, 2009

кои се постигнуваат поставените цели"[151]. Оттука за да се дефинира една организациона безбедносна структура, неопходно е да се знае кои се нејзините задачи и цели, како и реално согледување на теориските поставки. Секако не смее да се занемарат потребите и капацитетите.

За разлика од традиционалните, современите теории за организација, повеќе се насочени кон принципите, методите, критериумите и правилата на градење и развој на организационите структури. Со цел ефективна организациска структура и примена на соодветните принципи, критериуми, методи и правила, во процесот на обликување на елементите на секторот за безбедност мора де се внимава на:

- Обликот и бројот на организациони единици;
- Групирање и разграничување на обврските и ингеренциите;
- Распоредот, менаџерскиот тим и службениците за безбедност;
- Меѓусебното поврзувањена различни организациони единици.

За утврдување на носечките функции и елементи во безбедносните структури, како критериуми за идентификација би требало како насока, а врз основа на општите ставови[152] да се користат прашањата:

- Во кои области е потребно совршенство при извршувањето на безбедносните работи за да се остварат целите на корпоративната безбедност;
- Кои се "најосетливите" (fragile) области – т.е. областите во кои лошото функционирање на секторот за безбедност би причинле сериозни штети, па дури и би го загрозиле опстанокот;
- Кои вредности се круцијални за корпорацијата.

Останатите активности би ги ставиле во категорија „секундани", без разлика на значајност, материјалност и персонален ангажман. Секако, и тие мора да бидат анализирани, организирани и сместени во структурата, но најголемо внимание треба да му се посвети на оние активности кои се суштински за успехот на работната стратегија и достигнување на целите. Правило е дека треба прво клучните активности да се идентификуваат, дефинираат, организираат и сместат на централно место во организациската структура.

3. Приватната безбедност во регионален контекст, Југоисточна Европа

3.1. Правен третман и механизам на контрола

Во текот на последната деценија, голем број фактори (високата стапка на криминал, корупција во јавните институции, мулти-етничка недоверба и нетрпеливост) влијаеа на зголемувањето на побарувачката на услуги за приватна безбедност во земјите на Југоисточна Европа. Овој регион поминал низ една од најбрзите приватизации во целиот свет заарадди преминот од состојба на потполно отстуство на услугата на приватна безбедност кон крајот на 80-тите години до состојба која е денес, односно, оваа индустрија се јавува како голем работодавач и овозможувач на услуги за безбедност[153]

[151] Стратегијски менаџмент, М. Јовановиќ, Београд, 2001
[152]Management – Tasks, responsibilities, Practice, Harper Busines, P. F.Drucker, USA, 1993
[153]И.Димитријевиќ, Упоредни приказ сектора приватне безбедности Југоисточне Европе, Београд, 2006

Вообичаено, компаниите за приватна безбедност ги нудат услугите: физичко обезбедување на деловни простории, фабрики и други државни згради, пратење на транспортот на вредности и пари, но сепак некои од земјите во регионот имаат помал пазар на приватно обезбедување, кој најчесто е насочен кон услуги на физичка заштита, а поретко приватно обезбедување на приватни куќи.

Многу важен податок е дека во Југоисточниот регион преовладуваат домашните компании за приватна безбедност, заради законските ограничувања со кои би се соочиле меѓународните компании во случај. Делумна причина за тоа се ограничувањата за вршење на оваа дејност на меѓународни компании во многу земји. Во земјите кандидати за членство во ЕУ, сепак, пазарот на приватна безбедност е отворен кон странската конкуренција и одреден број меѓународни компании веќе го имаат пронајдено своето место во посочените рамки[154].

Од особена важност за земјите од Југоисточна Европа е да учат од своите меѓусебни искуства, кога станува збор за функционирањето на компаниите за приватна безбедност, како и да ги применуваат законските насоки, регулативи процедури од страна на Европската Унија.

Табела 1: Компаративна анализа на секторот за приватна безбедност во рамките на Југоисточна Европа[155]

Земја	Клучни аспекти	Препорака
Албанија	• Релативно мала и неразвиена приватна безбедност; • Некои компании работат без дозвола, со што се поткопува регулативата на системот; • Несоодветни врски помеѓу компаниите и политичките партии	1. Потреба од ревидирање на законодавството со цел обезбедување соодветно вооружување преку соодветна обука за истото.
Босна и Херцеговина	• Комплексна состојба поради децентрализираната власт во земјата; • Двојно законодавство, двојни правила за компаниите за приватна безбедност; • Голем број физички лица што работат нелегално;	1. Воведување национално законодавство; 2. Потребно е компаниите да работат на саморегулирање низ создавање соодветни правила на однесување

[154] П. Петровић, Приватизација безбедности у Србији, Безбедност Западног Балкана бр. 4, 2007

[155] Приватните безбедносни компании во ЈИЕ – развој и регулирање, Приватниот безбедносен сектор во компаративна перспектива, Приватна безбедност во XXI век, Искуства и предизвици, Скопје 2016 година

Бугарија	• Приватна безбедност е најразвиена во регионот; • Почетоци на поврзаност на компаниите со групи за организиран криминал; • Нелегално обезбедување на услугата (во помал %); • Присутна конкуренција помеѓу полицијата и компаниите за приватна безбедност;	1. Да се искорени натпреварот помеѓу полицијата и компаниите за приватна безбедност; 2. Законодавниот орган да биде проактивен во истражувањето на секторот за приватна безбедност (особено зголемување на парламентарната контрола).
Хрватска	• Приватната безбедност се развива во последните десет години; • Секторот се зголемува за 10% на годишно ниво; • Постои можност за поврзаност на компаниите за приватна безбедност со криминални групи;	1. Потребно е поедноставување на законската структура
Македонија	• Приватната безбедност се развива од 1994 година; • Мала индустрија во процес на експанзија; • Не постои можност за работа на странски фирми од овој домен во земјата; • Компаниите за приватна безбедност, во одреден домен имаат кадар кој потекнува од поранешни полициски и воени единици;	1. Потреба од надворешна контрола во спроведувањето на законот во земјата; 2. Соодветни безбедносни проверки на компаниите; 3. Унапредување на работната пракса и подобро регулирање на употребата на оружје преку соодветни обуки.
Србија	• Најпроблематична ситуација во регионот; • Поврзаност на компаниите со групи на организиран криминал; • Можност за злоупотреба на службеното оружје за приватни цели;	1. Потребно е да се усвои систем за издавање на дозволи за оваа дејност со цел да се елимнинираат непрофесионалните делови од индустријата; 2. Прифаќање на меѓународни правила во овој домен.

Црна Гора	• Секторот се развива кон крајот на деведесетите години; • Постои систем за издавање дозволи, но не е спроведен во целост; • Службениците во полиција остваруваат двојна функција, државна и приватна по завршување на работното време, што предизвикува судир на интереси.	1. Поголема транспрарентност во регулирањето на компаниите за приватна безбедност и воведување прецизни програми за обука.
Косово	• Приватната сопственост се појавува со меѓународната интервенција во 1999 година. Под контрола на ООН во Косово; • Високо ниво на конкуренција помеѓу индустријата за приватна безбедност и Косовската полиција и служби;	1. Потреба од ефикасен систем на обука и безбедносна проверка; 2. Потреба од воспоставување јасна линија помеѓу државниот и приватниот сектор

4. Меѓународни документи и организации како имепартив.

Европската унија нема усогласена правна рамка со која се регулира приватниот сектор за безбедност, но сепак располага со широко прифатени стандарди, кои претставуваат основни насоки и процедури, коишто земјите аспиранти (ЈИЕ) треба да ги усвојат со цел, олеснување на патот кон Европската унија.

Во таа насока би го споменале **Монтре Документот - Montreux Dokument**[156], кој е на заедничка иницијатива на Швајцарија и Меѓународниот комитет на Црвен крст, покрената во 2006 година резултат, а ги поставува стандардите за функционирање на компаниите за приватно обезбедување. Овој документ потсетува на обврската на државата, компаниите за приватна безбедност и нивните вработени да работат во согласност со меѓународното право, во услови кога компаниите на приватното обезбедување, од која било причина, се ангажирани во текот на вооружен судир[157].

Според Montreux Dokument-от, компаниите што вршат приватно обезбедување се обврзани да дејствуваат во согласност со меѓународните хуманитрани или човекови права што се пропишани во државните, односно националните закони (кривично право, закон за данок, имиграциски закон, работни права и сл). Доколку приватниот сектор за безбедност лоцира недостаток на регулативи во конкретна област, се пристапува кон донесување дополнителни закони за тие потреби.

Можеме да констатираме дека приватно обезбедување во меѓународен контекст сепак е релативно уредено со законодавството на Европската унија, првенствено поради учеството на приватниот сектор за безбедност во единствен европски пазар, услуги, слобода на движење и сл.

---

156 https://www.icrc.org/eng/assets/files/other/icrc_002_0996.pdf

157 Joanna Spear, The Political Economy of Private Military Companies, Private Sector Activity in Armed Conflict, Fafo 2006. http://www.fafo.no/index.php/nb/zoo-publikasjoner/fafo-rapporter/item/market-forces

Дополнително, Европскиот суд за правда има надлежност за прашањата поврзани со приватното обезбедување и активности поврзани за регулирање на единствениот пазар на Европската унија. Понатаму, Советот на Европа влијае врз приватниот сектор на безбедност низ бројни конвенции што ги усвојува, кои се однесуваат на заштита на човековите права и правото на владеење, по пат на Европски конвенции за човекови права и заштита на поединците во врска со автоматска обработка на лични податоци, како и препоракте за потреба од хармонизација на националните регулативи, кои се однесува на носење и користење оружје.

5. Приватното обезбдување и меѓународните мисии

Новите закани и ризици, наметнати од новите начини на војување и геостратегиски интереси, како и зголемениот број на жаришта, секако доведоа до недостаток и на воени капацитети кои се неопходни за логистичко, па и друго обезбедување. Оттука, големите дебати на таа тема доведоа до распространето учество на компаниите за приватно обезбедување, како на пример Blackwater од САД.

Европската унија и нејзините земји-членки се повеќе се потпираат на приватните изведувачи во мултилатералните операции, на пример:

- ЕУ има вработено приватни чувари за заштита на седиштето на ЕУПОЛ во Авганистан;
- За обезбедување на просториите на мисијата ЕУЛЕКС во Косово;
- Обезбедување на мисијата ЕУПОЛ во Демократска Република Конго и др.

Поради зголемената улога на компонентата за приватно обезбедување во операциите за заедничка безбедносна и одбранбена политика (ЗБОП), ЕУ и нејзините земји-членки, со приоритет треба да му пријдат и го разгледаат можното влијание што вооружените и невооружените безбедносни изведувачи можат да го имаат врз мисиите и постигнувањето на целите на мисиите. Досегашните искуства покажуваат дека потенцијалните негативни ефекти се движат од намалената демократска одговорност и владината контрола на перцепциите на неказнивоста и несигурноста на изведувачите меѓу цивилното население во земјите домаќини. Засега нема решение за овие проблеми, а за многу влади, предностите за ангажирање на приватни безбедносни изведувачи, како што се потребите за итно пополнување на капацитети и недостаток на персонал, економичност и експерти по специјалност, ги надминуваат недостатоците. Со оглед на моменталните финансиски и персонални ограничувања на европските вооружени сили, веројатно е дека употребата на приватните компании ќе се зголеми уште повеќе. Затоа е неопходно да се развијат соодветни механизми за решавање на можните проблеми со таквата употреба, односно да се дејствува превентивно пред да се појават.

Во рамки на ЗБОП, ЕУ учествуваше во поеќе операции од 2003 година, во кои приватните изведувачи обезбедија широк спектар на услуги за да ги поддржат овие операции од разни причини, вклучувајќи ограничувања на војниците, недостатокот на специфични капацитети, финансиски ограничувања и развојни цели. ЕУ не го финансираше централно договарањето на приватните обезбедувачи за воените операции на ЗБОП до усвојувањето на механизмот АТЕНА во 2004 година. Сепак, нема формални ограничувања за вработување

на компаниите за приватно обезбедување за заеднички операции, а се појасно е дека ваквиот ангажман во ќе се зголемува. Придружните фактори се пренатрупаноста на националните вооружени сили, недостатоците на капацитети, ограничувањата на војниците и идеолошките преференции за надворешно извршување на неатрактивни функции. Во однос на воените операции, одлучувачките фактори на земјите-членки претпочитаат да обезбедат војници за воени операции, а не да ги употребуваат за помошни функции како што се заштитата на персоналот и средствата.

Регулативите и политиката на ЕУ одиграа клучна улога во промовирањето на националните и регионалните контроли во врска со обезбедувањето и извозот на разни воени и безбедносни услуги[158], но за жал не постојат заеднички прописи за приватните компании за обезбедување, регистрирани во ЕУ, како и за извозот од нивните услуги во странство. Во најдобар случај, постоечките контроли во рамките на ЕУ може да послужат како пример за разни механизми кои би можеле да се искористат за подобрување и регулирање на приватната безбедносна индустрија. Оттука произлегува потребата од понатамошни дискусии и координации околу:

- Заеднички упатства на ЕУ за вработување и користење на компаниите за приватно обезбедување;
- Заеднички критериуми на ЕУ за извоз на оружје;
- Регулирање на брокерското посредување;
- Техничка помош за ембарго на дестинации;
- Ембарга на ЕУ за воени услуги и приватни безбедносни служби.

Од понов датум е Усвоениот текст на ЕУ Парламентот за **Резолуцијата за Приватните компании за обезбедување во јули 2017 година**[159].

Главни црти на текстот:

На потреба од регулативна рамка на ниво на ЕУ укажаа и анкетите на Евробарометер според кои, граѓаните на ЕУ сакаат ЕУ да биде поактивна во областа на безбедноста и одбраната. Приватните безбедносни компании сè повеќе се ангажирани од страна на националните влади, не заоостануваат ниту воените, ниту цивилни агенции, кои не само на домашен терен, туку се јавуваат како чинител за поддршка во странство. Бројките покажуваат дека повеќе од 1,5 милиони приватни безбедносни изведувачи биле вработени во околу 40 000 приватни безбедносни компании во Европа во 2013 година, а овие бројки се во пораст.

Од витално значење е да се даде приоритет во воспоставувањето на јасни правила за интеракција, соработка и помош помеѓу полицијата и приватните безбедносни компании. Приватните компании за обезбедување играат важна комплементарна улога во помагањето на државните воени и цивилни агенции за затворање на јазот во потребните капацитети, креиран со зголемената побарувачката за употреба на силите во странство.

Операциите и активностите кои се извршуваат од страна на приватните компании во областите на конфликти треба да се ограничат на обезбедување

[158] http://www.consilium.europa.eu/showPage.aspx?id=1484&lang=en

[159] http://www.europarl.europa.eu/oeil/popups/summary.do?id=1497100&t=e&l=en

на објекти, логистичка поддршка и заштита на инсталациите, без нивно присуство во областите каде што постојат борбени активности. **Употребата на Приватните компании за обезбедување (ПКО), под никакви околности не може да биде замена за персоналот на националните вооружени сили.** ПКО мора да бидат свесни за локалните обичаи и навики, под никакви околности не треба да им се дозволи да учествуваат или да спроведуваат истраги.

Секое учество на приватните безбедносни компании во воените операции мора да биде оправдано, со јасно дефинирани цели кои можат да се верификуваат со опипливи индикатори, да имаат целосно детален буџет, времетраење на услугата (почетен и краен датум) и да бидат регулирани со строг етички код.

За државите да имаат корист од предностите што ги нудат ПКО и да бидат сигурни во нивната одговорност, треба да се воспостави правна рамка со задолжителни регулаторни механизми и механизми за следење на меѓународно ниво за да се регулира нивната употреба и да се обезбеди адекватна контрола врз нивните активности.

Резолуцијата ја нагласува и важноста на парламентарниот надзор над државната употреба на ПКО од страна на земјите-членки. Во таа наскоа се истакнува дека во конфликтни средини, вработувањето на ПКО за одредени должности може да има негативни несакани ефекти по ЕУ, особено за нејзината легитимност, во коалиција со вооружените актери во конфликтна област, со негативни реперкусии во случај на вооружени инциденти.

За регулирање на работата на ПКО се препорачува:

- Дека Комисијата подготвува Зелена книга со цел да се утврдат основните правила за ангажирање и позитивни практики;
- Креирање на специфични секторски ЕУ стандарди за квалитет, како и дефинирање на ПКО, пред да се воведе ефективно регулирање на нивните активности, бидејќи недостатокот на таква дефиниција може да создаде законски дупки;
- Советот без одлагање да додаде воени и безбедносни служби од страна на ПКО на Заедничката воена листа на Европската унија.

Од Комисијата се бара да развие ефикасен европски регулаторен модел, кој ќе има за задача:

- Да помага да се усогласат правните разлики помеѓу земјите-членки со директивата;
- Ре-евалуација, а со тоа да ги редефинира современите стратегии за соработка помеѓу јавноста и приватниот сектор;
- Поставување на високи стандарди за давателите на приватни безбедносни услуги во рамките на ЕУ или работа надвор;
- Да се обезбеди непристрасно известување за неправилностите и незаконитостите на ПКО и овозможи нивна одговорност за прекршоци, вклучувајќи ги и кршењето на човековите права за време на нивните активности во странство.

Што се однесува до САД, тие имаат долга историја во ангажирањето на приватни контрактори за поддршка на полициски мисии и воените

операции во странство. Денес САД овие компании интензивно ги ангажира во меѓународни интервенции за:

- Логистичка поддршка;
- Одржување и поправка;
- Управување со бази и изведувачи;
- Разузнавање и сослушување;
- Обука на воени и полициски сили;
- Реформа на безбедносниот сектор;
- Програми и чувари на безбедност[160].

Меѓутоа, широката употреба на вооружените чувари во воените интервенции е со кратка историја, тесно поврзан со влошувањето на безбедносните ситуации во Ирак и во Авганистан. Според Канцеларијата за одговорност на Владата на САД, главните причини за ангажирање на ПКО се:

- заштеда на пари;
- способност за брзо мобилизација и демобилизација на безбедносниот персонал;
- Ослободување на униформиран персонал за вршење офанзивни борбени операции[161]".

Како и во Европа, дополнителна причина се и политичките ограничувања на распоредувањето на воениот персонал во интервенции надвор. Првиот поголем пораст на вооружените безбедносни изведувачи на тој начин може да се забележи во Ирак по завршувањето на борбената фаза во април 2003 година. Тоа беше директна последица на одлуката на американската влада да ги ограничи своите војници на 300.000, и покрај фактот што лидерите на американската војска предвидуваа дека им се потребни 500.000 војници за успешно реализирање на задачие во Ирак[162]. Покрај тоа, во Ирак Министерството за одбрана на САД за првпат изјави дека обезбедувањето на безбедноста на цивилното население не е мисија на американската армија[163].

ЗАКЛУЧОК

Безбедноста, од која дел е и приватното обезбедување, е бенефит на денешното време, која има исклучително значење и улога. Секако, мора да се најде рамнотежа помеѓу безбедноста и слободата, односно да се изнајде/создаде средина, во која поединецот ќе се чувствува сигурно и слободно во исто време.

Ако го поставиме прашањето: Дали безбедноста и нејзиниот дисциплинарен развој се задача само на државата или и на приватните безбедносни компании?, секако ќе дојдеме до заклучок дека, државата е голем побарувач/клиент на услугите на приватно обезбедување и неговите

[160] A. Stanger, One Nation Under Contract: The Outsourcing of American Power and Future Foreign Policy , Yale University Press, 2009; Avant, Market for Force; Krahmann, States, Citizens and the Privatization of Security.

[161] Schwartz, The Department of Defense's Use of Private Security Contractors in Iraq and Afghanistan.

[162] US Senate Armed Services Committee, February 2003; E. Schmitt, 'Pentagon Contradicts General on Iraq Occupation Force's Size', New York Times, February 2003.

[163] M. Sassoli, 'Legislation and Maintenance of Public Order and Civil Life by Occupying Powers' The European Journal of International Law, Vol. 16, No. 4 (2005).

активности[164]. Исто така, ќе мора да се обезбеди правна и професионална имплементација на законите и пристоен живот на безбедносниот персонал.
Поради глобалните безбедносни случувања, приватната безбедност има многу предизвици и отворени прашања пред себе, кои може да бидат надминати со перманентна координација помеѓу теоретичарите, практичарите и државата. Односно, поголема поврзаност на теоријата и праксата во полето на приватното обезбедување, отворање на нови полиња за работа на приватното обезбедување, повисоко ниво на свесност, меѓусебна поврзаност и сл. Во однос на регулаторот, односно државата, пожелни се поинтензивно промовирање на приватното обезбедување, со цел граѓаните да ја сфатат важноста на безбедноста, идентификување на заканите на критичната инфраструктура и друга заштитени подрачја.
Неопходна е јасна правна рамка која ќе ја разграничи улогата на приватна и јавната безбедност во сите случаи , како и заедничките договори помеѓу полицијата и компаниите за приватна безбедност во чиишто рамки припадниците на полицијата и персоналот за физичко обезбедување ќе работат заедно.
Растот на потребата за ангажирање на вооружени безбедносни изведувачи во мисиите и операциите на ЗБОП (CSDP Common Security Defence and Policy), како и улогата на ПКО во мултилатералните интервенции, секако доведоа до интензивни размислувања и потреба за правна регулатива и заедничко финансирање на овие компании од страна на меѓународните организации. Најважниот фактор кој доведе до зголемена потреба од овие услуги е секако, неусогласеноста помеѓу политичките амбиции и воените капацитети, т.е. претераната интензивирана употреба на националните вооружени сили поради повеќекратни истовремени интервенции. За операции на ЕУ тоа значи дека земјите-членки кои придонесуваат не се подготвени да обезбедат униформирани војници за околинска/реонска заштита и други функции за поддршка. ПКО нудат решение за овој проблем, со брзо распоредување на голем број на чувари, во временска рамка во која ќе им биде побарано. Поедини приватни компании имаат капацитети и за давање на услуги од типот: стратешки воздушен транспорт, вршење истраги и сл[165].
Сите обиди на земјите-членки на ЕУ за употреба на ПКО кои би работеле надвор од нивните национални територии резултираа со повторување на меѓународното хуманитарно право и создавање на доброволен индустриски кодекс на однесување, врз основа на Монтре Документот. Несомнена е заложбата за подобрување на контролата од страна на ЕУ со лиценцирање и регистрирање на ПКО со седиште во ЕУ, како и лиценцирање на договори за обезбедување на воени и безбедносни служби надвор од ЕУ.
Тргнувајќи од постулатот дека земјите треба да учат од меѓусебните искуства, особено доколку потекнуваат од ист регион каде што во одредена мера владеат слични правила за слични проблематики, како и заложбите на Р. Македонија за полноправно членство во ЕУ, неодложно наметнува сеопфатна

[164] Preparation of public calls, where a condition to get business is not simply the lowest offered price, supervision over "economic" justified price, supervision of implementation of Minimal Wage Act (2010), as well as Work Relations Act (2013).

[165] The Role of Private Security Companies (PSCs) in CSDP Missions and Operations, 2011

мобилизација на сите чинители и фактори кои на бил кој начин имаат улога или влијание во целиот процес на правно регулирање, употреба и контрола врз ПКО.

Во таа насока **Р. Македонија внатре** треба да се насочи кон: отвореност, меѓуресорска соработка, зголемување на угледот, транспарентност, интегритет во работењето, морална и друга одговорност, поголема професионализација, контрола, ориентација кон самата дејност, одговорност кон општеството, одговорност пред законот, определување минимална цена на услугите, унифицирање и сл.

Регионално – перманентна соработка со земјите од ЈИЕ, организирање на модалитети на соработка за размена на искуства, билатерални соработки, по можност организирање на мултилатерални вежби (следење конвој, обезбедување мигранти) итн.

На ниво на ЕУ – формирање на тело или сектор со одлука на Владата на РМ, во некоја од релевантните институции или Комората за обезбедување, кое ќе ги преземе обврските за следење, анализа и имплементирање на сите регулативи кои ќе бидат донесени од ЕУ, а ќе имаат импликација по ПКО и детективската дејност. На овој начин ќе им помогнеме на нашите ПКО да бидат конкурентни со компаниите од другите држави, а со тоа и би имале отворен пат како контрактори да учествуваат во меѓународни мисии, поконкретно во ЗБОП операции и мисии.

Литература

1. https://www.biography.com/people/allan-pinkerton-9441102
2. Б. Ванковска State-Building and Privatisation of Security in Macedonia, Скопје 2016
3. Recommendation1402, The Parliamentary Assembly of the Council of Europe, 1999
4. Code od Conduct on Politico-Military Aspects of Security, Organization for Security and Co-operation in Europe, Dec 1994
5. Management – Tasks, responsibilities, Practice, Harper Busines, P. F.Drucker, USA, 1993
6. Закон за организација и работа на органите на државната управа, "Службен весник на РМ" бр. 58/2000
7. Службен весник на РМ бр. 41/00
8. Приватните безбедносни компании во ЈИЕ – развој и регулирање, Приватниот безбедносен сектор во компаративна перспектива, Приватна безбедност во XXI век, Искуства и предизвици, Скопје 2016 година
9. https://www.icrc.org/eng/assets/files/other/icrc_002_0996.pdf
10. Joanna Spear, The Political Economy of Private Military Companies, Private Sector Activity in Armed Conflict, Fafo 2006. http://www.fafo.no/index.php/nb/zoo-publikasjoner/fafo-rapporter/item/market-forces
11. Lilly, D., Green Paper submission: private military companies: options for reg-ulation, International Alert, July, 2002
12. http://www.consilium.europa.eu/showPage.aspx?id=1484&lang=en
13. http://www.europarl.europa.eu/oeil/popups/summary.do?id=1497100&t=e&l=en
14. M. Sassoli, Legislation and Maintenance of Public Order and Civil Life by Occupying Powers' The European Journal of International Law, 2005.

М-р Ебру Ибиш
Европски Универзитет Република Македонија
Климент Охридски 68
Македонија, Скопје 1000
тел: +389(0)2 3202098
факс: +389(0)2 3202030
е-маил: ebru.ibis@eurm.edu.mk

Реформа на казненото материјално право во Република Македонија (1996-2002)

Апстракт

Република Македонија како земја во транзиција доживеа голем број реформи од областа на кривичното право. По осамостојувањето на Македонија од 1991 година, беа направени реформи од областа на кривичното материјално и процесното право. Првата реформа во кривичното материјално право започна во 1996 година со усвојувањето на Кривичниот закон, главните цели на овој закон беа поврзани кон општиот и посебниот дел на законот и системот на санкции. Следната реформа беше во 1999 година, главните причини за оваа реформа беа изградба на нова стратегија за спречување на современи видови криминал, како што се организираниот криминал и корупцијата; следејќи ги реформите на земјите на ЕУ и меѓународните обврски на Македонија. Следната реформа од 2002 година, беше повеќе фокусирана на општиот дел од кривичниот закон, евроинтеграцијата, промените во структурата на криминалот и новите форми на криминал.

Клучни зборови: реформа, кривичен закон, систем на санкции, криминал, материјално казнено право

M.Sc Ebru Ibish
European University Republic of Macedonia
Kliment Ohridski 68
Macedonia, Skopje
Tel: +389(0)2 3202098
fax: +389(0)2 3202030
e-mail: ebru.ibis@eurm.edu.mk

Reform of criminal material law in Republic of Macedonia (1996-2002)

Abstract

Macedonia as a country in transition had many reforms in the area of criminal law. Periodization of criminal law is part of this article, novelty as a method was used as a part of the reforms in field of criminal code. After the independence of Macedonia from 1991 so many reforms were made in the area of criminal material and criminal procedural law. First reform in criminal material law started in 1996 with the adoption of the Criminal Code the main aims of this code was related in two things: in reform of the general and specific parts of articles and system of sanctions. The

next reform was in 1999, the main reasons of this reform were building a new strategy for prevention of modern types of crime such as a organized crime and corruption; following the reforms of EU countries and international obligations of Macedonia. The upcoming reform was at 2002 which was more focused on the general part of criminal code, euro integration, changes of the structure of the crime and new forms of crime. Finally the last part of this article is in field of juvenile delinquency and the reform as a most important reforms in the area of criminal law.

Key words: reform, criminal code, system of sanctions, crime, material criminal law

1. Историски развој на казненото право

Постојат различни ставови во однос на периодизацијата на казненото право, како база на периодизација се земаат различни цели, на пример: појава на криминалот; општествена реакција; современиот период на казненото право и сл. Со оглед на горенаведното може да се заклучи дека постојат различни класификации околу периодизацијата. Една од најшироко прифатените периодизации е дека казненото право се дели во две етапи: предисторија и вистинска историја што започнува од почетокот на XIX век со афирмацијата на начелото на законитост како негово темелно начело.[166] Од големо значење е да се наведе важноста на казните и преминот од композиција (помирување на страните) и одмазда на јавна казна. Една од значајните закони која е позната по нејзините драконски казни е Хамурабиевиот законик од XX век п.н.е, законикот е познат по принципот на талион: *око за око, заб за заб*. Од начелото на талион произлегува идејата за спреведлива одмазда, односно од одредбите во законикот може да се забележи дека владее следната максима: "со што некој греши со тоа се казнува" (per quod quis peccat, per idem punitur) како пример може да се наведат следните одредби од законикот: [167]

"Ако некој извршил разбојништво и биде фатен, да се убие" (член 22)
"Ако синот го тепа својот татко, да му се исечат рацете" (член 195)
"Ако некој на некого му уништи око, да му се уништи неговото око" (член 196)

Појавата на јавната казна игра значајна улога во периодот на премин од првобитна заедница во држава. Правото на казнување (ius gladii) ги предизвикала следните трансформации во начинот на казнувањето: наместо компензација- парична казна; наместо крвна одмазда примена на смртна казна или телесни повреди и исклучувањето од заедница се трасформира во протерување од држава. Кога станува збор за еволуција на казните а воедно и историскиот развој на казненото право, неизбежно е да ги споменеме законите во античка Грција и Римската империја. Во античка Грција е познат кодифицираниот закон на владетелот Дракон, кој вовел строги и сурови казни дури и за ситни дела, како на пример: кражбите се казнувале со смртна казна па затоа често за овој законик се вели дека тоа се закони *пишувани со крв,* следната реформа е направена од страна на Солон во 594 година п.н.е. За време на Римската империја усвоени се значајни законици како што е законот на XII таблици во петти век, поточно 451 година п.н.е. Во Римската империја

[166] Камбовски, Владо, "Казнено право – општ дел" Универзитет Св. Кирил и Методиј, Скопје, 2011, страна 27.
[167] Поповска, Билјана, "Историја на правото", Правен Факултет Јустинијан Први- Скопје, 2-ри Август Ц-Штип, Скопје, 2005, страна 108 и 126.

врв на реформата претставува Јустинијановата кодификација (*Corpus Iuris Civilis*) од 529 година која била составена од 5 дела: *novus codex Iustinianus; digesta (pandectae); institutiones; codex repetitae praelectionis; novellae.*

Големата реформа на казненото право можеме да ја разгледаме во три главни точки: преку Чезаре Бакарија, Џереми Бентам и Француската револуција од 1789 година. Делото на Чезаре Бакарија *"За злосторствата и казните"* е најзначајно дело во казненоправна мисла врз основа на која се развива казненоправната теорија во XIX век. Џереми Бентам е еден од највлијателните и најважните претставници на утилитаризмот, неговите казненоравни ставови се истакнати во делото: " Вовед во начелата на моралот и законодавството". Конечно Француската револуција од 1789 година може да се зборува за значајни докумнти како што е: Декларацијата за правата на човекот и граѓанинот која претставува прв современ уставноправен документ. Кодификацијата на казненото право од XIX век резултира со многу значајни кодификации меѓу кои се: Наполеоновиот Code Penal, баварскиот казнен законик, австрискиот КЗ од 1852 година, холандскиот КЗ од 1881 година, белгискиот КЗ од 1867 година, унгарскиот КЗ од 1878 година, турскиот КЗ од 1858 годин, италианскиот КЗ од 1889 година.

2. Цели на реформата на казненото материјално право

Пред да преминеме со анализата на фазите на реформите во Македонското казнено право важно е да потенцираме дека постојат две различни методи на спроведување на казненоправните реформи. Првата метода е со донесување на *нови кривични закони* а втората со *новелирање.*

Имајќи го во предвид фактот дека современото казнено право, од XIX век до денешницата инсистира почитување во прв ред начелото на законитост и начелото на владеење на правото, со цел градење на демократска правна држава, важно е да констатираме дека во оваа фаза на развој, заштитата на човековите слободи и права се стават на прв ред. Од осамостојувањето на Република Македонија во 1991 година, определени прописи (меѓу кои е и казненото законодавство) од поранешна Југославија, останале во сила. Пред стапувањето на сила на новиот КЗ во Република Македонија се применувало југословенскиот КЗ од 1977 година. Прва фаза на реформата на Македонското казнено материјално право започнува во 1996 година со донесување на Кривичниот законик. Една од најважните цели на реформата се сведуваат на следните две фази:

прва фаза: Се придава место за донесување на нов кривичен законик со измени од општиот и посебниот дел во законот;

втора фаза: посебно внимание било поставено околу системот на санкции;

Кривичниот законик од 1996 година е прв законодавен акт со која започна реформата во Република Македонија а неа ја проследија Законот за кривична постапка; Законот за извршување на санкции и Законот за прекршоци кои во целина ја оцртуваа современата демократска правна Република Македонија. Нацртот за донесување на Законот за кривична постапка беше понуден во 1995 година од страна на министерство за правда. Ова е првата фаза на реформата во областа на процесното право. Основните цели на реформата беа: усогласување на дотогашниот Закон за кривична постапка со Уставот на Република Македонија, со најзначајните меѓународни акти што ги засегаат човековите права- со ЕКЧП, со МПГПП и со другите документи како и со

јуриспруденцијата на ЕСЧП во Стразбур и комитетот за човекови права на ООН.[168]

Усвојувањето на новото казнено законодавство претставуваше составен дел и основна претпоставка за длабоките промени на општествениот, политичкиот и економскиот систем! Тие имаат карактер на коренета општествена реформа што значат редефинирање на појдовните начела: наместо политички и партиски монизам- плурализам и парламентарна демократија, наместо општествена-приатна сопственост, наместо политичка и партиска-правна држава итн.[169] Следно прашање во врска со реформата е усогласување на терминологијата. Наместо зборот кривично кој потекнува од *"кривица"* се користи казнено, (сега наместо кривично право имаме казнено право, казнено дело, казнена санкција, казнено законодавство и сл.) со цел да е соодветен на македонскиот јазик. Една од главните постулати на новиот Кривичен законик освен почитувањето на основните човекови слободи и права кои се природни права *(jus naturalis)*, внесување на нов систем на вредности, усогласување на мекедонското казнено право со европското казнено право, обврските на државата на меѓународен план како што се имплементација на определени меѓународни договори и развивање на човековите права е и создавање на ефикасен казнено-правен систем што може да се каже дека е од клучно значење бидејќи станува збор за создавање на систем за успешно сузбивање на потешките видови на криминал: корупција, перење пари, организиран криминал и сл. Имајќи ја во предвид комплицираноста на организираниот криминал важно е да кажеме дека поновите дефиниции од истата област во законите за јавно обвинителство и полицијата. Така во *Законот за полициските овластувања и одговорности* на австралиската држава Квинсленд од 1997 година организираниот криминал е дефиниран како продолжителен криминален пофат во вршење на тешки дела на систематски начин, шо инволвира определен број лица и заедничко планирање и организација.[170]

Во првата фаза на реформата извршени се определени инкриминации, кривичниот законик создава нова концепција за вината. Имајќи го во предвид член 17 од КЗ (не е кривично одговорен сторителот на кривично дело кој од оправдани причини не знаел и не можел да знае дека тоа е забрането и ако сторителот на кривичното дело можел да знае дека делото е забрането, може да се казни поблаго[171]) за дејството на правната заблуда која значи напуштање на психолошката концепција и преминување на нормативната концепција на вината според која вината ја сочинуваат: пресметливост, умисла или небрежност и свест за противпарвноста на делото. Редефиниран е поимот на пропуштањето односно несторувањето, извршени се определени инкриминации околу системот на казните исто така редефинирана е целта на казната согласно член 32: "*покрај остварувањето на првдата целта на казнувањето е: спречување на сторителот да врши кривични дела и негово*

---

[168] Матовски, Никола, Б.Лажетиќ, Гордана, Калајџиев, Гордан, "Казнено Процесно Право", 2-ри Август Ц Штип, Скопје, 2011, страна 29.

[169] Камбовски, Владо, "Казнено-правната реформа пред предизвиците на XXI век" Bato&Divajn Graphic Auter, Скопје, 2002, страна 342.

[170] Камбовски, Владо, "Организиран Криминал", 2-ри август Ц Штип-Скопје, 2005, страна 25.

[171] Каневчев, Методија, "Кривичен Закон", 2-ри Август Ц-Штип, Скопје, 2010, чл.17.

превоспитување и воспитно да се влијае врз другите да не вршат кривични дела“ . Минимумот на затворот со новата реформа е подигнат на **30 дена** а максмумот на **15 години**, предвидена е и парична казна. Извршени се реформи во областа на системот на мерките на безбедност.Во кривичниот законик темелно е реконструиран концептот на рехабилитација согласно член 103 постои законска рехабилитација и судска рехабилитација. Согласно член 104 законската рехабилитација се состои во бришење на осуди од казнената евиденција, на казна затвор до три години ако по истек на законско определениот рок (од зависност на тежината на стореното кривично дело) осудениот не стори ново кривично дело. Согласно член 105 судската рехабилитација се состои во предвремен престанок на правните последици од осудата што се однесуваат што се однесуваат на забрана на стекнување на определени права, предвремен престанок на мерките на безбедност што се состојат во забрани, како и во бришење на казнената евиденција на молба на осудениот при осуда на казна затвор над три години, ако осудениот во определен рок, различен од различните видови осуди не изврши ново казнено дело.[172] Во посебниот дел направени се инкриминации кај делата против животот и телото; делата против слободите и правата на човекот и граѓанинот; заштита на правото на приватност како што се наовластено објавување на личн податоци. Изборните инкриминации се издвоени во посебна глава, направени се инкриминации исто така и кај делата против работните односи; дела против половата слобода и половиот морал, делата против бракот, семејството и младината, изршени се определени измени кај делата против здравјето на луѓето, кај делата на пренесување на заразна болест; делата против животната средина со оглед на актуелноста на загадувањето на околината, заштита на еко системот; делата против безбедноста на јавниот сообраќај; делата против вооружени сили; делата против службена должност; делата против правосудството; злосторствата против човечноста и меѓународното право и сл. Измените и дополнувањата на кривичниот законик на Република Македонија од 1999 година се извршија користејќи ја методата на новелирање. Измените од 1999 година се сведуваат на следните три причини: градење на сериозна стратегија за сузбивање на организираниот криминал и корупцијата како една од најтешките форми на криминал, второ следење на реформите во европските земји и законосавства и трето обврските на Република Македонија во меѓународен план. Воведени се нови инкриминации во следните дела: измама во службата, злоупотреба на службена положба и овластување, извршени се определени инкриминации на тешките убиства, одредбата епроширена за убиство на судија, јавен обвинител, адвокат при вршење на неговата дејност согласно член 123 ст.2. Освен измените кај тешките убиства внесена е нова одредба за убиство на повеќе лица, воведени се определени измени кај делата против честа и угледот.

Новелата на кривичниот законик од 2002 година не е толку обемна како и претходната, може да се каже дека се направени мали измени и дополнувања со цел усогласување на одредбите. Како позначајни измени би можеле да ги

---

[172] Камбовски, Владо, “Казнено-правната реформа пред предизвиците на XXI век“ Bato&Divajn Graphic Auter, Скопје, 2002, страна 354.

одвоиме одредбите околу компјутерскиот криминал согласно член 251 неовластено навлегување во компјутерски систем со намера на прибавување на имотна корист; одредби околу трговија со луѓе и конечно би можеле да ја споменеме усогласувањето на конвенцијата од Палермо позната како Конвенција на ООН против транснационалниот организиран криминал и нејзините дополнителни протоколи. Во 2002 година започнува и втората фаза на казнено правната реформа која повеќе е насочена кон измените во општиот дел, како една од важните сегменти ќе ја напоменеме и евроинтеграцијата од една страна и промените во структурата и обемот на криминалот и појавата на нови форми на криминал од друга страна. Со цел да направиме споредба околу обемот и динамиката на криминалот од осамостојувањето на Република Македонија (1991) па се до реформата во 2002 година ќе ги погледнеме показателите на статистиката на криминалот.

Вкупно пријавени обвинети и осудени полнолетни лица:[173]

Години	1991	1992	1993	1994	1995	1996	1997	1998	1999	2000	2001
Пријавени	13429	17149	22816	20283	19969	19452	19277	20582	19383	20220	18018
Обвинети	9678	8801	8496	8534	9579	8012	7167	7891	8533	8078	7509
Осудени	7095	6660	6538	6724	7711	6341	4732	6128	6783	6496	5952

Во посебниот дел се предлагаат определени измени во однос на конфискација на имот, измама при работење со хартии од вредност, поднесување лажни докази, и сл. освен наведените измени воведени се нови изрази како една од најактуелните е семејното насилство, согласно член 122 ст.21 од кривичниот закон, под *семејно насилство се подразбира малтретирање, грубо навредување, загрозување на сигурноста, телесно повредување, полово или друго психичко или физичко насилство со кое се предизвикува чувство на несигурност, загрозување или страв, спрема брачен другар, родителите или децата или други лица кои живеат во брачна или вонбрачна заедница или заедничко домаќинство, како и спрема поранешен брачен другар или лица кои имаат заедничко дете или се наоѓаат во блиски лични односи.*[174]. Една од значајните новини на реформата се определени одредби од областа на малолетничкото казнено право, поточно проширување на казните и воведување на алтернативните мерки. Како нови казни биле предложени протерување на постар малолетник од земја и забрана за управување со моторно возило кој и денес се користат како еден вид на казна за деца додека како алтернативни мерки предложени биле општокорисната работа и условно одлагање на казната. Имајќи го во предвид малолетничкиот криминал како дел од проблематиката во општеството а и воведување на нови казни од истата област од важност е и да се прегледа состојбата на малолетничкиот криминал од 1991 година па се до 2001 година поточно периодот пред реформата на казненото материјално право.

[173] www.stat.gov.mk

[174] Каневчев, Методија, "Кривичен Закон", 2-ри Август Ц-Штип, Скопје, 2010, чл.122 ст 21.

Заклучок

Законите се огледало на секоја земја во однос на нивната традиција, морални и етички вредности, социјална и економска состојба, образование и менталитет. Реформите во областа на кривичното материјално право во Република Македонија беа поврзани со општествените промени, новите видови криминал, интеграцијата во еврото, следењето на европските закони, креирањето на нова криминална политика итн.

Од 1991 година Македонија беше земја во транзиција, овој период е добро познат и со економската криза, статистички зголемување на бројот на криминал и појава на нови форми на криминал, наведените рабти се показатели на потреба од нова реформа. Големите реформи во областа на кривично материјалното право во Македонија беа направени во следните години: 1996, 1999, 2002, 2004, 2009 и 2014 година исто така од важност е да се сподели дека една од најзначајните реформи беше реформата во областа на малолетничкото кривично право во 2007 година.

Потребата од посебен закон во облста на малолетничка правда беше поради зголемувањето на бројот на малолетни деликвенти. Во 2007 година беше донесен Законот за малолетничка правда. Оваа реформа создаде посебна постапка за малолетници, посебни санкции како што се: казнување за малолетници, алтернативни мерки, воспитни мерки и безбедносни мерки. Подоцна во 2013 година беше донесен новиот закон од областа на малолетничкото казнено право, поточно станува збор за Закон за правда за децата, една од главните причини за усвојување на нов Закон со различен назив, беше усогласување на Законот за правда за децата со Конвенцијата за правата на детето.

Реформата на кривичното законодавство во повеќето земји во транзиција е комплициран процес кој сериозно може да ја загрози идејата за правната држава и човековите слободи и права, периодот на транзиција е последица на напуштањето на еден систем на вредности и тешкотии во прифаќањето на нов систем на вредности, заедно со создавање на нови економски односи и нова законска институционална рамка. Имајќи ја во предвид важноста на реформите за кривично материјално право, треба да се нагласи дека воглавно овие реформи се клучни за создавање на "правна држава", вклучувајќи ги и принципите на законитост и владеење на правото.

Користена литература

1. Камбовски, Владо, “Казнено право – општ дел “Универзитет Св. Кирил и Методиј, Скопје, 2011

2. Камбовски, Владо, “Казнено-правната реформа пред предизвиците на XXI век“ Bato&Divajn Graphic Auter, Скопје, 2002

3. Матовски, Никола, Б.Лажетиќ, Гордана, Калајџиев, Гордан, “Казнено Процесно Право“, 2-ри Август Ц Штип, Скопје

4. Методија Каневчев, Кривичен законик на Р.М (Criminal Code of Republic of Macedonia), 2-ри Август Ц-Штип, Скопје, 2010

5. Поповска, Билјана, “Историја на правото“, Правен Факултет Јустинијан Први- Скопје, 2-ри Август Ц-Штип, Скопје, 2005

6. Council of Europe Convention on preventing and combating violence against women and domestic violence, 2011

7. https://www.britannica.com

8. https://www.unodc.org

9. https://www.stat.gov.mk

М-р Ебру Ибиш
Европски Универзитет Република Македонија
Климент Охридски 68
Македонија, Скопје 1000
тел: +389(0)2 3202098
факс: +389(0)2 3202030
е-маил: ebru.ibis@eurm.edu.mk

Феноменологија на малолетничкиот криминалитет во Република Македонија

Апстракт
Малолетничката деликвенција претставува сериозна закана за општеството од криминална гледна точка, но исто така и за развојот на детето од образовен аспект. Долго време во криминолошките истражувања, поголемо значење се придаваше на современите облици на криминал, организиран криминал и др, но земајќи го во предвид фактот дека престапниците се малолетници, може да се заклучи дека ова се лица кои уште од рана возраст градат криминална кариера, се запознаваат со различни видови на кривични дела и најчесто извршуваат кривични дела против имотот со цел полесен начин за добивање на средства и задоволување на сопствените потреби, овој процес носи уште еден проблем: градење криминална кариера и во иднина создавање на профил на професионален криминалец. Од феноменолошки аспект, со цел да се идентификуваат облиците на малолетничкиот криминал, важно е да се споменат обемот, динамиката, структурата и карактеристиките на малолетничкиот криминал во Република Македонија. Клучен фактор за зголемување на бројот на сторители на кривични дела, покрај главните криминогени фактори, вклучувајќи ја сиромаштијата, богатството и невработеноста од етиолошка гледна точка, една од клучните работи е системот на санкции против малолетниците и непреземање на превентивни мерки пред сторување на кривичните дела.

Клучни зборови: малолетнички криминал, малолетничка деликвенција, феноменологија, статистика за криминал, рецидивизам

M.Sc Ebru Ibish
European University Republic of Macedonia
Kliment Ohridski 68
Macedonia, Skopje
Tel: +389(0)2 3202098
fax: +389(0)2 3202030
e-mail: ebru.ibis@eurm.edu.mk

Phenomenology of juvenile crime in Republic of Macedonia

Abstract
Juvenile delinquency poses a serious threat to society from a criminal point of view, but also to the development of the child from an educational aspect. For a long time in criminological researches, more importance was attached to modern forms of crime, organized crime etc. but taking into account the fact that the offenders are juveniles it can therefore be concluded that these are persons who from a very early age build their criminal career, get acquainted with different types of crimes and mostly commit crimes against property with the target of an easier way of obtaining funds and satisfying their own needs, this process brings another problem: building criminal career and becoming a professional criminal as an adult. From the phenomenological point of view in order to identify the forms of juvenile crime, it is important to mention the scope, dynamics, structure and characteristics of the juvenile crime in the Republic of Macedonia in order to obtain a general picture of the situation. The key factor of increasing the number of perpetrators of crimes, apart from the main criminogenic factors, including poverty, wealth and unemployment from an etiological point of view, the most important think is the inefficiency of the system of punishment against juveniles, and not taking preventive measures from an early age towards the juveniles

Key words: Juvenile crime, juvenile delinquency, phenomenology, statistics of crime, recidivism

Вовед
Криминалитетот претставува нејтежок облик на престапничко однесување под кое се подразбира кршење на кривично-правните норми. Низ човековата историја, интересот на човекот е насочен токму кон задоволување на сопствените потреби, но дали тоа секогаш е на праведен начин? Велиме дека криминалот е огледало на општеството, па оттука може лесно да ги одвоиме малолетните сторители на кривични дела и нивната положба во општеството.
Во изминатиот период се бележи брз развој на средствата за комуникација. Мобилните телефони, интернетот, компјутерите и кабелските телевизии им овозможуваат на младите за многу кратко време да стигнат до потребните информации. Нивните побарувања се зголемуваат од ден на ден, а кризата во која се наоѓа нашата држава не оди во прилог кон задоволување на потребите на децата. Незадоволувањето на потребите е доволна причина за малолетникот да ја активира својата почетна криминална кариера. Обемот на

малолетничкиот криминалитет[175] како во сите држави, така и кај нас не е статичен, истиот покажува пораст од година во година. Причините за пораст на криминалитетот се: сиромаштијата, невработеноста, лошите услови за живот, околина, неквалитетно образование, економската криза и сл.
Зачудува податокот што малолетничкиот криминалитет сè уште се карактеризира како машка појава, стапката на женските деца – сторители на кривични дела е многу мала дури незначителна.
Во однос на превенцијата на малолетничкиот криминалитет најзначајно место заземаат: семејството, околината, училиштето и центрите за социјална работа. Родителите треба да создадат неделни активности за детето кои ќе бидат продуктивни за неговиот развој со цел да нема премногу вишок на време. Освен тоа многу е значајна околината и лицата со кои се дружи детето, затоа што доколку само едно лице има информации во однос на било каков криминал, доволно е да ги сподели со другите деца за да некој од нив стане дел од криминалот. Училиштето, по семејството има најголем и највлијателен ефект врз детето. Основните и средните училишта треба да имаат посебни програми со цел да ги едуцираат децата колку негативно може криминалот да влијае врз животот на детето. Општеството треба да се стреми да ги задоволува интересите на децата, со цел да има пониска стапка на малолетнички криминалитет во идните години.

ФЕНОМЕНОЛОГИЈА НА МАЛОЛЕТНИЧКИОТ КРИМИНАЛИТЕТ ВО РЕПУБЛИКА МАКЕДОНИЈА

1. Феноменологија на криминалитетот

Посебно значење за криминалната феноменологија претставува изучување на појавните облици на криминалот. Во рамките на криминологијата поимот феноменологија се употребува за да ги означи надворешните манифестации, формите и облиците на криминалитетот. Врз основа на современите научни истражувања на малолетничкиот криминалитет утврдено е дека: криминалитетот е во рапиден пораст, но во уште поголем пораст е малолетничкиот криминалитет. Освен негативните фактори коишто влијаат врз криминалното однесување на малолетниците, истовремено е забележано поголемо учество на малолетници во социо-патолошки појави како што се алкохолизмот, проституција, наркоманија, питачење и сл.[176] Во последните години малолетниците учествуваат сè повеќе во дела на насилство и организиран криминал, забележан е и пораст на рецидивизмот кај малолетниците. Како главен елемент на малолетничкиот криминалитет е и агресивноста на малолетниците. Поради општествената опасност и специфичност на личноста, малолетничкиот криминалитет бара посебна

[175] Со донесувањето на Законот за малолетничка правда, а потоа и Законот за правда за децата, се напушти терминологијата малолетник и истата се замени со терминот дете. Сепак, во литературата сè уште се користат термините малолетник, малолетнички криминалитет, малолетничка деликвенција и сл. Оттука, авторот на трудот ги користи овие термини во трудот.
[176] Durak, İzzet, "Suç Öncesi ve Sonrası Suçlu Piskolojisi", Kitapyurdu, İstanbul, 2013, стр. 154

интервенција на општеството и потреба од реагирање на надлежните органи на казнениот прогон.[177]

Кај нас евиденција за малолетнички криминалитет водат: органите за внатрешни работи, јавните обвинителства, Државниот завод за статистика, Министреството за правда, основните судови и центрите за социјална работа коишто водат евиденција за децата и малолетните сторители на кривични дела и други делинквентни поведенија спрема критериумите на малолетничката запуштенст и престапништво.[178] Понатаму во трудот, анализирани се статистички податоци за периодот 2009-2016 година, врз основа на кој презентираме општа слика за обемот, појавните облици, структурата, динамиката на малолетничкиот криминалитет.

2. Обем и динамика, појавни облици и структура на малолетничкиот криминалитет

Обемот односно тоталитетот на криминалитетот претставуваат едно од примарните квантитативни обележја на оваа појава.[179] Динамичноста како поим, општо не само за малолетничкиот криминалитет, туку и за секој вид на криминалитет е од клучно значење, затоа што криминалитетот не е статична појава, туку напротив, таа е динамична и променлива. Подлабоките економски, општествени, социјални и културни промени директно влијаат врз динамичноста на малолетничкиот криминалитет. Во однос на карактеристиките на малолетничкиот криминалитет понатаму во трудот се анализирани: полот, возраста, повратот, материјалниот статус и местото на живеење. Структурата на малолетничкиот криминалитет ги опфаќа податоците на видовите кривични дела и внатрешната структура на кривични дела.

2.1 Обем и динамика на малолетничкиот криминалитет

Во периодот од 2009 до 2016 година се забележува дека во 2009 година има 1519 пријавени малолетници и во 2010 година - 1244 пријавени малолетници година, што претставува највисок број на пријавени малолетни лица. Додека кај полнолетните најмногу пријавени полнолетни лица има во 2009 година со 15.511 полнолетни лица и 2014 година - 16.113 полнолетни лица.

Табела бр.1 Број на пријавени малолетни и полнолетни лица во Република Македонија во периодот 2009-2016 година[180]

Година на Пријавување	Вкупно пријавени полнолетни лица	%	Вкупно пријавени малолетни лица	%	Вкупно
2009	15.511	91.1	1519	8.9	17.030
2010	15.383	92.5	1244	7.5	16.627
2011	14.267	90.3	1163	9.7	15.790
2012	15.480	93.2	1001	6.8	16.481
2013	15.102	93.7	1005	6.3	16.107
2014	16.113	94.3	972	5.7	17.085
2015	15.408	95.2	772	4.8	16.180
2016	11.866	95.3	587	4.7	12.453

Извор: Државен завод за статистика

[177] Велкова, Татјана, "Феноменологија на малолетничкиот криминалитет во Република Македонија во периодот1982-2000 година", 2-ри Август Ц-Штип, Скопје, 2006, стр.135

[178] И. Јосифовски, Љ. Арнаудовски, "За статистиките за криминалитетот" Институт за социјални и политичко правни истражувања, Скопје, 1963, стр.

[179] Арнаудовски, Љупчо,"Криминологија, 2-ри Август – Штип, Скопје, 2007, стр.244

[180] http://www.stat.gov.mk/OblastOpsto.aspx?id=6

Во 2016 година се забележува намален број на малолетни и полнолетни сторители на кривични дела. Во 2015 година за разлика од 2014 година, исто така, се бележи опаѓање на бројот на пријавени малолетни и полнолетни лица. Во 2011 година се забележува ниска стапка на криминалитетот кај полнолетните лица, додека кај малолетниците најниска стапка на криминалитетот има во 2016 година.

Според податоците на Државниот завод за статистика, во 2009 година бројот на пријавени полнолетни лица во споредба со 2008 година е зголемен за 0.3%. Бројот на пријавените малолетни лица во споредба со 2008 е зголемен за 12.1%. Во 2010 година бројот на пријавени полнолетни лица во споредба со 2009 е намален за 0.8%, за разлика од полнолетните, кај малолетните лица се забележува намалување на криминалитетот за 18.1%. Во следната 2011 година бројот на пријавени полнолетници во споредба со минатата 2010 година е намален за 4.9%; кај малолетните лица бројот на пријавени за разлика од 2010 година е намален за 6.5%. Во 2012 година бројот на пријавените полнолетни лица за разлика од 2011 е зголемен за 5.8%, кај малолетните лица се забележува опаѓање во споредба со 2011 година од 13.9%. Во 2013 година бројот на пријавени полнолетни лица во споредба со 2012 година е намален за 3.0%, а кај малолетниците забележуваме зголемување на бројката на пријавени од 0.4%. Во 2014 година бројот на пријавените полнолетни лица сторители, во споредба со 2013 година, е зголемен за 7.3%, кај малолетниците забележуваме 3.3% намалување во споредба со претходната година. Во 2015 година има пријавени полнолетни (15.408) и малолетни (772) лица. Конечно, во 2016 година има најниска стапка на пријавени полнолетни (11.866) и малолетни (587) лица.

Како што е напоменато претходно во трудот, криминалитетот не е статична појава, таа е динамична и зависи од условите што ги овозможува општеството. На пример, во периодот кога стапката на невработеност е многу ниска, може да се забележи зголемување на криминалитетот и обратно кога има висока стапка на вработеност, тогаш има пониска стапка на криминалитет. Сигурно е дека со пронаоѓање на различни методи и со добра општествена организација, може да има намалување на криминалитетот, но не и негово елиминирање.

Табела бр.2 Број на обвинети малолетни и полнолетни лица во Република Македонија во периодот од 2009-2016 година

Година	Вкупно обвинети полнолетни лица	%	Вкупно обвинети малолетни лица	%	Вкупно
2009	11.305	87.4	1030	12.6	12.935
2010	11.239	93.7	750	6.3	11.989
2011	12.219	92.4	1002	7.6	13.221
2012	11.311	91.6	778	8.4	12.089
2013	12.297	94.9	657	5.1	12.954
2014	13.699	95.1	712	4.9	14.411
2015	11.951	96.2	465	3.8	12.416
2016	9320	96.4	702	3.6	10.022

Извор: Државен завод за статистика на Република Македонија.

Како што може да видиме од табелата број 2, најголем број на обвинети полнолетни лица има во 2014 година - 13.699 лица и во 2013 година - 12.297 лица, додека најнизок број на обвинети полнолетници е забележан во 2016 година - 9320 лица. За разлика од полнолетните кај малолетните обвинети лица највисока стапка на обвинети има во 2009 година - 1030 малолетници и во 2011 година - 1002 малолетни лица, додека, пак, најнизок број на обвинети малолетници е 702 лица во 2016 година.

Табела бр.3 Број на осудени малолетни и полнолетни лица во Република Македонија во периодот од 2009-2016 година

Година	Вкупно осудени полнолетни лица	%	Вкупно осудени малолетни лица	%	Вкупно
2009	9810	92.9	748	7.1	10.549
2010	9169	94.4	547	5.6	9710
2011	9810	93.1	722	6.9	10.532
2012	9042	94.2	556	5.8	9598
2013	9539	95.2	473	4.8	10.012
2014	11.683	96.2	461	3.8	12.144
2015	10.312	96.7	348	3.3	10.660
2016	8172	94.6	468	5.4	8640

Извор: Државен завод за статистика

Од изнесените податоци во однос на осудени малолетни лица може да забележиме дека има тенденција на намалување на криминалитетот во последните 2 години. Важно е да се напоменат сите надворешни фактори кои влијаат врз намалување на криминалитетот кај малолетните лица, а тоа се: образованието, добрите односи со родителите, вработеноста, здравството, околината на детето и добро ангажирање на времето.

Со цел намалување на малолетничкиот криминалитет и криминалитетот, воопшто, Република Македонија мора сериозно да ги ангажира општествените фактори во насока на намалување на криминалитетот и ресоцијализација на малолетните сторители на кривични дела. Ресоцијализацијата е од клучна важност кога станува збор за малолетници, поради фактот што малолетничката делинквенција претставува загрозеност во социјалниот развој, мерките за ресоцијализација се насочени кон:[181] оспособување за вклучување во процесот на трудот и самостоен живот; стекнување на образование; интеграција на малолетните делинквенти во социјална средина; динамичен однос спрема последиците и мерките за надминување на ситуацијата и хуманистички вредности.

[181] Љ.Чонева, В.Чачева, Љ.Арнаудовски, М.Станкова, М.Марковиќ, Г.Станковска, "Малолетничкиот криминалитет во транзицијата во Република Македонија", Институт за социолошки и политичко-правни истражувања, Скопје, 2007, стр.153

Табела бр.4 Пријавени малолетни лица според кривичното дело, полот и припадноста кон етничка заедница (2007-2016)

Видови кривични дела (2007)	М	Ж	Вк.	Македонци	Албанци	Власи	Роми	Турци	Срби	Бошњаци	Останато	Непознато
Кривични дела против животот и телото	71	1	72	40	23	2	2	/	/	/	2	3
Кривични дела против слободите и правата на човекот и граѓанинот	1	/	1	/	2	/	/	/	/	/	/	/
Кривични дела против половата слобода и половиот морал	19	/	19	9	6	3	1	/	/	/	/	/
Кривични дела против бракот, семејството и младината	3	/	3	3	/	/	/	/	/	/	/	/
Кривични дела против животната средина и природата	3	/	3	2	/	/	/	/	/	/	/	1
Кривични дела против имотот	947	25	967	334	226	27	332	/	2	3	24	19
Кривични дела против јавните финансии платниот промет и стопанството	12	/	12	4	6	/	1	/	/	/	/	1
Кривични дела против општата сигурност на луѓето и имотот	11	/	11	5	5	/	1	/	/	/	/	/
Кривични дела против безбедноста на јавниот сообраќај	62	5	67	33	22	2	4	/	/	/	1	5
Кривични дела против правосудството	2	/	2	1	/	/	/	/	/	/	/	1
Кривични дела против правниот сообраќај	25	11	36	24	9	/	2	/	/	/	1	/
Кривични дела против јавниот ред	27	2	29	15	10	1	1	/	/	/	1	1
Видови кривични дела (2008)	**М**	**Ж**	**Вк**	**Македонци**	**Албанци**	**Власи**	**Роми**	**Турци**	**Срби**	**Бошњаци**	**Останато**	**Непознато**
Кривични дела против животот и телото	84	/	84	62	10	/	6	/	/	/	2	4
Кривични дела против слободите и правата на човекот и граѓанинот	7	/	7	1	1	/	1	1	/	1	/	/
Кривични дела против честа и угледот	1	/	1	1	/	/	/	/	/	/	/	/
Кривични дела против половата слобода и половиот морал	18	/	18	4	7	/	2	4	/	/	1	/
Кривични дела против бракот, семејството и младината	4	/	4	/	3	/	1	/	/	/	/	/
Кривични дела против здравјето на луѓето	15	3	18	13	1	/	2	1	/	/	/	/
Кривични дела против животната средина и природата	4	/	4	3	1	/	/	/	/	/	/	/

Кривични дела против имотот	994	29	1023	408	166	/	366	28	2	2	18	39
Кривични дела против јавните финансии платниот промет и стопанството	21	/	21	17	4	/	/	/	/	/	/	/
Кривични дела против општата сигурност на луѓето и имотот	4	/	4	2	1	/	1	/	/	/	/	/
Кривични дела против безбедноста на јавниот сообраќај	72	5	77	44	29	/	2	1	/	/	/	1
Кривични дела против службена должност	1	/	1	/	1	/	/	/	/	/	/	/
Кривични дела против правосудството	8	4	12	10	1	/	/	/	/	/	/	1
Кривични дела против правниот сообраќај	20	5	25	15	8	/	/	1	/	/	/	1
Кривични дела против јавниот ред	53	/	53	17	26	/	5	3	2	/	/	1
Кривични дела од посебни закони	3	/	3	/	3	/	/	/	/	/	/	/
Видови кривични дела (2009)	**М**	**Ж**	**Вк**	**Македонци**	**Албанци**	**Власи**	**Роми**	**Турци**	**Срби**	**Бошњаци**	**Останато**	**Непознато**
Кривични дела против животот и телото	102	1	103	60	28	/	2	1	/	1	/	
Кривични дела против слободите и правата на човекот и граѓанинот	2	/	2	1	1	/	/	/	/	/	/	/
Кривични дела против изборите и гласањето	1	/	1	/	1	/	/	/	/	/	/	/
Кривични дела против честа и угледот	1	/	1	1	/	/	/	/	/	/	/	/
Кривични дела против половата слобода и половиот морал	17	/	17	4	7	/	6	/	/	/	/	/
Кривични дела против бракот, семејството и младината	1	/	1	/	/	/	1	/	/	/	/	/
Кривични дела против здравјето на луѓето	11	1	12	8	2	/	/	2	/	/	/	/
Кривични дела против имотот	1150	42	1192	469	249	1	295	35	6	6	17	14
Кривични дела против јавните финансии платниот промет и стопанството	10	2	12	9	2	/	/	/	/	/	1	/
Кривични дела против општата сигурност на луѓето и имотот	1	/	1	1	/	/	/	/	/	/	/	/
Кривични дела против безбедноста на јавниот сообраќај	81	7	88	44	31	/	6	1	1	/	1	4
Кривични дела против службената должност	1	/	1	/	1	/	/	/	/	/	/	/
Кривични дела против правосудството	6	4	10	5	2	/	1	/	/	1	1	/

Кривични дела против правниот сообраќај	6	2	8	5	1	/	1	1	/	/	/	/
Кривични дела против јавниот ред	69	1	70	35	21	/	11	/	/	/	/	3
Видови кривични дела (2010)	**М**	**Ж**	**Вк**	**Македонци**	**Албанци**	**Власи**	**Роми**	**Турци**	**Срби**	**Бошњаци**	**Останато**	**Непознато**
Кривични дела против животот и телото	106	1	107	71	25	/	4	2	2	3	/	/
Кривични дела против слободите и правата на човекот и граѓанинот	2	/	2	/	2	/	/	/	/	/	/	/
Кривични дела против честа и угледот	4	/	4	4	/	/	/	/	/	/	/	/
Кривични дела против половата слобода и половиот морал	12	4	/	/	/	/	7	1	/	/	/	/
Кривични дела против половата слобода и половиот морал	24	/	24	12	4	7	/	1	/	/	/	/
Кривични дела против бракот, семејството и младината	1	1	2	/	/	/	2	/	/	/	/	/
Кривични дела против здравјето на луѓето	14	/	14	11	2	/	1	/	/	/	/	/
Кривични дела против животната средина и природата	5	1	6	4	/	/	2	/	/	/	/	/
Кривични дела против имотот	917	20	937	362	189	/	310	56	4	4	10	2
Кривични дела против јавните финансии платниот промет и стопанството	14	/	14	10	2	/	/	1	1	/	/	/
Кривични дела против општата сигурност на луѓето и имотот	10	/	10	3	7	/	/	/	/	/	/	/
Кривични дела против јавните финансии, платниот промет и стопанството	14	/	14	10	2	/	/	1	1	/	/	/
Кривични дела против безбедноста на јавниот сообраќај	60	1	61	28	25	/	4	3	/	/	/	/
Кривични дела против правосудството	2	1	3	1	1	/	1	/	/	/	/	/
Кривични дела против правниот сообраќај	1	/	1	/	/	/	1	/	/	/	/	/
Кривични дела против јавниот ред	55	1	56	16	28	/	3	3	/	5	1	/
Кривични дела од посебни закони	2	/	2	/	1	/	/	1	/	/	/	/
Видови кривични дела (2011)	**М**	**Ж**	**Вк**	**Македонци**	**Албанци**	**Власи**	**Роми**	**Турци**	**Срби**	**Бошњаци**	**Останато**	**Непознато**
Кривични дела против животот и телото	87	1	88	57	20	/	1	5	/	2	3	/

Кривични дела против слободите и правата на човекот и граѓанинот	1	/	1	1	/	/	/	/	/	/	/	/
Кривични дела против половата слобода и половиот морал	14	/	14	1	/	/	/	/	/	/	/	/
Кривични дела против бракот, семејството и младината	2	1	3	/	1	/	1	/	/	/	1	/
Кривични дела против здравјето на луѓето	9	2	11	9	/	/	2	/	/	/	/	/
Кривични дела против имотот	899	16	917	312	246	/	301	31	1	4	11	11
Кривични дела против јавните финансии платниот промет и стопанството	12	2	14	6	6	/	/	/	/	/	2	/
Кривични дела против општата сигурност на луѓето и имотот	13	1	14	8	2	/	4	/	/	/	/	/
Кривични дела против безбедноста на јавниот сообраќај	41	2	43	18	14	/	3	3	/	/	1	4
Кривични дела против вооружените сили	1	/	1	/	1	/	/	/	/	/	/	/
Кривични дела против правосудството	2	/	2	/	1	/	/	1	/	/	/	/
Кривични дела против правниот сообраќај	7	/	7	2	5	/	/	/	/	/	/	/
Кривични дела против јавниот ред	44	1	45	20	12	/	9	3	/	/	1	/

Видови кривични дела (2012)	**М**	**Ж**	**Вк**	**Македонци**	**Албанци**	**Власи**	**Роми**	**Турци**	**Срби**	**Бошњаци**	**Останато**	**Непознато**
Кривични дела против животот и телото	59	1	60	39	12	/	1	1	1	5	/	1
Кривични дела против слободите и правата на човекот и граѓанинот	6	/	6	5	/	/	1	/	/	/	/	/
Кривични дела против половата слобода и половиот морал	10	/	10	2	5	/	1	1	/	/	1	/
Кривични дела против бракот, семејството и младината	1	1	2	1	/	/	1	/	/	/	/	/
Кривични дела против здравјето на луѓето	15	1	16	8	4	/	1	/	/	/	/	3
Кривични дела против имотот	753	20	773	276	157	/	269	49	1	2	8	11
Кривични дела против јавните финансии платниот промет и стопанството	10	/	10	5	1	/	2	/	1	1	/	/
Кривични дела против општата сигурност на луѓето и имотот	9	/	9	1	5	/	1	1	/	1	/	/
Кривични дела против безбедноста на јавниот сообраќај	49	1	50	25	17	/	3	1	/	/	2	2

Кривични дела против правосудството	5	1	6	/	4	/	1	/	/	/	/	1
Кривични дела против правниот сообраќај	1	1	1	1	/	/	/	/	/	/	/	/
Кривични дела против јавниот ред	51	1	52	25	18	/	7	1	1	/	/	/

Видови кривични дела (2013)	**М**	**Ж**	**Вк**	**Македонци**	**Албанци**	**Власи**	**Роми**	**Турци**	**Срби**	**Бошњаци**	**Останато**	**Непознато**
Кривични дела против животот и телото	63	3	66	36	16	1	4	2	/	4	/	3
Кривични дела против слободите и правата на човекот и граѓанинот	5	/	5	2	1	/	1	/	/	1	/	/
Кривични дела против половата слобода и половиот морал	19	/	19	2	9	/	6	2	/	/	/	/
Кривични дела против бракот, семејството и младината	3	1	4	1	1	/	2	/	/	/	/	/
Кривични дела против здравјето на луѓето	8	/	8	2	3	/	1	/	/	/	/	/
Кривични дела против имотот	723	22	745	251	182	/	237	29	2	18	4	22
Кривични дела против јавните финансии платниот промет и стопанството	4	/	4	3	1	/	/	/	/	/	/	/
Кривични дела против општата сигурност на луѓето и имотот	8	/	8	1	4	/	/	1	/	/	/	2
Кривични дела против безбедноста на јавниот сообраќај	27	1	28	15	8	/	2	1	/	1	/	1
Кривични дела против правосудството	/	1	1	1	/	/	/	/	/	/	/	/
Кривични дела против јавниот ред	116	1	117	41	59	/	4	4	1	1		7

Видови кривични дела (2014)	**М**	**Ж**	**Вк**	**Македонци**	**Албанци**	**Власи**	**Роми**	**Турци**	**Срби**	**Бошњаци**	**Останато**	**Непознато**
Кривични дела против животот и телото	61	3	64	41	11	/	4	1	2	1	/	4
Кривични дела против слободите и правата на човекот и граѓанинот	4	1	5	3	1	/	1	/	/	/	/	/
Кривични дела против половата слобода и половиот морал	25	/	25	8	3	/	12	/	/	/	/	/
Кривични дела против бракот, семејството и младината	1	/	1	/	/	/	1	/	/	/	/	/
Кривични дела против здравјето на луѓето	20	3	23	10	7	/	5	/	/	/	/	1
Кривични дела против имотот	613	41	654	204	118	/	262	14	1	6	3	46

Кривични дела против јавните финансии платниот промет и стопанството	5	/	5	1	3	/	/	/	/	/	/	1
Кривични дела против општата сигурност на луѓето и имотот	6	/	6	1	2	/	3	/	/	/	/	/
Кривични дела против безбедноста на јавниот сообраќај	26	3	29	11	11	/	2	/	/	/	1	4
Кривични дела против правосудството	2	/	2	1	/	/	/	/	/	/	/	1
Кривични дела против јавниот ред	151	6	156	67	56	/	9	2	/	1	/	21
Видови кривични дела (2015)	**М**	**Ж**	**Вк**	**Македонци**	**Албанци**	**Власи**	**Роми**	**Турци**	**Срби**	**Бошњаци**	**Останато**	**Непознато**
Кривични дела против животот и телото	67	1	68	30	16	/	12	3	1	/	1	5
Кривични дела против слободите и правата на човекот и граѓанинот	2	1	3	1	/	/	1	/	/	/	1	/
Кривични дела против половата слобода и половиот морал	18	1	19	7	1	/	8	1	/	1	/	1
Кривични дела против бракот, семејството и младината	/	1	1	/	/	/	1	/	/	/	/	/
Кривични дела против здравјето на луѓето	19	1	20	13	6	/	1	/	/	/	/	/
Кривични дела против имотот	493	27	520	178	78	/	216	10	2	6	4	26
Кривични дела против јавните финансии платниот промет и стопанството	2	/	2	/	2	/	/	/	/	/	/	/
Кривични дела против општата сигурност на луѓето и имотот	3	1	4	1	/	/	2	/	/	1	/	/
Кривични дела против безбедноста на јавниот сообраќај	30	3	33	17	12	/	2	1	/	/	1	/
Кривични дела против правосудството	/	1	1	/	/	/	/	/	/	/	/	1
Кривични дела против јавниот ред	100	/	100	55	18	/	14	3	1	3	1	5
Видови кривични дела (2016)	**М**	**Ж**	**Вк**	**Македонци**	**Албанци**	**Власи**	**Роми**	**Турци**	**Срби**	**Бошњаци**	**Останато**	**Непознато**
Кривични дела против животот и телото	50	3	53	29	19	1	1	1	/	1	/	1
Кривични дела против слободите и правата на човекот и граѓанинот	8	3	11	5	2	/	3	1	/	/	/	/
Кривични дела против половата слобода и половиот морал	4	/	4	1	1	/	2	/	/	/	/	/
Кривични дела против здравјето на луѓето	7	/	7	6	1	/	/	/	/	/	/	/

Кривични дела против имотот	376	23	399	107	95	/	107	5	/	16	1	5
Кривични дела против јавните финансии платниот промет и стопанството	5	/	5	2	3	/	/	/	/	/	/	/
Кривични дела против општата сигурност на луѓето и имотот	4	/	4	1	1	/	1	/	/	1	/	/
Кривични дела против безбедноста на јавниот сообраќај	23	2	25	14	5	/	4	2	/	/	/	/
Кривични дела против јавниот ред	65	1	66	21	30	/	8	1	/	6	/	/
Останати кривични дела	10	3	13	8	1	/	1	2	1	/	/	/

Извор: Државен завод за статистика

Имајќи ги предвид горенаведените статистички податоци лесно може да се разликува положбата на машкиот пол при извршување на кривичните дела во однос на женскиот пол. Статистичките податоци на женските сторители на кривични дела во компарација со машките е незначителна а оттука важно е да се сподели дека машките претежно се насилни при извршување на кривични дела, додека кај женските наведената карактеристика не е многу застапена. Анализата во рамките на 2007-2016 година покажува дека на прво место најзастапеното кривично дело е кривичното дело против имотот потоа следуваат кривичните дела против животот и телото, кривичните дела против јавниот ред и четвртото најзастапено дело е кривично дело против безбедноста на јавниот сообраќај

1.1 Карактеристики на малолетничкиот криминалитет

Карактеристиките на малолетничкиот криминалитет ги согледуваме преку одредени варијабли, и тоа: пол, возраст, материјален статус, повратност и место на живеење на малолетникот. Сите горенаведени варијабли како фактори, на директен начин влијаат врз развојот на малолетникот. Современиот малолетнички криминалитет се карактеризира со организираност на младите во малолетнички групи или банди заради сторување на кривични дела. Во различни земји, малолетничките банди имаат различни имиња, така во Англија се викаат “teddy boys”, во САД ”teenagers”, во Франција “blausos noires”, во Јапонија”tao zoku”.[182]

1.1.1 Пол

Малолетничкиот криминалитет и криминалитетот, воопшто, сè уште кај нас и во светот се карактеризира како машка појава. Тука се земаат во предвид агресијата, бруталноста, насилството, тепачките и слични појави. Учеството на женските малолетници во криминалитетот е многу понизок за разлика од оној на машките. Но, доколку би требало да направиме една класификација во однос на учество на малолетниците во кривични дела според полот, тогаш важно е да се каже дака, машките малолетници повеќе учествуваат во насилничкиот криминалитет, додека женските малолетнички учествуваат и во

[182] Dinitz, Simon, Dynes, Rowe Russell, Clarke, Alfred, “Deviance; studies in the process of stigmatization and societal reaction”, Oxford University Press, London, 1969, стр.30

проституцијата. Статистичките податоци покажуваат дека најголемиот број проститутки се полнолетни, но малолетните се јавуваат како резерва за постојано пополнување. Проституцијата на младите најчесто е резултат на судири во семејството или опфатеност со други социопатолошки појави. Се покажува дека бројот на малолетните проститутки постојано се зголемува.[183]

1.1.2 Возраст

Варијаблата возраст игра значајна улога во рамките на малолетничкиот криминалитет, бидејќи станува збор за деца и нивниот развој, па оттука и нивните позитивни и негативни особини коишто ги примаат од семејството и околината. Возраста кај малолетници како посебна концепција на истражување ги интересира и детската психологија и социологијата. При развојот на детето треба да се внимава и на основните особини како што се: способностите, мотивациско-емоционалните диспозиции, социјално-општествените диспозиции, когнитивните фактори (интелигенција, комуникација и карактер) и темпераментот.[184]

Интересен е фактот што кај децата од 4-12 години се забележува повеќе учество во питачењето, кај помладите малолетници, односно од 14 до 16 годишна возраст, постои промена во однесувањето и карактерот затоа што тоа е период кога детето го завршува основното образование и преминува во средно образование, во рамките на овој временски интервал запознава нова околина и голема е веројатноста заради нестабилноста на карактерот и периодот на пубертет да го започне својот криминален живот. Во овие години најчесто малолетните стануваат дел од: тепачки, алкохолизам, дрога, вагабундажа и имотни деликти. Кај постарите малолетници т.е од 16 го 18 годишна возраст најчесто се бележат кривични дела против: имотот, безбедноста на јавниот сообраќај, против животот и телото и јавниот ред.

1.1.3 Повратност

Порастот на повторот т.е рецидивизмот е значаен индикатор на неуспех на казнената политика. Врз таа основа тој се потврдува како тврдокорна и отпорна појава на мерките што општеството ги презема за неговото спречување.[185] Примената на казните се покажува дека не ги дава очекуваните резултати. Забележано е дека сите повратници, својата криминална кариера ја започнале како малолетници. Фактори што влијаат за намалување на повторот кај малолетниците се следните: училишниот успех и способностите, стилот на учење и усвојување нови вештини, способноста за емпатија и воспоставување врски, волјата да се промени однесувањето, мотивацијата за разрешување на животните проблеми итн.[186]

Рецидивизмот е специфичен проблем на која му се посветува посебно внимание од криминолошки, кривично-правен и криминално-политички аспект. Голем дел од пријавените малолетници не се изведуваат пред суд, доколку за

---

[183] Арнаудовски, Љупчо, "Социјална Патологија", Студентски збор, Скопје, 1983, стр.321

[184] Станковска, Гордана, Руси, Муќереме, "Медицинска психологија", Пергамент публик, Скопје, 2011, стр.53

[185] И, Јосифовски, "Криминалитетот и другите облици на девијантно поведение како израз на отуѓеност на човекот, Докторска дизертација, Љубљана, 1965, стр. 99

[186] Ковачевиќ, Ранко, Суљагиќ, Семир, Љуца, Џенита, Муфиќ, Един, "Рецидивизмот по третман во дисциплински центар за малолетници", Факултет за специјална едукација и рехабилитација, Тузла, 2014, стр.46

време на извршување на кривичното дело немале 14 години. Рецидивизмот кај малолетниците не е толку висока бидејќи 4 години (14-18) е релативно краток период за да лицето може да рецидивира.[187]

2.2.4. Материјален статус на делинквенот

Во Република Македонија материјалниот статус на семејствата е променлива категорија. Невработеноста и сиромаштијата не само што создаваат неповолни услови за живот, туку и стануваат една од причините на нарушување на односот помеѓу детето и родителот. Нискиот социо-економски статус на семејството, се наведува како основна причина за нивно девијантно однесување. Меѓусебните односи помеѓу родителите и децата, добро ангажирање на времето и максимален надзор врз детето може да ја надвладее лошата економска состојба, односно сите овие активности на некој начин помагаат за детето да не го осети лошиот материјален статус во семејството, а и со тоа да не биде дел од криминалитетот.

Заклучок

Децата не ги чувствуваат длабоките промени во општеството, заради тоа што имаат многу нови работи околу себе што им го привлекува вниманието, а тоа се: околината, училиштето, активностите што ги вршат во слободно време.

Велиме појдовните точки на малолетничкиот криминалитет се: лошото примарно воспитување од страна на семејството, недоволен надзор од страна на родителите, неквалитетното образование, лошата околина и криминогените фактори особено невработеноста и сиромаштијата кои директно влијаат врз семејството и децата.

Развивањето на националната правна рамка од областа на малолетничка правда и усвојувањето на разни меѓународни конвенции не се доволни за сузбивање на малолтничкиот криминал .

Прво, не треба да се чека за појава на некое проблематично дејствие кое во иднина ќе прерасне во криминал, за да се донесе соодветно решение, туку напротив општеството и општествените институции секогаш треба да ги претпоставуваат причините и имајќи ги во предвид сите претпоставки да подготвуваат програми пред да се појави проблемот.

Посакуваниот ефект околу намалувањето на малолетничкиот криминалитет ќе се добие откако ќе се развијат превентивни програми за криминал на малолетници кои се насочени кон елиминирање на факторите кои би предизвикале сторување на кривични дела од страна на малолетници.

Второ, треба да се инвестира во создавање на институции кадешто децата ќе го минуваат слободното време со рекреативна настава: спорт, цртање, музички рекреации, театарски претстави и сл. Овие институции ќе му овозможат на малолетникот своето слободно време да го минува продуктивно за разлика од шетање низ маало или стапување во врска со гета.

Трето, треба да се обврне внимание на создавање на „програми за превенција на малолетничкиот криминалитет“ кои се покажаа доста ефикасни во развие-

[187] Груевска-Дракулевски, Александра “Рецидивизам код малолетничког криминалитета у Републици Македонији као индикатор за (не)ефикасност казнене политике“ у Зборник радова Двадесет и првог сусрета на тема: Право и индивидуалне вредности, Правни живот, часопис са правну теорију и праксу, Копаоничка школа природног права Удружења правника Србије, Београд, 2008, стр. 3-4

ните земји преку едукација на малолетници, нивните семејства и блиската околина.

Користена литература

1. Арнаудовски, Љупчо (2007),“Криминологија, 2-ри Август – Штип, Скопје
2. Арнаудовски, Љупчо (1983),“Социјална Патологија“, Студентски збор, Скопје
3. Велкова, Татјана (2006), “Феноменологија на малолетничкиот криминалитет во Република Македонија во периодот1982-2000 година“, 2-ри Август Ц-Штип, Скопје
4. Груевска-Дракулевски, Александра (2008), “Рецидивизам код малолетничког криминалитета у Републици Македонији као индикатор за (не)ефикасност казнене политике“ у Зборник радова Двадесет и првог сусрета на тема: Право и индивидуалне вредности, Правни живот, часопис са правну теорију и праксу, Копаоничка школа природног права Удружења правника Србије, Београд
5. И, Јосифовски(1965), “Криминалитетот и другите облици на девијантно поведение како израз на отуѓеност на човекот, Докторска дизертација, Љубљана
6. И. Јосифовски, Љ. Арнаудовски (1963),“За статистиките за криминалитетот“ Институт за социјални и политичко правни истражувања, Скопје
7. Ковачевиќ, Ранко, Суљагиќ, Семир, Љуца, Џенита, Муфиќ, Един (2014), “Рецидивизмот по третман во дисциплински центар за малолетници“, Факултет за специјална едукација и рехабилитација, Тузла
8. Љ.Чонева, В.Чачева, Љ.Арнаудовски, М.Станкова, М.Марковиќ, Г.Станковска (2007),“Малолетничкиот криминалитет во транзицијата во Република Македонија“, Институт за социолошки и политичко-правни истражувања, Скопје
9. Станковска, Гордана, Руси, Муќереме (2011), “Медицинска психологија“, Пергамент публик, Скопје
10. Dinitz, Simon, Dynes, Rowe Russell, Clarke, Alfred (1969), “Deviance; studies in the process of stigmatization and societal reaction”, Oxford University Press, London
11. Durak, İzzet (2013), “Suç Öncesi ve Sonrası Suçlu Piskolojisi“, Kitapyurdu, İstanbul
12. УНИЦЕФ(2004), “Ефикасноста на мерките што се применуваат спрема малолетните лица“, Институт за социолошки и политичко правни истражувања, Скопје
13. http://www.stat.gov.mk

М- р Виолета Паунковска
ЕУРМ – Скопје
Тел: 076/220-191; Емаил: violeta.paunkovska@eurm.edu.mk

ДИГИТАЛНАТА ТРАНСФОРМАЦИЈА, ИМПЕРАТИВ ВО БИЗНИСОТ, АКАДЕМСКАТА ЗАЕДНИЦА И МОДЕРНИТЕ КОРПОРАЦИИ

АПСТРАКТ
Во овој труд сакам да ја истакнам неодложната потреба на современата дигитална технологија на која мора да се одговори во глобалниот пазар на корпоративните компании како и академските заедници. Некои од нив иако се исклучително успешни ги менуваат целите индустрии. Затоа дигиталната трансформација стана неопходност за зрелите, веќе воспоставените компании кои сакаат да бидат конкурентни под нови дигитални термини. Се отвораат академии кои се насочени кон сите што сакаат да го интензивираат знаењето во дигиталната транформација. Тие најчесто се дизајнирани за директори во правниот сектор, директори за маркетинг продажба, бизнис архитекти, менаџери на деловни единици, аналитичари, управување со хумани ресурси и друго.
Дигиталната трансформација е исклучиво тешка задача за менаџерите и нивните компании бидејќи потребни се екипи со повеќе вештини кои ќе работат со интегриран интензитет. Често се потребни и радикални промени во самите компании за кои би можеле да бидат неуспешни ако не се приближат на вистинскиот начин.

Клучни зборови: глобален пазар, академски заедници, процес на дигитализација, дизајнерски тим, дигитален талент.

DIGITAL TRANSFORMATION, IMPERATIVE IN THE BUSINESS, THE ACADEMIC COMMUNITY AND MODERN CORPORATIONS

ABSTRACT
In this paper, I want to emphasize the urgent need of modern digital technology, which must be answered in the global market of corporate companies and the academic community. Some of them, although they are extremely successful, are changing entire industries. Therefore, digital transformation has become a necessity for mature, already established companies that want to be competitive under new digital terms. Academies are open to those who like to intensify their knowledge in digital transformation. They are most often designed for law enforcement directors, marketing sales executives, business architects, work unit managers, analysts, human resources management and others.
Digital transformation is an extremely difficult task for managers and their companies because teams with more skills are required to work with integrated intensity. Often radical changes are needed in the companies themselves, which could be unsuccessful if they do not get the right way.

Keywords: global market, academic communities, digitization process, design team, digital talent.

ВОВЕД

Важна улога во сите свери на животот и работата на современото општество како што се индустријата, медицината, образованието, трговијата па дури и функционирањето на власта е развојот на техниката и технологиите. Всушност со развојот и примената на електронските системи во сверата на дизајнот, анализата, експлоатацијата и севкупните општествени аспекти се менува и самата парадигма на поимот општество т.н. електронско општество.
Најголемиот фокус на академската заедница, модерните корпорации и образовните системи веќе не се само обезбедување на квалитет во истите, туку како тие да се релевантно за моменталните и идни потреби на пазарот на трудот, кои многу брзо се менуваат, да обезбедат можности за секого, како и да одговараат на постојаните промени носени од глобализацијата и технолошкиот развој. Информатичката и комуникациска технологија, телевизијата, радиото, компјутерите, телефоните и интерентот, се оние алатки кои го имаат потенцијалот да ја потпомогнат промената и реформата во општеството. Ако правилно се користат, овие алатки можат да обезбедат пристап до информации и можности за учење, да ја зголемат релевантноста за потребите на пазарот на труд, и да го подобрат квалитетот на учење со поврзување на темите, активностите и проблемите со секојдневни ситуации од реалниот живот.
Како дигиталната трансформација и структурираните бази влијаат врз мотивацијата на вработените во модерните корпорации и ја олеснуваат нивната работа, како и нивното влијание врз поуспешното совладување на истата? Многу компании се свесни за промените (или веќе чувствуваат) и имаат визија за тоа како ќе ја бранат својата дигитална конкуренција. Прашањето е како да се воведат промени во пракса или како да се подготват вработените за нив?
Дигиталната трансформација започнува со луѓето. Таа е во полн замав и ништо повеќе не може да ја запре. Неопходно е во компаниите да се прилагодат на неа, ако сакаат да бидат во бурна бизнис средина, со традиционални врски и секој ден да создаваат нови бизнис модели. Во дијалог со сите засегнати страни, администрацијата мора да воспостави свест за итноста и промените и да најде лице кое ќе ги насочи овие промени и ќе ги привлече вистинските луѓе кон проектот. Со самото тоа што технологијата е се поприсутна, ова ќе биде голем предизвик за сите компнии во наредните години. Експертите од оваа област се повеќе се побарувани, затоа грижата за мотивација на постојаниот кадар и прилекувањето на дефицитарните кадри во областа на дигитализација ќе бидат централна задача на администрациите во наредните години.

ИСТОРИЈА НА ДИГИТАЛИЗАЦИЈАТА И НЕЈЗИНИТЕ ПРЕДНОСТИ ВО БИЗНИСОТ

Почетокот на инженерската технологија за генерирање и толкување на сигнали е означен во дваесетиот век со пронаоѓањето на телеграфот за пишување и гласовниот телефон. Теоријата на сигналот почна да се

разделува како посебна техничка, инженерска и научна дисциплина, независно од самата математика.

,,Првите теоретски врски помеѓу аналогните и дискретни сигнали беа откриени од страна на Nyquist, 20-ти години на минатиот век, истражување на оптимални телеграфски механизми за пренос. Шенон го надгради откритието на Никола и ја формира теоремата Шенон-Никола семплификација, која го доведува во прашање бројот на примероци доволно за сигналот што треба да биде верно реконструиран на еден многу убав начин. Наскоро, кон крајот на 1940-тите, се појавиле дигитални компјутери. Сепак, тие исто така беа сеуште премногу бавни и немаа можност да складираат доволно голем број на броеви, колку што е потребна за обработка на дигитални сигнали. На крајот на 80-тите, со брзиот развој на компјутерите и со зголемување на нивната меморија, т.е. складирање и складирање на податоци, како и изглед компактен диск, кој е со префрлување од магнетна во оптички, исто така овозможија складирање и пренос на значително поголеми количини на податоци од претходно, сите пречки што ги имаат развојот на обработка на дигитални сигнали е решен. Почеток на дигитализација ...'' [188]

Дигиталната технологија има големи предности во однос на аналогните - квалитетот на информациите не е зависи од квалитетот на медиумите, што резултира со фактот дека квалитетот на копирање е неспоредливо подобар од квалитетот на истиот во аналогната технологија - копијата е целосно идентична со оригиналот. Процесот на дигитализација создава организација без присуство на хартија во кој се користат професионални оператори кои заштедуваат на време, пари, фрустрации. Бизнисот треба да се води без хартија односно без пишување, причини за тоа се:

- Нема физички ограничувања за складирање
- Може да се пристапи преку Интернет
- 24/7 достапност на пристап
- Голема заштеда на простор (пример: библиотека)
- Зачувување на стари текстови / ракописи
- Лесно пронаоѓање на информации користејќи клучни зборови
- Интегрирано споделување на интернет-ресурси
- Поевтино е да се задржи дигиталната библиотека од библиотеката за книги
- Поврзување и мрежни можности
- Колку пати дигиталните датотеки можат да се удвојат со точност.
- Многумина можат истовремено да пристапат до дигитална датотека.
- Тактички предности на дигитализацијата.[189]

Клучната тактичка корист од дигитализацијата е да се подобри ефикасноста на клучните деловни процеси - корист што доаѓа преку искористување на тактичките предности понудени од дигитализацијата. Фаќањето документи и

[188] http://www.sveti-sava.edu.rs/otpremljeno/Digitalizacija1.pdf
[189] http://www.managedoutsource.com/blog/2007/10/advantages-of-digitization.html

податоци на местото на потекло или приемот во организацијата овозможува многу тактички предности, вклучувајќи, но не ограничувајќи се на:

- Елиминирање на транскрипционите грешки
- Спроведување на електронски процеси на работа
- Создавање ревизорски траги
- Спроведување на безбедносни протоколи
- Креирање на еден извор на вистината за секој документ / предмет на податоци
- Подобрување на достапноста до информации
- Интегрирање на деловните системи.[190]

За постигнување на горенаведеното потребна е личност со искуство за да ги евидентира и управува овие информации со што ќе произлезат поволни финансиски бенифиции.Но, позади оваа личност потребен е цел административен и дизајнерски тим, соработници надворешни и внатрешни. Затоа во компаниите потребни се работници кои ја разбираат ситуацијата и ќе се залагаат за промени. Тим кој ќе воспостави врска помеѓу поединечните оделенија и потесниот дигитален тим.

ДИГИТАЛНАТА ТРАНФОРМАЦИЈА ВО ОБРАЗОВНИОТ ПРОЦЕС И АКАДЕМСКАТА ЗАЕДНИЦА

Се смета дека образованието е една од последните институции во која се прават големи промени и истите се држат на застарени методи и практики. Дигиталната технологија е таа која во последната деценија овозможи пораст на образовната технологија во која професорскиот кадар почна драстично да ги менува своите инструкции, проценки, воедно и промена на физичката структура во самите предавални за полесно учење. Значи едукаторите од сите нивоа добија голема придобивка од дигиталната технологија.

Овие актуелни трендови воведуваат наслови во образованието, поради начините на кои тие влијаат врз учењето на учениците:з големена реалност, виртуелна реалност, мешана реалност.

Деновите во кои студентите и учениците тивко седеа во своите клупи за време на предавањата, помина. На сметка, на дигитална транформација нивното учење се сведе на интерактивно и ,,online" учење. Се зголеми виртуелната и мешана реалност која истовремено создаде интересни и забавни часови за студентот и ученикот.Со виртуелната реалност надворешниот свет е внесен во училницата и обратно. На пример: апликацијата ,, Unimersiv" може да ги пренесе учениците во Античка Грција или ,,Cospaces" им овозможува на учениците да ги споделат своите креации виртуелно низ светот. Всушност оваа виртуелна реалност овозможува зголемување на визуелната писменост, технолошката писменост и внимание кон публиката. Студентите не мора да одат до технолошката лабараторија за да имаат пристап до комјутер. Последните години во образовните институции, училниците се обезбедија со компјутери што беше овозможено во дел од државното финансирање. Денешното ,,online" окружување претставува возбудлива можност за студентите и

[190] http://www.changefactory.com.au/our-thinking/articles/benefits-digitisation/

учениците правилно да се едуцираат, истото така и сајбер безбедност и индивидуална одговорност.
Ширум светот отворени се многу Академии за дигитална трансформација чија цел е едукација на сите организациски нивоа за задоволување на бизнис целите. Од нивните наставни програми имаат корист сите. На пример: програма за индустријата, применети практични проекти, релевантни студии на случај и други интегрирани методологии за стекнување практично искуство со користење на најновите дигитални алатки и технологии и всушност да ги имплементираме за вашата организација.
,,Академијата за дигитална трансформација е дизајнирана да ги едуцира донесувачите на одлуки за новите технологии кои ќе имаат потенцијално значително влијание врз бизнисот и како да ги насочат во бизнис план и да ја искористат можноста што ја носат. Академијата Totally Gaming Academy и GamCrowd ги здружија силите за опремување на гејмерската индустрија со увид потребни за да се осигура дека бизнисите се свесни, опремени и подготвени за технолошката револуција. Директорот на курсот, Крис Север, заедно со 4 стручни обучувачи, кои вклучуваат од учесници во индустријата, ќе ви дадат увид во клучните технолошки трендови кои влијаат на индустријата за коцкање и како да се насочи и да се подготват за нив."[191]
,,Мисијата на Simplearn е да ги задржи вашите вработени актуелни во најновите технолошки вештини и сертификати. Денешните организации се соочуваат со најголемата промена на технологијата во последниве децении, дигитална трансформација. За да ве подготвиме со основните знаења и алатки кои ја водат оваа деловна револуција, Simplilearn ја објавува својата Дигитална трансформациска академија. Дигиталната технологија се развива со неверојатна брзина. Организации кои не успеваат да се здобијат со нови вештини и да се прилагодат на променливите процеси ризикуваат исчезнување од денешниот деловен свет."[192]
Промените што произлегуваат од оваа постапка создаваат огромни можности и придобивки за компаниите кои прво ќе ја разберат и усвојат стратегијата на дигитална трансформација и ефикасно ќе ја спроведат во своите внатрешни структури.

ДИГИТАЛНО ВРЕМЕ НА МОДЕРНАТА КОРПОРАЦИЈА

Да размислиме за зголемениот број на компании кои стартуваат со технологијата и прават нешто што некогаш изгледаше незамисливо: предизвик и нарушување на традиционалните корпоративни гиганти. Дури и оние кои работат во индустриите кои традиционално не се сметаат за индустрии поврзани со технологијата, не биле поштедени од влијанието на новите пристигнувања и како резултат на трансформацијата во деловното опкружување. Со порастот на дигиталните технологии, секоја корпорација сега мора да стане агилна, иновативна и што е уште поважно, да дејствува како да се динамични технолошки компании. Игнорирањето на предизвикот од мрежната возраст и дигиталната револуција веќе не е опција, бидејќи само ќе го забрза падот и неуспехот на големите корпорации.

[191] http://www.totallygamingacademy.com/digital-transformation-academy
[192] https://www.simplilearn.com/simplilearn-digital-transformation-academy-article

Значи, како треба да работат големи, добро воспоставени корпорации во денешното деловно опкружување? Одговорот се чини едноставен: со учење од најиновативните (особено старт-ап) компании. Значајно е што овие понови компании ги совладале четири дигитални технологии при развивање на нови важни производи и услуги, имено cloud computing, големи податоци, мобилни и социјални медиуми. Процесите на донесување одлуки сè повеќе се засноваат на дигитални податоци, дигиталните стапалки стануваат важен фактор за успех, а политиките во врска со употребата на дигиталните технологии се прилагодени на очекувањата на потрошувачите. Што е најважно, производите и услугите во моментов се дизајнирани со дигитални технологии во умот. Овие стартапи имаат корист од можностите што ги нуди зголемената глобална поврзаност.

Компаниите кои се способни да се препознаат себеси со прифаќањето на претприемачкиот дух или враќањето на "чувството за почеток" веројатно се најдобро подготвени за идните можности и предизвици. Развивањето на подобро разбирање за тоа како може да се направи ова може да обезбеди основа за внатрешни организациони реформи, како и повторно размислување за значењето на корпоративното управување во мрежна и дигитална ера. Структурите на корпоративното управување на фирмите, кои го изгубиле почетното чувство, исто така, имаат потреба од дотерување. Меѓутоа, еден од главните проблеми е тоа што регулаторното опкружување создаде корпоративна култура во која односот меѓу менаџерите, директорите и инвеститорите е хиерархијата е базиран на агенции. Како резултат на ова, акционерите и одборите на директори имаат тенденција да се фокусираат на контролата на раководното несоодветно однесување и следењето на претходните перформанси и одржливост на компанијата, наместо активно да придонесуваат за нејзиниот иден успех. Фактот дека академските теории типично го гледаат ,,одвојувањето на сопственоста и контролата" како еден од обележјата на модерната корпорација не помага. Постојат примери за воспоставени корпорации кои биле во можност да го задржат или вратат моделот ориентиран кон иновации, и покрај агенциската и претерано регулираната околина. Овие корпорации во суштина се доведување до уметноста на измислување на иновативни производи и градење на пионерски бизниси назад во првите редови на нивните активности. Компаниите кои се најдобри во нивната класа самите презеле за да дизајнираат практики на управување што ги направија подобри иноватори.

Заедничко за сите овие компании е начинот на управување од директори со визионерски дух кои позиционираат како ,,менаџерски партнери'' или доминантни лидери на ,,корпоративно партнерство''. Овие компании имаат инклузивен колективен стил на управување во кој засегнатите страни се сметаат за заедница која работи заедно за создавање релевантни нови производи и услуги.

ЗАКЛУЧОК

Мора да се прифати фактот дека технологијата не е таа која е водич во дигиталната трансформација на една компанија, бизнис и академска заедница. Зад се ова стои цел дизајнерски тим, дигитален талент кој со својот потенцијал го достигнува врвот на глобалниот пазар. Корисничкото искуство

оди уште подалеку, надвор од дигиталните канали на комуникацијата кое треба да биде еден од основните делови на современиот маркетинг. Поголем дел од компаниите го постигнаа ова ниво со фокусирање на целокупното искуство вклучувајќи го и односот на потрошувачите.

Дигиталната трансформација гледана од бизнис перспектива мора да се носи со: траспарентност, флуидни работни позиции, одлуки базирани на податоци, мултидисциплинарни тимови подготвени да прифатат неуспех, но и да ја прифатат идејата што доаѓа од различни места, желни за учење и прифаќање на промена. Дигиталната трансформација мора да е реализирана од големите консултантски куќи за да не биде турната на оперативно ниво од креативните маркетинг агенции кои порано ја имаат прифатено оваа промена и се свесни за нејзиниот императив да ги променат начините на кои се пристапува кон бизнис размислувањето.

Во едно сите се сигурни и обединети а тоа е дека дигиталната трансформација значи далеку повеќе од прифаќање на нови технологии. Таа значи голема инвестиција во нацрт планови и разбирање на новите, различни искуства за сите подеднакво и соодветна промена на целокупниот однос кон нив.

Користена литература

1. Национален проект "Хрватско културно наследство", Дигитализација на архивски, библиотечни и музејски згради, Загреб 2007, Насоки за избор на објекти за дигитализација, Работна верзија.
2. ,,Насоки за дигитализациски проекти'', Национална библиотека на Црна Гора,, Ѓурѓе Црнојевиќ.
3. CONWAY, P. (2001). Проект за управување, и зачувување опции во дигитален светот: да снимате или да скенирате. Andover, MA, Североисточна конзервација на документи, Центар.
4. ПЕТС, Д. И ПИКОВЕР, М. (2001). DISA: увид на африкански модел за дигитални,.Развој на библиотеки.
5. SITTS, M. K. (2000). Прирачник за дигитални проекти: алатка за управување за зачувување и пристап. Andover, MA, Североисточно зачувување на документи
6. НАСОКИ ЗА ДИГИТАЛИЗАЦИСКИ ПРОЕКТИ 97, Корисни извори
7. Здружение на колеџ и истражувачки библиотеки, САД Информативна писменост стандарди за компетентност за високо образование
8. Проект за дигитализација во Колорадо. Дигитална Лента со алатки.
9. ХАРВАРДСКА УНИВЕРЗИТЕТСКА БИБЛИОТЕКА. Избор за дигитализација. Одлучување.
10. Универзитет на Калифорнија, Лос Анџелес (УКЛА). Дигитални проекти. Проект управување.
11. http://www.dlib.org/dlib/november01/peters/11peters.html
12. http://www.nedcc.org/digital/dighome.htm
13. http://www.ala.org/acrl/ilcomstan.html
14. http://coloradodigital.coalliance.org/toolbox.html
15. http://coloradodigital.coalliance.org/toolbox.html
16. http://preserve.harvard.edu/bibliographies/matrix.pdf
17. http://digital.library.ucla.edu/about/estimating/projectmanagement.html
18. http://www.managedoutsource.com/blog/2007/10/advantages-of-digitization.html
19. http://www.sveti-sava.edu.rs/otpremljeno/Digitalizacija1.pdf
20. http://www.changefactory.com.au/our-thinking/articles/benefits-digitisation/
21. http://www.totallygamingacademy.com/digital-transformation-academy
22. http://www.totallygamingacademy.com/digital-transformation-academy

М-р Тања Крстева
Европски Универзитет Република Македонија
Тел: +38978201900
Е-маил: Email: tanja.krsteva@eurm.edu.mk

Предизвиците и стратегиите на дигиталната деловна трансформација

АПСТРАКТ
Организациите од сите големини во целиот свет се обединети во разговорот околу една тема: дигитална деловна трансформација. Дигиталната трансформација е околу нас. Дигиталното нарушување е опсесија број еден што ги прогонува денешните менаџерски тимови низ целиот свет. Иако тоа може да значи различни работи на различни луѓе, лидерите насекаде ја гледаат вредноста која има цврста деловна технологија која ќе го забрза времето на пазарот, ќе ја оптимизира ефикасноста и ќе го подобри целокупното корисничко искуство- што во крајна линија ќе доведе до подобрена продажба, раст на бизнисот и намалување на трошоците.

Клучни зборови: Деловна трансформација, дигитална трансформација, интернет, стратегии, ЕРП.

The Challenges and Strategies Behind Digital Business Transformation

ABSTRACT
Organizations of all sizes throughout the world are united in a conversation around a single topic: digital business transformation. Digital transformation is all around us. Digital disruption is the number one obsession haunting today's management teams worldwide. While it may mean different things to different people, leaders everywhere see the value that having a solid business technology structure in place will speed time to market, optimize efficiency and improve the overall customer experience — ultimately leading to improved sales, business growth and reduced costs. Social institutions and commercial sectors across the board have experienced it, and are still going through it. The new digital-born enterprises are typically free of any physical assets such as fleets, factories, machinery and other goods.

Keywords: Business transformation, digital transformation, internet, strategies, ERP.

1. Going Digital?

Companies today are rushing headlong to become more digital. At any given point of time, every organization is focused on different things depending on their company maturity, industry/market trends, operational and tactical issues on hand and the long-term strategic initiatives. For some executives, it's about technology. For others, digital is a new way of engaging with customers. And for others still, it represents an entirely new way of doing business.

None of these definitions is necessarily incorrect. But such diverse perspectives often trip up leadership teams because they reflect a lack of alignment and common vision about where the business needs to go. This often results in piecemeal initiatives or misguided efforts that lead to missed opportunities, sluggish performance, or false starts.

Almost every company wants to "Go Digital." Being digital requires being open to reexamining your entire way of doing business and understanding where the new frontiers of value are. For some companies, capturing new frontiers may be about developing entirely new businesses in adjacent categories; for others, it may be about identifying and going after new value pools in existing sectors.

Unlocking value from emerging growth sectors requires a commitment to understanding the implications of developments in the marketplace and evaluating how they may present opportunities or threats. The Internet of Things, for example, is starting to open opportunities for disrupters to use unprecedented levels of data precision to identify flaws in existing value chains. In the automotive industry, cars connected to the outside world have expanded the frontiers for self-navigation and in-car entertainment. In the logistics industry, the use of sensors, big data, and analytics has enabled companies to improve the efficiency of their supply-chain operations.

At the same time, being digital means being closely attuned to how customer decision journeys are evolving in the broadest sense. That means understanding how customer behaviors and expectations are developing inside and outside your business, as well as outside your sector, which is crucial to getting ahead of trends that can deliver or destroy value.

2. Digital Tech Performance Challenges and Maturity

The meaning of "digital" differed significantly between organizations. The complexity of engagement was also wide-ranging. While some companies are effectively "defining industry 4.0", others are still focusing on getting all their staff "on to email". The term "digital" is clearly too vague and managers need to be specific about what they mean by digital in the context of the task at hand, or the company's business objectives.

The digital initiatives companies engaged in touched primarily on the marketing, sales and business processes. Where China differed significantly from the rest of the world is in its high engagement in activities related to data management and analytics, laying a strong foundation for future competitive advantage in a world that is becoming increasingly data driven.

Some managers may discover that it is their own world view which is inhibiting their own effectiveness. Those managers who have regarded management to be an acquired skill, which exists largely external to themselves may still be trying to reconcile these two opposing views. Other managers have made the simultaneous realization that it often is their own thinking that limits their performance.

In the hard systems approach improvement are seen as stemming from the achievement of four fundamental goals:

1. Reduction of uncertainty levels through rationalization,
2. Prediction of future states of the systems,
3. Preparation for these predicted future states

4. Control of all relevant forms of performance through negative feedback mechanisms, to assure efficiency.

Companies can have four levels of digital maturity: high digital and transformation management intensity, low digital and transformation management intensity, or mix of the two. Companies in the lower left are Digital Beginners. These businesses do very little with advanced digital capabilities, although they may be maturing with more traditional applications such as ERP or electronic commerce. Although companies may be Digital Begınners by choice, more often than not they are in this quadrant by accident.

Organizations in the top leeft are Digital Fashionistas. These companies have implemented or experimented with many digital applications. Some of these initiatives may create value, but many do not. While they may look good together, these digital aplications are not implemented with the vision of gaining synergies among the items. Digital Fashionistas are motivated to bring on digitally powered change, but their digital transformation strategy is not founded on real knowledge of how to maximize business benefits. Companies lacking enterprise-level governance may find they are in this quadrant at the corporate level, even if digital efforts are more mature in some business unites.

Transformation teams may add value by helping to translate business requirements into technology design requirements. It improvement opportunities may involve considering new systems, modifying existing systems, considering new IT governance approaches, or considering alternative sourcing options. The clients goals for these improvement efforts may be focused on IT performance, reliability and security. In a transformational context, the business performance goals are the ultimate objective, not the tehnology itself.

3. Social media

By leveraging social networks, companies can solicit not only their customers' ideas for product improvement, but also their feedback on product performance. For example, one food manufacturer has used "votes" on social forums to develop new flavors of potato chips.

Social media can also help companies customize products. Some companies also use data about consumer preferences to design the next versions of their products.

Analytics and big data enable data capture from vast and disparate audiences, which can lead to sharper insights and better decision making. Leading manufacturers can see how people are using their products, as well as what features are and are not popular. They can then leverage that information to help prioritize which new features to include in the next generation of vacuum cleaners, dishwashers, refrigerators and TVs.

By developing mobile applications that respond to what they learn about customer needs, top players are positioning themselves as potential winners in the connected world of the "Internet of things." Smartphone apps let property owners control domestic security systems while away from home; "intelligent" scales linked by WiFi to a pedometer app on a phone let exercisers know how many calories they've burned.

Mobility, of course, also enables greater PLM connectivity. Customers, employees and suppliers can communicate and participate in PLM processes more quickly and easily, reducing wait time and accelerating speed to market.
Then there's the cloud model. With its pay-per-use commercial framework, swift implementation and flexibility, it allows a company to quickly and efficiently scale up its computing needs during the early phase of product development and then scale back down later. This alleviates the need to continually build new engineering infrastructure to support product development—as well as the need to pay for such infrastructure when it's not in use.

CONCLUSION

Companies today are rushing headlong to become more digital. At any given point of time, every organization is focused on different things depending on their company maturity, industry/market trends, operational and tactical issues on hand and the long-term strategic initiatives. Being digital means being closely attuned to how customer decision journeys are evolving in the broadest sense.

The digital initiatives companies engaged in touched primarily on the marketing, sales and business processes. Companies can have four levels of digital maturity: high digital and transformation management intensity, low digital and transformation management intensity, or mix of the two. Transformation teams may add value by helping to translate business requirements into technology design requirements. The clients goals for these improvement efforts may be focused on IT performance, reliability and security. In a transformational context, the business performance goals are the ultimate objective, not the tehnology itself.
Social media can also help companies customize products. Some companies also use data about consumer preferences to design the next versions of their products.

REFERENCES

1. Ganesh Shermon, 2017, "Digital Talent - Business Models and Competencies", LULU Publishing, Raleigh, NC.
2. Ioan Hosu, Ioana Lancu, 2017, "Digital Entrepreneurship and Global Innovation ", Igi Global, USA

М-р Младен Трајков, Пензионер од МВР
М-р Александар Нацевски, Вработен во МВР

Корпорациската конспиративност-можност за побрз развој

АПСТРАКТ
Преку обработка на темата ,,Корпорациската конспиративност-можност за побрз развој", направен е обид за анализирање на правните инструменти и можностите кои стојат на располагање на менаџментот за примена и користење на корпорациската конспиративност која може да им послужи во нивниот побрз развој. Истовремено низ трудот провејува значењето на општата и конкретната конспиративност кои се поврзани со развојот на корпорацијата, иновациите, развојните механизми и друго. Преку конкретни механизми за примена на корпоративна конспиративност, овозможуваме на еден попластичен начин да се осознае значењето на овој инструмент за развојот на корпорацијата. Токму непочитувањето на корпорациската конспиративност, придонесува до развој на индустриската, технолошката и другите видови на шпионажа со што во светски рамки е многу тешко да се заштитат: иновациите, новите технологии и други механизми во развојот на корпорациите. Примери за претрпените штети од непочитување на корпорациската конспиративност се секојдневните производи (плагијати-фалсификати), примена на украдени иновации кои се развивани со години во една корпорација и за кои во развојната корпорација се потрошени огромни финансиски и други ресурси.

Клучни зборови: корпорација, конспиративност, развој

CORPORATE CONSPIRACY – THE OPPORTUNITY FOR FASTER DEVELOPMENT

ABSTRACT
Through the processing of the topic "Corporate Conspiracy - the opportunity for faster development", an attempt has been made to analyze the legal instruments and the possibilities available to the management for the application and use of corporate conspiracy that can serve them in their faster development. At the same time, the paper examines the significance of the general and concrete conspiracy that are related to the development of the corporation, innovations, development mechanisms, and so on. Through concrete mechanisms for applying corporate conspiracy, we enable in a more plastic way to become aware of the significance of this instrument for the development of the corporation. The disrespect of corporate conspiracy contributes to the development of industrial, technological and other types of espionage, which is very difficult to protect globally: innovations, new technologies and other mechanisms in the development of corporations. Examples of damage suffered by disrespecting corporate conspirators are the everyday products (plagiarism-fakes), the use of stolen innovations that have been developed for years by a corporation and for which huge financial and other resources have been spent in the development corporation.

Key words: corporation, conspiracy, development

Вовед

Развојот на современите технологии во светски рамки придонесе до зголемени можности и до леснодостапност и до оние информации[193] кои претставуваат како државни тајни така и индустриски и друг вид на тајни податоци, за кои постои интерес од нивно осозновање на конкурентски корпорации, други држави или поединци. Ваквата состојба со пристапот до информациите, од менаџментот во корпорациите бара развивање на нови способности, вештини и технологии како би ги заштитиле своите корпорациски интереси и сознанија со цел побрз општествен развој на корпорацијата. Токму заради ваквите моментални состојби во светски размери, истите не мотивираа да се позанимаваме со оваа тематика и малку подлабоко да навлеземе во истата со што истовремено на корпорацискиот менаџмент ќе му овозможиме поблиски информации за состојбите.

Дефинирање на корпорацискатa конспиративност

Со цел разјаснување на феноменот на тајноста во работењето а особено во развојот на корпорациите, ќе направиме обид преку дефинирање и објаснување на поимот консирација во делот на безбедноста да го објаниме и неговото значење за корпорациите.

Конспиративен (лат. conspirativus) заверенички, кој има карактер на завера, уротнички, таен, строго доверлив[194].

Конспирација (лат. conspiratio – завера, урота, тајност во работењео), систем и метод на подземните организации за заштита на тајноста на своето илегално работење и членовите на илегалната организација....[195]

Конспиративност лат. доверливост, тајност на работењето, скриеност од власта[196].

Претставените поими за конспиративност ни овозможуваат да осознаеме дека развојот на новите технологии во процесот на производството, развојот на новите производи кои овозможуваат примат во општеството, на пазарот и во економската свера се поврзани со велот на тајноста, се со цел, никој да не дознае на што се работи и што се развива како би се попречило стекнатите сознанија да дојдат до конкуренцијата а потрошените средства во развојот да не можат да се повратат бидејќи конкурентите први го изнеле производот на пазараот и остварile солидна финансиска добивка.

Механизми преку кои се штити корпоративната конспиративност

Заради заштита на сопствените интереси, корпорациите во својата структура и систематизација воспоставуваат однос на подреденост и надреденост но истовремено и врвен или топ менаџмент, кој што е надлежен за успешно работење и развој на корпорацијата. За секоја сериозна компанија, клучот и патот на развојот се поставени во мисијата и визијата на истата, а развојот, се одвива преку краткорочните, среднорочните и долгорочните планови. Според

---

[193] Информација е сознание кое може да биде пренесено во било која форма, предвидено во Закон за класифицирани информации, Службен весник на Република Македонија бр.9/2004, чл. 5, т. 1

[194] Милан Вујаклија, Лексикон страних речи и израза, Просвета Београд, 1980, Београд, стр. 455

[195] Обрен Ђорђевић, Лексикон безбедности, Партизанска књига, Београд, 1986, стр.162

[196] Љубо Миќуновиќ, Современ лексикон на странски зборови и изрази, Наша книга, Скопје, стр. 308

ваквата поставеност на работите неопходно е постигнување на целите кои се поставени а за тоа се надлежни менаџментот и секако одделот за развој. Со цел, успешно функционирање на внатрешната организација и системот, истите се објаснуваат и уредуваат со соодветни правилници, а од особена важност е правилникот за пристап до одредени информации и нивото кое е дозволено за вработените. Се разбира, одделот за развој ***(безбедносна зона)***[197], е посебен оддел и пристапот во него и излезот од него е определен со одреден многу построг режим. Во развиените и големи корпорации постојат повеќе нивоа на заштита: физичка, техничка и друга. Нивото на физичка заштита најчесто е поврзано со нивото на електронска заштита и безбедносен документ за идентификација, идентификациски отисок, скен на лице или друг вид на видео заштита. Особено е важно да се напомене дека во делот на заштитата од особена важност е елиминирање на можноста од внесување на електронски уреди (медиуми за снимање) во забранетата зона (дефицит на фото, видео и друг вид документирање заради изнесување надвор), но истовремено и забрана за внесување, а особено на изнесување на хартиени и други документи. Многу често, кога се работи за особено осетливи развојни програми и активности, постои зголемување на нивото на безбедност, кое се протега и на личната безбедност на вработените и нивните семејства па тие се преселуваат да живеат во строго контролирани затворени средини (особено во високотехнолошките зони - силиконската долина, развој на нови оружја, технологии, заштитна опрема, атомски и други технологии). Во овој контекст е и развојот на автомобилската индустрија каде што развојот на новите концепти и нивното тестирање се остварува преку нивно камуфлирање, тестови на затворени стази за тестирање на возила, непристапни и сокриени терени за тестирање и потврдување на возните својства на возилото, далеку од јавноста а особено од фоторепортерите.

Фотографија бр. 1 Развојна фотографија од нов модел на Мерцедес-Бенз[198]

[197] 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, предвидено во Закон за класифицирани информации, Службен весник на Република Македонија бр.9/2004, чл.5, т. 14

[198] Преземено од: http://tocka.com.mk/vesti/259606/mercedes-se-podgotvuva-za-lansiranje-na-nov-krosover

Фотографија бр. 2 Развојна фотографија од нов модел на Мерцедес-Бенз[199]

Бидејќи електронската комуникацијска безбедност е особено ризична и многу често мета на напади на заинтересирани поединци и групи, поради што е неопходно да се зголеми нивото на сајбер безбедност во корпорацијата[200] на електронскиот систем на корпорацијата и многу други елементи. Сепак, во сите корпорации во кои има над 50 вработени (во 2013 бројот е намален на над 25 вработени)[201], прво и основно е водење евиденција на вработените при влез и излез од работа и почитување на работното време, ова е основниот и почетен модел на корпоративна безбедност, при што, во кругот на корпорацијата може да влезат само вработените или посетители кои ќе бидат евидентирани и документирано каде се движат (контрола на движењето, комуникацијата).

Позитивни ефекти од корпоративната конспиративност

Особено е важно сите вработени во корпорацијата од највисоката до најниската позиција да го сватат значењето на корпорациската конспиративност, бидејќи од нејзе зависи развоот на корпорацијата и продолжување на работниот однос, редовната исплата на личниот доход и секако добивање одредени бенефиции од остварениот профит. Уште позначајно е сите бработени да ги почувствуваат позитивните придобивки од развојот и на тој начин да се почувствува нивната вклученост во процесот, истовремено на тој начин да бидат мотивирани и самите да придонесат до одредени подобрувања и иновации во процесот.

[199] Преземено од: http://automedia.investor.bg/a/0-nachalo/25404-mercedes-benz-zagatna-za-nov-sporten-model/

[200] Александра Станковска, Сајбер закана за финансискиот сектор, Втора меѓународна научна и стручна конференција, Општествени, економски, правни, безбедносни и социјални детерминанти за развојот на корпоративната безбедност во Република Македонија, регионот и пошироко, Асоцијација за корпоративна безбедност во Република Македонија, со финансиска поддршка на НИКОБ Македонија, Скопје, 2017, стр.45

[201] Закон за изменување и дополнување на законот за работни односи, Службен весник на Република Македонија бр. 25/2013, чл. 21 во кој е изменет претходниот чл.116 став 7.

Негативни ефекти од непримeнувањето на корпоративната конспиративност

Многу позначајни или суштински се негативните ефекти од непримeнувањето на корпоративната конспиративност. Прашањето е зошто? Постојат многу причини кои заради просторните можности во текстот ќе бидат само наброени:

- Овозможување достапност на особено важни информации на лица кои во никој случај не смеат да ги дознаат (индустриска деловна шпионажа)[202];
- Јавно пренесување на доверливи информации од процесот на развој на новите производи и нанесување директни штетни последици на корпорацијата;
- Предизвикување на кривична[203] или прекршочна одговорност а секако и одредена дисциплинска одговорност за вработените кои овозможиле пристап до информации, простории или документи кои претставуваат: деловна, службена, државна или друг вид на класифицирана информација;
- Губење на инвестираните средства за развој на одреден концепт (технологија) кои се пресметуваат во милионски суми;
- Немање можност за вадење на нов производ на пазарот а застарениот веќе не се купува, ова има дирекни негативни финансиски ефекти;
- Рестрикции и неможност за нови инвестиции;
- Рестрикции на вработените, намалување на личните доходи, големи отпуштања од работа и затворање на одредени производствени капацитети;
- Крајно или нужно зло е стечај или комплетно затворање на производствениот процес, корпорацијата и особено тежок период за вработените без средства за лична егзистенција.

Заклучни согледувања

Дали заклучокот е доволен за една вака осетлива тема е прашање кое треба да биде упатено до врвниот менаџмент на секоја сериозна компанија-корпорација. Средствата кои се инвестирани во обуки и развој на целокупниот кадар на полето на безбедноста треба да бидат сватени како средства за развој бидејќи позитивните ефекти кои ќе бидат придобивки од стекнатото знаење и вештини се можност за развој на корпорацијата. Од друга страна континуираниот процес на надградба на полето на безбедноста на и во корпорацијата може да донесе само позитивни придобивки а плодовите од истите треба да ги користат ,,сите вработени" не само сопствениците, управителите и лицата од менаџментот. Клучно и можеби најважно од се е чувството на секој вработен дека лично тој е кариката која преку своето работење и давањето и прифаќањето на добри и новативни предлози и самиот е особено значаен во развојот и напредокот на корпорацијата. Конспиративноста и нејзиното применување и почитување во секој поглед, кога е насочена во развојот на корпорацијата има само позитивни ефекти, и тикму затоа е особено важно менаџментот од време на време за истата да ги потсетува вработените и пред нив

[202] Оливер Бакрески, Драган Триван, Сашо Митевски, Корпорациски безбедносен систем, Комора на Република Македонија за обезбедување на лица и имот, Скопје, 2012, стр. 126

[203] Кривична одговорност според Кривичниот законик, Службен весник на на Република Македонија бр. 37/96 и сите подоцнежни измени и дополнувања

да ги презентира позитивните и секако негативните ефекти од нејзиното непочитување.

Користена литература

1. Александра Станковска, Сајбер закана за финансискиот сектор, Втора меѓународна научна и стручна конференција, Општествени, економски, правни, безбедносни и социјални детерминанти за развојот на корпоративната безбедност во Република Македонија, регионот и пошироко, Асоцијација за корпоративна безбедност во Република Македонија, со финансиска поддршка на НИКОБ Македонија, Скопје, 2017
2. Владо Водинелиќ, Криминалистика-пето измењено и проширено издање, Савремена администрација, Београд, 1984
3. Гоце Џуклески, Вовед во криминалистика, График Мак Принт, Скопје, 2006
4. Гоце Џуклески, Вовед во криминалистика (второ дополнето издание), График Мак Принт, Скопје, 2008
5. Методија Ангелески, Криминалистика (општа криминалистичка теорија), НИО ,,Студентски збор",Скопје, 1993
6. Методија Ангелески, Вовед во криминалистика, Графос, Скопје, 2007
7. Милан Вујаклија, Лексикон страних речи и израза, Просвета Београд, 1980, Београд
8. Обрен Ѓорѓевиќ, Лексикон безбедности, Партизанска књига, Београд, 1986
9. Оливер Бакрески, Драган Триван, Сашо Митевски, Корпорациски безбедносен систем, Комора на Република Македонија за обезбедување на лица и имот, Скопје, 2012
10. Оливер Бакрески, Милан Даничиќ, Желимир Кешетовиќ, Сашо Митевски, Приватна безбедност-теорија и концепт, Комора на Република Македонија за приватно обезбедување, Скопје, 2015
11. Тодор Витларов, Казнено правни аспекти на корпоративната безбедност, Зборник, Втора меѓународна научна и стручна конференција, Општествени, економски, правни, безбедносни и социјални детерминанти за развојот на корпоративната безбедност во Република Македонија, регионот и пошироко, Асоцијација за корпоративна безбедност во Република Македонија, со финансиска поддршка на НИКОБ Македонија, Скопје, 2017
12. Љубо Миќуновиќ, Современ лексикон на странски зборови и изрази, Наша книга, Скопје

Законски и други прописи

1. Закон за класифицирани информации-Консолидиран текст, Службен Весник на Република Македонија, бр.9/2004, 113/07, 145/10, 80/12, 41/14 и 21/18
2. Закон за кривична постапка, Сл. весник на РМ бр.15/1997, 44/2002, 74/2004, 83/2008, 67/2008, како и Одлуки на Уставен суд; Убр.36/38 објавена во Сл. весник на РМ бр.18/99, одлука бр.У. бр. 144/2003 објавена во Сл. весник на РМ бр. 27/2004, одлука У.бр. 34/05 објавена во Сл. весник на РМ бр.75/2006, одлука У. Бр. 63/2008 објавена во Сл. весник на РМ бр. 53/2009.
3. Кривичен законик, неофицијален пречистен текст, Сл. весник на РМ бр. 37/96 и закон за измени и дополнување на Кривичниот законик, Сл. весник на РМ бр. 80/99, 4/02, 43/03, 19/04, 81/05, 60/06, 73/06, 87/07, 7/08, 139/08, 114/09, 51/11, 135/11, 185/11, 42/12, 166/12, 55/13, 82/13, 14/14, 27/14, 28/14, 115/14, 132/14, 160/14, 199/14 и 41/15.
4. Закон за изменување и дополнување на законот за работни односи, Службен весник на Република Македонија бр. 25/2013
5. http://tocka.com.mk/vesti/259606/mercedes-se-podgotvuva-za-lansiranje-na-nov-krosover
6. http://automedia.investor.bg/a/0-nachalo/25404-mercedes-benz-zagatna-za-nov-sporten-model/

М-р Џихан Ахмед
Европски Универзитет Република Македонија
Климент Охридски 68
Македонија, Скопје 1000
тел: +389(0)2 3202098
факс: +389(0)2 3202030
е-маил: cihan.ahmed@eurm.edu.mk

ДИГИТАЛИЗАЦИЈАТА ПРЕДИЗВИК ЗА ТРАНСФОРМАЦИЈАТА НА АДМИНИСТРАЦИЈАТА ВО СОВРЕМЕНИТЕ КОРПОРАЦИИ

Апстракт
Во постапката за дигитализација и градење е-архива е создадена вредност за иднината. Во подготвителната постапката за дигитализација е создаден архивски план на скенирање и план на употребна вредност на документарен материјал во кој сите документи се атрибутизирани, класифицирани и лесни за пребарување и употреба. Во современите компании администрацијата има професионални сервери опремени со УПС системи за непречено напојување на истите со електрична енергија 24/7, антивирусни програмски решенија во вид на апликативен софтвер опериран од страна на информатички администратори на мрежата кои можат да бидат и надворешни правни лица кои на компаниите им ја пружаат оваа услуга. Поради тоа компаниите вработуваат соодветни стручно оспособени лица за извршувањето на оваа работа кои водат грижа за неможност од пристап до архивираните документи од страна на неовластени лица, било да станува збор за лица вработени во компанијата или пак за надворешни лица, т.н. хакери кои прават напори за влегување во електронските информациони системи на компанијата преку глобалните светски мрежи, т.е. интернетот.

Клучни зборови: *дигитализација, администрација, архиви, скенирање, постапки, интернет*

MSc. Cihan Ahmed
European University Republic of Macedonia
Kliment Ohridski 68
Macedonia, Skopje
Tel: +389(0)2 3202098
fax: +389(0)2 3202030
e-mail: cihan.ahmed@eurm.edu.mk

DIGITALIZATION CHALLENGE FOR TRANSFORMATION OF ADMINISTRATION IN CONTEMPORARY CORPORATIONS

Abstract
The digitalization and building of an e-archive has created value for the future. In the preparatory procedure for digitization, an archive scanning plan and a plan for the use of documentary material were created in which all documents are attributed, classified and easy to search and use. In modern companies, the administration

has professional servers equipped with UPS systems or known as Uninterruptible Power Supply uninterrupted power supply 24/7, antivirus software solutions in the form of application software operated by IT administrators on the network, which can be also external legal entities that their companies provide this service. As a result, companies employ suitable professionals for the performance of this job, which takes care of the inability of access to archived documents by unauthorized persons, whether it's about employees in the company or for external persons, the so-called. hackers who make efforts to enter the company's electronic information systems through global global networks, i.e. the Internet.

Keywords: *digitalization, administration, archives, scanning, procedures, internet*

Вовед

Секојдневното работење на една компанија продуцира големо количество на хартија. Традиционалната архива стана гломазна, тешка за одржување и го отежнува пребарувањето на потребниот документ. Согласно законските прописи и нормативи секој документ во компанијата треба да се складира, чува и архивира во претходно дефиниран временски период. Се поголемото користење на системи за дигитализација на хартиените материјали и документи како и измените во законските прописи наметнаа потреба од користење на електронски деловодник и електронско архивирање.

Дигитализацијата, односно преносот на конвенционалниот архивски и документарен материјал во неконвенционален архивски и документарен материјал е начин да ја зголемите вредноста, ефикасноста, безбедноста и трајноста на вашите документите. Конечен производ на нашата услуга е документ во електронска форма (PDF, PDF/A,JPG, TIFF) кој авторизираните лица од вашата компанија можат непрекинато да го користат преку нашата услуга Е-Архива или да го добијат на посебен медиум (оптичко-магнетен медиум (цврст диск), компакт диск (CD), DVD, Flash меморија).

Во зависност од нивната функционална важност и нивниот формат, услугата на дигитализација преку процесите на скенирање и индексирање може да ги конвертира вашите документи во формат со врвна употребна вредност кој е едноставен за преглед, пренос и манипулација. Во Инбох може да се дигитализираат сите документи независно од нивниот тип, од видот и форматот на хартијата (A0-A8), како и конверзија на микрофилм во дигитална копија.

За нас безбедноста на податоците е вредност со која не правиме компромис. Во рамките на услугата дигитализација на деловна документација ние ја гарантираме безбедноста на сите податоци кои се дигитализираат согласно регулативата од Законот за заштита на лични податоци. При процесот на дигитализација се опфатени бројни безбедносни и контролни механизми за заштита на информацискатa вредност на документот, како и неговиот физички интегритет.

Процесот за дигитализација и градење Е-Архива

Во процесот за дигитализација и градење Е-Архива, создаваме вредност за иднината. Во подготвителната постапка за дигитализација се креира соодветен план за скенирање и индексирање. Планот опфаќа класификација

на документите по функционални типови и одредување на параметри за индексирање во согласност со вашето работење, чија цел е брзо и лесно пребарување на истите.

- Дигитализација на документација во простории на клиентот

Проектната дигитализација која претставува скенирање и обработка на документација од одреден временски период, одреден сектор или одредена функционална важност, може да биде извршена и во ваши простории.

Имателите на приватен архивски и документарен материјал се должни да водат основна или сопствена евиденција за архивскиот и документарниот материјал, да донесат план на архивски знаци со листа на архивски и документарен материјал, да вршат тековно одбирање на архивскиот од документарниот материјал и да го чуваат трајно архивскиот материјал согласно овој закон.

Конвенционален архивски и документарен материјал е оној материјал кој е запишан на хартија и за кое читање не е потребен специјален уред. Дигитализација претставува пренесување на архивскиот материјал од физички и аналогни облици во електронски облик. Неконвенцијален архивски и документарен материјал е оној материјал кој е запишан на посебен медиум (микрофилм, оптичко-магнетен медиум (цврст диск), компакт диск (CD), DVD, Flash меморија или холографски диск). За читање на содржината на овој материјал се потребни посебни уреди. Во неконвенцијален материјал спаѓаат: електронски документи креирани со помош на компјутери и други електронски уреди во дигитален облик; податоци евидентирани во бази на податоци врз основа на кои преку нивна обработка се креираат конвенцијални документи и дигитални слики добиени со некоја постапка на дигитализација на конвенцијалните документи

ПРОСТОР, ОПРЕМА и УСЛОВИ за чување и заштита на архивски и документарен материјал

Податоците евидентирани во дигитални бази на податоци и дигиталните слики на документи добиени со дигитализација на конвенцијални документи, се чуваат на начин кој ги обезбедува од неовластен пристап, бришење, менување или губење на податоците, во согласност со закон и други прописи за управување и заштита на информациските системи (правење на бекап копии секојдневно на компакт диск, DVD, магнетна трака, мобилен цврст диск или на сервер од некој провајдер кој дава услуги за чување на база на податоци во согласност со законските прописи).

Основна евиденција за сите примени и сопствени документи/записи е деловодникот или друга посебно пропишана книга за евиденција. Пописот на документи/записи служи за заведување на документи/записи од ист вид што се примаат или создаваат во поголем број, а по кои се води иста постапка[204] (на пример: потврди, уверенија, фактури, решенија за годишен одмор и други). Пописот на документи/записи е составен дел на деловодникот.

3. ИНТЕРНА ДОСТАВНА КНИГА – СЕ ПОПОЛНУВА СО ЕДЕН КЛИК
4. КНИГА ЗА ПОШТА – СЕ ПОПОЛНУВА СО ЕДЕН КЛИК

[204] Džorž Soros „O globalizaciji“, Samizdat B92, Beograd, 2003

5. КНИГА ЗА МЕСТО – СЕ ПОПОЛНУВА СО ЕДЕН КЛИК

Архивски сеф

Архивски сеф е физички простор од цврста градба за чување на конвенционален и неконвенционален архивски и документарен материјал кој:
- има статика на конструкцијата на објекот/депото од 9+ според европската сеизмичка скала;
- има двојно контролиран пристап (физички и електронски);
- има алармен систем за откривање и дојава на неовластен пристап;
- обезбедува огноотпорност од најмалку 60 минути спрема внатрешно и 180 минути спрема надворешно опкружување;
- има систем за рано откривање, дојава и гаснење на пожар според сертифициран противпожарен елаборат;
- обезбедува константна и контролирана температура од 16 до 20 целзиусови степени;
- обезбедува константна и контролирана релативна влажност од 30% до 50% и
- обезбедува антистатичка заштита.

Серверска соба

Серверска соба е физички простор од цврста градба за чување на неконвенционален (електронски) архивски и документарен материјал, кој:
- е со контролиран пристап со физичка и електронска брава;
- обезбедува огноотпорност на надворешна средина од најмалку 60 минути;
- има алармен систем за откривање и дојава на неовластен пристап;
- има алармен систем за рано откривање и дојава на пожар;
- има соодветен систем за гаснење на пожар;
- обезбедува константни и регулирани микроклиматски услови со температура од 16 до 20 целзиусови степени и влажност од 35% до 50% и
- поседува соодветна антистатичка заштита.

Серверската соба не се организира заедно или во склоп на документарната соба или архивата на имателот. Простор, опрема и услови за чување и заштита на архивски и документарен материјал Чувањето на архивскиот и документарниот материјал, во зависност од обемот и обликот (конвенционален или неконвенционален) се врши во соодветен простор, и тоа во:
а) документарен ормар;
б) документарна соба (писарница);
в) архива;
г) архивски сеф ...

Документарен ормар е означен монтажен физички простор за чување на архивски и документарен материјал кој овозможува контролиран пристап до материјалот преку физичка или електронска брава. Документарниот ормар се поставува во просторија која има инсталиран систем за откривање на пожар и сигнален уред за алармирање или дојава (електронски сигнал) на пожар.

Документарниот ормар во неговата најниска точка е подигнат од основниот под на просторијата во која се наоѓа на висина од најмалку 10 см. Документарна соба е простор од цврста градба до 50 м2, за чување на конвенционален архивски и документарен материјал, која овозможува заштита од неовластен пристап или злоупотреба, преку контролиран пристап со физичка или електронска брава.[205]

Документарна соба

Документарната соба треба да:
- обезбедува огноотпорност кон внатрешен и надворешен простор од најмалку 60 минути;
- има инсталиран систем за рано откривање и алармирање на пожар и
- поседува соодветен уред за противпожарна заштита.

Во документарната соба не се чуваат електрични апарати под напон, хемиски и биолошки материјали кои можат да доведат до трајно оштетување или уништување на архивскиот и документарниот материјал.
Архивата е физички простор за чување на конвенционален архивски и документарен материјал кој:
- има простор за чување на материјалот над 50 м2;
- има физички или електронски контролиран пристап;
- има алармен систем за откривање, сигнализација и дојава на неовластен пристап;
- обезбедува огноотпорност од најмалку 60 минути на надворешно влијание;
- има контролирана внатрешна електрична инсталација;
- има систем на рано откривање, сигнализација и дојава на пожар;
- има противпожарна заштита и
- има хигиенско-технички услови.

Архивата е простор што е исклучиво наменет за чување и заштита на архивски и документарен материјал и не се користи за чување на други материјали.[206]

Клучни фактори за реализација на е-архивата во администрацијата во современите корпорации

Важно е да се потенцира дека новата стратегија може да биде целосно и успешно имплементирана само доколку се обезбедат четири клучни предуслови за нејзина имплементација - обезбедување на релевантни податоци, добра организација, координација и финансиска одржливост. Овој заклучок произлегува од искуствата и научените лекции во спроведувањето на претходната стратегија. Имено, обезбедувањето на точни и релевантни податоци за областите кои ќе бидат предмет на реформата, правилното лоцирање на институциите кои ќе бидат надлежни за спроведување на поодделни делови од истата, нивната соодветна организација, капацитетите и

[205] AA Berle and GC Means The Modern Corporation and Private Property (2nd edn Harcourt, Brace and World, New York 1967- (https://www.repository.law.indiana.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=5120&context=ilj)
[206] Collier Paul, Dollar David „Globalization, Growth and Poverty: Building an Inclusive World Economy“, Oxford University Press and World Bank, 2002

демонстрираното лидерство од страна на раководните лица на овие институции, добрата координација и прецизните механизми за следење на реализацијата на активностите, како и прецизната проценка на трошоците за нејзина имплементација но и прецизно дефинираните извори на средства за таквите активности, се "conditio sine qua non" во однос на успешна имплементација.

Како клучни предуслови кои задолжително мора да бидат исполнети за да се обезбеди реализација на стратешките определби и кои долгорочно треба да обезбедат унапредување и трансформација на администрацијата во сервис на граѓаните се следните:

- Посветеност, што подразбира обезбедување на разбирање и поддршка пред се од највисоките раководни структури, но и од вработените;
- Регулатива, која опфаќа постоење на соодветни регулативи, усогласеност на постојни закони, донесување на стандарди, стратегии, политики и други документи;
- Имплементација, што подразбира континуирана примена на регулативата и ставањето на проектите во функција, и организациски дизајн на силни институции одговорни за сервисна ориентираност и координирано управување;
- Дигитализација, која се однесува на знаења за актуелни теми, соодветни капацитети, модерни ИТ решенија и друго.

Како предуслов за ова е дигитализацијата и прочистувањето на сите јавни регистри од чии податоци директно зависи квалитетот на услугите; и

- Вклученост, која подразбира вклученост на граѓанскиот сектор, бизнис секторот, стручната и научната јавност и други засегнати страни.

Недостатоците и ризиците на процесот на децентрализацијата се однесуваат пред се на:

1. Недоволната екипираност и обученост на општинската администрација за превземање на трансвериранитe надлежности на делот на локалната власт,
2. Проблеми во управувањето како недостаток на соодветна координација на нискиот квалитет на справување со новата ситоација на трансферирана локална власт,
3. Непостоење на стратегија за финансиската децентрализација на локалната самоуправа,
4. Зголемување на ингеренциите на локално ниво без извршена финансиска децентрализација и сигурно буџетирање на општините и др.[207]

Заклучок

Администрација ќе претставува вистински и целосен сервис на потребите на граѓаните, нивен партнер и основен двигател на општествениот развој и напредок. Ќе се овозможи трансформација на свеста кај службениците, преку нивно континуирано обучување и правилно оценување на нивната работа со прифаќање на современите европски трендови и најдобрите практики на добро владеење. Ќе има целосна отчетност, транспарентност и одговорност на сите носители на јавни овластувања, кои ќе бидат под непосредна и

[207] Collier Paul, Dollar David „Globalization, Growth and Poverty: Building an Inclusive World Economy", Oxford University Press and World Bank, 2002

континуирана контрола на граѓаните. Техничко-технолошкиот развој и развојот на информатичката технологија ќе бидат препознаени и максимално искористени во процесот на дигитална трансформација на администрацијата. Современите електронски алатки ќе бидат од суштинско значење за поголема ефикасност и економичност на јавната администрација. Ќе се зголеми довербата на граѓаните, на компаниите и на сите останати општествени чинители кон администрацијата, доверба која ќе произлезе од зголемената одговорност, професионалниот однос и сервисната ориентација на службениците.

Користена литература

- AA Berle and GC Means The Modern Corporation and Private Property (2nd edn Harcourt, Brace and World, New York 1967 (https://www.repository.law.indiana.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=5120&context=ilj)
- Collier Paul, Dollar David „Globalization, Growth and Poverty: Building an Inclusive World Economy“, Oxford University Press and World Bank, 2002
- Džorž Soros „O globalizaciji“, Samizdat B92, Beograd, 2003

М-р Марија Цизалоска
Факултет за Економски науки
Европски Универзитет – Република Македонија, Скопје
mcizaloska@yahoo.com

BLOCKCHAIN ТЕХНОЛОГИЈА

АПСТРАКТ
Bitcoin, дефинитивно е термин кој ја одбележа 2017 година. Неверојатниот раст на вредноста, како и на неговата популарност го доведе во центарот на вниманието на финансиските аналитичари и ги редефинираше законите на пазарно однесување. И после години означување на криптовалутите како експеримент, балон и шпекулација, пазарот постои, но останува прилично волатилен и неизвесен.
Но она што во последно време го привлекува вниманието на инвеститорите е концептот на дигиталната валута, односно технологијата која стои позади него и чија цел е да овозможи брзи, ефикасни и сигурни трансакции, без присуство на посредници, а тоа е – Blockchain. Ако Bitcoin беше само увертира, Blockchain е револуционерна технологија во IT секторот, подготвена да го промени светот.
Прашањето е што е Blockchain, на кој принцип работи и какви промени може да предизвика во индустријата?

Клучни зборови: Bitcoin, blockchain, технологија, финансиска индустрија, дигитална револуција

BLOCKCHAIN TECHNOLOGY

ABSTRACT
Bitcoin was definitely the buzzword of 2017. Its incredible rise in value as well as popularity made it the focus of attention of financial analysts and redefined the laws of the market. After years of being viewed as experiment, instruments of speculation, bubble, now there is a market for cryptocurrencies, however it is very volatile and uncertain.
But what has been capturing the attention of investors lately is the concept of a digital currency, or rather the technology behind it aimed at ensuring fast, efficient and safe transactions without mediators and that is Blockchain. If Bitcoin was the opening act, Blockchain is the revolutionary technology in the IT sector ready to change the world.
The question is what is Blockchain, how does it work and what are the changes it can make in the industry?

Keywords: Bitcoin, Blockchain, technology, financial industry, digital revolution

Што е Blockchain технологија?

Blockchain прв пат се појави 2009 година како технологија која го овозможи креирањето на Bitcoin-от, првата глобална, дигитална валута. Основните концепти се развиени во оригиналниот документ на Satoshi Nakamoto од 2008 година, со наслов: Bitcoin: A peer-to-peer Electronic Cash System[208]. Започна со Bitcoin, се прошири и на другите дигитални валути, а сега оваа технологија бара примена и во други сегменти од животот. Идејата на Bitcoin- от беше децентрализирана, анонимна и целосна слобода на пазарот – во што и успеа.
Blockchain технологијата е комбинација од докажани технологии применети на нов начин. Комбинацијата на peer-to-peer (P2P) мрежата и дистрибуираниот сервер кој ја забележува секоја трансакција со временски печат, создаде база на податоци која е автономна и дистрибуирана помеѓу сите учесници во мрежата. Резултатот е систем за дигитална интеракција за која не е потребна трета страна.
Во суштина, Blockchain (ланец на блокови) содржи мрежа на шифрирани блокови на податоци. Blockchain е база на податоци која ја чинат повеќе блокови, меѓусебно дигитално поврзани, а кои содржат податоци за дигитални информации од било кој вид. Овие податоци не може да бидат изменети или хакирани, бидејќи секој блок на податоци во ланецот е поврзан со претходниот и заштитен со криптографски клуч, наречен Hash. Во одредена смисла, blockchain е отворена, дигитална книга (слично како и главната книга во сметководството) која содржи информации за сите финансиски трансакции во мрежата. Во секој блок на податоци може да се запише одреден број на податоци или трансакции. Кога блокот ќе се пополни, се креира нов блок и така натаму. На овој начин се формира непрекинат блок на информации, кои се меѓусебно поврзани и невозможно е истите да бидат прекинати. Тие се конзистентни. Како што книгата оди страница по страница, така blockchain има датотека по датотека кои се поврзани.
Со тоа што податоците се хаширани, истите неможат ретроактивно да бидат променети. Затоа оваа технологија е толку добра – еднаш запишан податок, не може повеќе да се измени. Значи нема криење на податоци, менување на истите или бришење. Се останува запишано во еден од блоковите на податоци кои го чинат blockchain.

Што е неговата иновативност?

Колку пати до сега сте се пожалиле на високата провизија во банките и на чекањето во редови? Кога и да сакаме да испратиме писмо, пари, пакет, e-mail, sms… мораме да користиме посредници. Посредниците обично ги зголемуваат трошоците на пренос, доцнат и претставуваат ризик. Тие чуваат голема количина наши податоци кои подоцна можат да бидат злоупотребени од страна на хакери. Посредниците можат да ни ја блокираат сметката, да ни ги замрзнат средставата или воведат ограничувања. Сега, по прв пат, повеќе

[208] https://bitcoin.org/bitcoin.pdf

не мора да ги користиме. Тоа е она што blockchain технологијата ни го овозможува.
Банкарските сметки, државните тајни информации и други централизирани податоци лесно можат да бидат хакирани. Меѓутоа, доколку сакате истото да го направите со Blockchain, мора да хакирате ланец на блокови, што е фактички невозможно. Оттука, доколку овој начин на собирање податоци во иднина најде широка примена, функционирањето на системот нема да се заснова на довербата во некорумпираните административни и банкарски службеници т.е нема да зависи од човечки фактор – туку ќе зависи од Blockchain ланецот. А Blockchain никогаш не греши. Токму и непоткупливоста на системот кој се базира на непроменливост на информациите, е она што го прави Blockchain погоден за употреба и во многу други сфери, освен финансиите, како и во економијата, администрацијата, здравството, гласањето преку интернет и слично. Едноставно кажано – Blockchain технологијата овозможува брз, ефтин и сигурен пренос на вредни пратки, без посредници и без хакирање.

Може ли Blockchain да направи револуција во светската економија?

Blockchain технологијата нуди нови алатки за автентикација и овластување во дигиталниот свет и создавање на нови дигитални односи. Многу компании и невладини организации настојуваат на примена на Blockchain во своето работење. Од Тоуота сметаат дека оваа технологија може да постигне големи резултати ако се примени на автоматизација на возилата и во полето на осигурување. Имено, сензорите во автомобилите, собраните податоци во текот на возењето, би ги чувале во Blockchain ланецот, за подоцна истите да бидат испратени на осигурителните друштва, кои на тој начин многу подобро ќе можат да направат проценка на штета.
Интернетот денес стана премногу централизиран и контролиран од страна на влади и неколку големи играчи. Не е ни чудно што и самиот креатор на интернетот, Tim Berners-Lee, во март 2017, кажа: „ Изгубивме контрола врз нашите лични податоци“. Обично на продавачите на интернет, потребно им е наше корисничко име, лозинка, детали на плаќањето и други лични податоци за да ја добиеме нивната услуга. Тоа е проблемот на поголемиот, ако не и на сите услуги поврзани со интернет – нашите информации и трансакции се чуваат на сервери, кои можат да ги инфилтрираат хакери кои се во потрага по лични податоци. Во таа смисла blockchain е неопходен и одличен за заштита и чување на нашите лични податоци. Според Microsoft, blockchain ќе ја елиминира потребата да се обезбеди „ широка согласност“ за безброј апликации и услуги (оваа ситуација ви е позната кога инсталирате некоја апликација на мобилните телефони). Вашиот идентитет не би бил дуплиран и проширен на повеќе провајдери како што се Twittwr, Facebook, Instagram, Google play, Amazon и други.
Aleks Simons, директор на програмскиот менаџмент на компанијата Microsoft Identiti Division, вели дека компанијата планира да креира платформа заснована на blockchain технологија за креирање на децентрализиран идентитет на лични податоци (DID). Тоа значи дека личните податоци нема да

бидат зачувани на сервери како што беше до сега, туку ќе бидат сместени во сигурна мрежа.
И Mark Zuckerberg, основачот на Facebook, внимателно ќе ги проучи сите можности кои ги дава Blockchain технологијата, за да може да го врати Facebook на оригиналната идеја за децентрализирана и независна социјална мрежа.

Заклучок

Несомнено е дека Blockchain технологијата е револуционерна технологија, која ќе редефинира разни аспекти на организациите. Не е ни чудно тогаш, зошто нејзината примена е предмет на истражување не само од страна на банките и технолошките компнаии, туку и на цели влади и индустрии од различни земји.
Целосна имплементација на Blockchain системот, може да се нарече еден вид апокалипса, а не револуција. Доколку неговиот полн потенцијал се реализира во финансиската сфера - банките, акционерските друштва и слични институции не би имале повеќе смисла за постоење, а иста судбина ќе имаат и нивните вработени. Целосната државна администрација ќе биде заменета со ултрапродуктивен и бескомпромисен систем ширум светот. Машините ќе бидат тие што ќе внесуваат, анализираат и ревизираат податоци во рок од неколку минути. Прашање е, што ќе се случи со индустријата, кога сите финансиски и економски информации ќе бидат автоматски достапни и навремени? Што ќе се случи со луѓето што ќе останат без работа? Само во Америка има 1,3 милиони вработени во сметководството. Технологијата во моментов им се заканува на сите, бидејќи нејзиниот напредок ги остава луѓето без работа.
Се предвидува дека и Blockchain, исто како и интернетот ќе го промени нашиот живот, ќе промени многу индустрии, пред се банкарството и осигурувањето. Она што беше интернетот во 90-тите, во наредните пет до десет години се предвидува да биде Blockchain технологијата.

Користена литература:

- www.blockgeeks.com
- www.coindesk.com
- www.wikipwdia.org
- www.startit.rs
- www.netokracija.rs
- www.bankar.me

Александар Рунески
Факултет за детективи и криминалистика при ЕУРМ
runeski21@gmail.com

МАЛОЛЕТНИЧКА ДЕЛИКВЕНЦИЈА

Апстракт
Целта на истражувањето во областа на малолетничка деликвенција е разграничување на малолетното лице како сторител на кривично дело од возрасните лица. При определување на поимот малолетник постојат некои општи сфаќања и претпоставки кои самите по себе не се доволно прецизни што доведува до нивно различно толкување.
Во трудот се поставени насоки за поделба на сторителите на кривични дела, како и дефициниja за тоа што претставува малолетник, што содржи неговата структура на личноста, каков е неговиот темперамент и кои се неговите карактеристики и состојби, односно неговата целокупна биофизичка и психофизичка состојба која понатаму би помогнала при одлуката за казнување.
Трудот е реализиран преку темелни истражувања и се заснова врз факти и податоци во однос на организацијата и составот на судовите за малолетници, како и нивното место и улога во кривично-правниот систем на РМ, надлежноста, кривичната постапка кон малолетници, малолетничката правда и целта на казнената постапка. Од тука произлегува и неговото значење.
Клучни зборови: малолетник, малолетничка деликвенција, кривично дело, пресуда, казнено-поправен дом.

JUVENILE DELINQUENCY

Abstract
The purpose of the research in the area of juvenile delinquency is to distinguish the juvenile person as a perpetrator of a crime from adults. In determining the notion of a juvenile there are some general assumptions which are not precise enough which leads to their different interpretation.
The research provides guidelines for the division of perpetrators of crimes, as well as deficiencies in what constitutes a juvenile and what contains its structure of personality, what is its temperament and what are the characteristics and conditions, that is, the overall biophysical and psycho-physical state that further would help with the decision for punishment.
The work is carried out through thorough research and is based on facts and data regarding the organization and composition of courts for juveniles, as well as their place and role in the criminal justice system of the Republic of Macedonia, jurisdiction, criminal procedure against minors, juvenile justice and the purpose of the criminal procedure. From there comes its meaning.

Keywords: juvenile, juvenile delinquency, criminal act, verdict, penitentiary house.

Граници на кривично – правната малолетност

Издвојувањето на малолетниците извршители на кривични дела од останатите старосни категории деликвенти и создавањето на посебни законски категории на малолетниците претставува одредување на старосни граници со помош на која можеме да го отфатиме оној дел од населението кој го нарекуваме малолетни деликвенти. Историскиот приказ за уважување на студијата за развојот на малолетниците во кривичното право ни покажува дека уште во стариот век поедини права (старото кинеско право, римското право) ги определувале старосните граници на малолетството поради посебното кривично-правно третирање на малолетниците. Некои европски права од средниот век го превземале римското право, се јавуваат и неодредени, еластични граници кои се поврзани со одреден достигнат развој на малолетниците .[209]

Во поново време преовладува тежнеењето прецизно да се одреди границата на малолетството, со што се одбегнува арбитребност и јасно одвојување на категоријата на малолетниците од останатите старосни категории. Можни се два начини за одредување на старосната граница на малолетството . Во некои земји се одредува само горната граница, т.е воздраст кога почнува кривично-правното полнолетство, така што во начелото секој малолетник (па и дете на пр. од седум години) мора да биде кривично одговорно за стореното дело. Во модерните законодавства преовладува друг начин по кој освен горната граница се одредува и долната старосна граница т.е периодот кога почнува одговорноста на малолетникот во кривичното право. Малолетниците под со закон определена долна граница на малолетство немаат потребна возраст за кривична одговорност и остануваат надвор од доменот на казненото право. На тој начин одредувањето на долната граница на малолетството се врши со разграничување помеѓу деца и категории на малолетници, а со одредувањето на горната граница се одвојува категоријата на малолетници од категоријата на возрасни, полнолетни сторители на кривично дело.

Структура на личноста

Особини на личноста се особини кои ја сочинуваат структуралната основа на една личност. Со ова прашање се занимавале научните работници на полето на медицината, психологијата и другите научници дисциплини од најраното доба на постанок на овие науки , односно од Хипократ – таткото на медицината па до современите теоретки и емпириски потфати на познати психолози како што се Олпорт(G.Alport) и Одберт (H.Odbert), Гилфорд(J.P.Guilforrd), Кател и др.[210] G. Alport и H.Odbert издвоиле околу 300 придавки кои означуваат релативно трајни универзални особини кои можат да се сретнат кај сите луѓе. Тие особини може да се поделат во повеќе категории:

- Особини со кое се означуваат особеностите на темпераментот

[209] Во некои стари варварски права на раниот среден век воздрасната граница помеѓу малолетството и полнолетството се одредувала со физичката способност за носење на оружје , а во исламското право според Коранот се усвојува граница во зависност од вистинското (биолошкиот) развој на поединецот . Види Б.Златарић , о .с.р 107

[210] Пошироко за тоа B.G Alport спом. Дело глава 2 и 3 стр 36 и 54 и H.Рот спом . дело стр 41- 46

- Особини со кои се означуваат особини на карактерот
- Особини со кои се означуваат способностити , и
- Особености на физичката конструкцијата [211]

Темпрерамент и негови карактеристики

Во психолошката наука денес главно преовладува мислењето дека темпераментот и неговите особености не се однесуваат само на емоционалните реакции, туку се изразуваат и на целокупната активност на човекот, во сите видови на психолошко реагирање како и во сите движења кои човекот ги извршува, односно тој покажува и брзина, сила и траење на реакциите на поединецот воопшто[212]. Темпераментот се однесува на карактеристични појави од емоционална природа на една индивидуа вклучувајќи ја и неговата осетливост на емоционалното поттикнување, нејзините вообичаени сили и брзина на реагирање, расположението кое преовладува и сите особини на расположението, воглавно се наследни по потекло.[213] Темпераментот не останува непроменет од раѓањето до смртта, туку и тој како телесната граѓа и интелигенцијата може да се менува со медицински и хирушки влијанија како и во текот на учењето и стекнувањето на животни искуства .

Судови
Историски развој на малолетничките судови

Во науката на кривичното право (материјално и процесно) нема сомневања во фактот дека идеите и настојувањата за обезбедување на посебен статус на малолетните сторители на казнени дела почнува да се остварува во воведувањето посебни судови или судски совети за малолетниците познати како специјализирани судови. Овај институт може успешно да ги следи промените и состојбите во однос на положбата на малолетникот во кривичното право.

Организација и состав на судовите за малолетници

Судовите за малолетници како специјализирани органи за третирање на малолетните сторители на кривичните дела се развиле од редовно кривично правосудство и за релативно кратко време на своето постоење морале да пронајдат свое место во судската организација на поедини земји. Тие тоа место го завземале постепено со специјализација на службената процедурата и проширување на надлежноста што овозможило да се организираат посебни судски единици кои се повеќе и повеќе се дистанцирале од редовните судови.[214]

---

[211] N.Rot spom delo str 41
[212] Ibid . стр 5
[213] B.G Alport спом дело 50-52
[214] F.Lox ,Fondaments , Limites et Formes de l`Intervention Judiciciaire des Magistrats de la Jeunesse ,VII-e Congres l`association international des magisteres de la jeuness , Paris ,1966 p.35

Место и улога на судовите за малолетниците во кривично- правниот систем на РМ

Согласно Законот за судови [215] во Република Македонија судската власт ја вршат Врховниот суд на Република Македонија, апелационите судови и основни-те судови основани со законот. Судовите се субјекти кои вршат една од основните функции во кривичната постапка и тоа функцијата на пресудување. Судската функција се состои во одлучувањето т.е. во примената на правните норми на фактичката положба на конкретни случаи во животот, утврдена во поспаката одредена со законот. Според тоа, пресудувањето е донесување на одлука за тоа која од двете страни меѓу кои се води спорот е во право.[216] Во вршењето на судската функција судот никогаш не може да одбие да донесе одлука по еден кривичен спор. Според ЗКП, во судовите постојат совети за малолетници. Првостепените судови се состојат од еден или повеќе судии за малолетници. Советот за малолетници во првостепениот суд е составен судија за малолетници и двајца судии поротници. Судијата за малолетници е претседател на Советот. Судиите поротници се избираат од редовите на професори, лекари, воспитувачи и други лица кои имаат искуство во воспитувањето на малолетници. Така, според понудените решенија во МКЗ[217] се предлага во основните судови, во апелационите судови и во Врховниот суд на Македонија да се формираат оддели за малолетници, што се состојат од совет за малолетници, судии за малолетници и стручна соработка од одредени профили кои работат со малолетници. Во Врховниот суд се формира совет за малолетници. Судиите за малолетниците во основните и апелационите судови и обвинителите за малолетници во основните и вишите јавни обвинителства се одредуваат со распоред за работата и постапувањер во предметите со малолетници. Судиите, јавните обвинители и полициските органи што постапуваат спрема малолетните лица поради стореното казнено дело, треба да имаат поседни стручни познавања од областа на детската психологија, криминологијата, социјалната патологија, педагогијата и социјалната заштита, како и смислата за постпапување со малолетници и разбирање за нивниот развој и потреби.

Надлежност на судот за малолетници

Кога станува збор за месната надлежност во постапката спрема малолетниците по правило се определува според местото на живеење (forum domicile), а ако нема живеалиште или тоа е непознато, надлежен е судот на престојувалиштето за тоа, а не се одредува според местото на извршување на кривичното дело (gorum delicti comissi) како што се одредува тоа во редовната постапка .

---

[215] Сл .весник на РМ 36/95

[216] Д-р Панта Марина ,Кривична постапка на СФРЈ , Култура , 1979 год.

[217] Проф .Д-р Љупчо Арнаудовски, Лазар Нанев , предолг нацрт текст , Малолетнички Казнен Законик , Совет за кревентивна Малолетничка деликвенција ,Охрид ,2001 година

Кривична постапка спрема малолетник

Во казненото постапување воопшто, а посебно кога е во прашање малолетен сторител на казнено дело од самиот момент на сторувањето на казненото дело, преку откривањето на сторителот, пред кривичната и подготвителната постапка, пресудувањето и извршувањето на санкцијата процесните дејствија претставуваат комплекс на активности што се насочени кон социјализацијата и ресоцијализацијата на малолетниот сторител на казненото дело. Нивниот успех е детерминиран од континуитетот на постапувањето на органите бидејќи тие се надоврзуваат едни на други. Од суштинско значење се постапувањата во предкривичната постапка бидејќи тие го одредуваат понатамошниот тек на целата постапка.

Положба на малолетникот во системот на малолетничката правда

Еден од најважните принципи во казненото право за малолетници кој треба да доминира над другите е следниов: казненото постапување не е во функција на тежината на делото или деликтот туку пред се е во функцијата на личноста и на потребите на детето или адолесцентот, освен ако ситуацијата не упатува на некоја примена на казна лишување од слобода. Овај принцип претставува основа за целата постапка и така треба да се гледа целата положба на малолетникот во кривичната постапка.

Така е во член 40[218]. За таа цел, државите потписнички на овие документи посебно гарантираат:

1. Ниту за едно дете неосновано да не се обвинува или да не се утврдува дека го прекршило кривичниот закон поради дело или пропуст што не биле забранети со националните или меѓународните закони во времето кога се сторени;
2. На секое дете за кое се тврди или кое е обвинувано за кршење на кривичниот закон да му се дадат барем следниве гаранции: да се смета за невино додека не се докаже според закон, да биде веднаш и директно известено за обвинението против него, постапката да се води брзо и ефикасно, без одлагања од страна на надлежен и непристрасен орган или судско тело, детето да не биде присилено да сведочи или да признава вина, а да се испитуваат сведоци од страната што обвинува, ако се смета дека детето го прекршило кривичниот закон, оваа одлука и секоја досудена мерка која од тоа произлегува повторно да се разгледува од повисок, надлежен орган, детето да има бесплатна помош од преведувач ако тоа не може да разбере или не го зборува јазикот на кој официјално се води постапката, да се почитува приватноста на детето на сите нивоа од постпаката.

За да се обезбеди постапување со децата на начин кој е во нивен интерес и кој е соодветен и на околностите и на стореното дело ќе бидат на располагање разновидните можности како што се грижата, советувањето, надзорот, правното застапување, условното казнување, прифаќањето образованието и

[218] Конвенција за правата на детето ,1989 година

програмите за стручно насочување и други можности на иституционата грижа според член 37[219].

Цели на казнената постапка

Казнената постапка е оној дел од казнениот систем преку кој треба да се оствари поставениот концепт за положбата на малолетникот во казненото право. Сепак казнената постапка треба да обезбеди остварување на овие цели :

1. Казнена постапка спрема малолетните сторители на казнени дела и децата малолетниците воопшто има за цел во согласност со уставот и казненото законодавство на државата и меѓународните документи со кои се гарантираат правата на дете и млад човек треба да обезбеди доследна примена на овие одредби во меѓународните документи со вградување во домашното право. На тој начин треба да се обезбеди остварување на загарантираните права и слободи и заштита од секаков вид повреда и ограничување и од злоупотреба.
2. Казнената постапка треба да обезбеди и гарантира постапување со децата и малолетните лица кога се јавуваат како сторители на казнени дела, постапувањето на сите учесници во постапката да виде во согласност со начелата на законитост и легитимитет. Законитото постапување треба да обезбеди 'владеење на правото' во сите односи вклучително и тогаш кога се води казнената постапка. Начелото на легитимитет треба да значи дека секоја постапка на органите на прогон на усесниците во казнената постепка е легитимна особено тогаш кога таа со себе носи присила, репресивност.
3. Казнената постапка нема за цел за сторителот на казненото дело да му се врати со зло примената на санкција. Казнената постапка има за цел да се остварува како: грижа на општеството за малолетникот чие поведени отстапува од општо прифатените општествени вредности и норми. Со казнено дело тоа малолетно лице покажало дека неговото поведение и неговиот систем на вредности отстапува од оној систем и поведение што општеството го прифатил и го смета за нормален.

Значење на кривичната пријава

Кривичната пријава е известување за стореното кривично дело или за постоење на веројатноста дека е сторено кривично дело за кое се гони по службена должност кое државните органи и правните лица кои вршат јавно овластување или граѓаните според законските обврски доброволно му го поднесуваат на јавниот обвинител непосредно или на друг начин кој според закон е овластен да ги прими[220] и да се потпише дека никогаш нема да го повтори кривичното дело. Родителите исто така го потпишуваат документот кој потоа му се праќа на јавниот обвинител односно судијата во форма на известување. Полицаецот ги известува родителите и малолетникот дека случајот е затворен и дека нема да има ништо понатаму, освен во случај на

[219] Конвенција на правата на детето , 1989 година
[220] Мате Јеремиќ :Коментар ЗКП , Загреб ,148

повторништво. Алтернативните мерки се поевтини од институционалните и затворите и не предизвикуваат поголем број на криминални повратници туку спротивно.

Заклучок

Од клучно значење во постапката спрема малолетниците е секој орган во фазата и во доменот на своето постапување да го утврди фактот што докажува дека малолетникот е сторител на казненото дело бидејќи без тоа нема постапка, нема санкција, но притоа е најзначајно секој од свој аспект да собира податоци за личноста на деликвентот: развој, својства, карактеристики, состојби што упатуваат на причините поради кои го сторил кривичното дело како и својствата и карактеристиките се однесуваат кон санкцијата што треба да се примени и да се совпаѓаат со целите што треба да се остварат .

Африм Цека
Факултет за детективи и криминалистика
Европски Универзитет Република Македонија

Концептот на слободите и правата на човекот наспроти репресивните овластувања на приватните обезбедувачи во Република Македонија

Апстракт
Приватната дејност на обезбедување во Република Македонија во изминаите години се етаблира сериозно во нашиот економски систем. Реформите во областа на приватното обезбедување доведоа до создавање нов концепт. Посебно се значајни реформските фокуси на овластувањата кои ги имаат припадниците на приватниот сектор за обезбедување. Новите законски измени се повеќе го доближуваат приватното обезбедување до овластувањата кои ги имаат полициските службеници, како што се: употреба на средства за присилба, предупредување на лице да се оддалечи од имотот што се обезбедува, забрана неовластено снимање, задржување на лице, преглед на лица, предмети, багаж и друго. Затоа се поставува и прашањето за потребата од почитување на човековите слободи и права при примената на овластувањата од страна на припадниците на приватното обезбедување. Во трудот, се анализира и Кодексот на професионална етика на вршителите на дејноста приватно обезбедување и негово целосно применување. Развивањето на безбедносната свест кај припадниците на приватното обезбедување е од големо значење за почитување на човековите слободи и права.
Клучни зборови: овластувања, слободи и права, обезбедување, доверба.

Human Rights and Freedoms vis-à-vis Repressive Powers of Private Security Providers in the Republic of Macedonia

Abstract
The private security industry in the Republic of Macedonia in the past years has become a serious part of our economic system. Private security reforms have led to the creation of a new concept. Of particular significance is the focus on the authority private sector security personnel has. New legal changes are increasingly bringing private security closer to the powers that police officers have, such as: the use of means of coercion, warning a person to distance himself/herself from the property, prohibiting unauthorized recording, holding a person, a review of persons, items, luggage and more. Therefore, the question of the need for respecting human freedoms and rights in the exercise of the powers of the members of the private security arises. The present paper looks at the Code of Professional Ethics of the private security businesses and its full application. The development of security awareness among members of the private security sector is of great importance to respecting human freedoms and rights.

Key words: powers, freedoms and rights, security, trust.

Вовед

Слободите и правата на човекот се вредности кои имаат глобално, наднационално значење заради неколку аспекти: прво, поминале многу векови за да го поминат патот и да го достигнат вредносното значење и почит; второ, демократскиот капацитет на една држава се перцепира преку нивото на заштита на човековите права; трето, националната рамка за гарантирање на човековите права и слободи се надополнува со меѓународни инструменти. "За меѓународната заштита на човековите права на глобално ниво, посебна улога има создавањето на светската Организација на Обединетите нации, како во однос на стандардите за заштита на човековите права содржани во нејзините документи (правните и концептуалните основи на меѓународното право за правата на човекот), така и за втемелувањето на институциите (тела) за меѓународна заштита (меѓународен интерес за правата на човекот)."[221] За транзиционите општества какво што е македонското, за државите во континуирана реформа во сите сфери на општественото живеење каква што е нашата слободите и правата на човекот се оној критериум кој овозможува да се мери успехот на декларираните стратегии, концепции и доктрини. Овој критериум со вредносно значење има примат над сите останати и со својата содржина во материјална смисла придонесува да се зацврстат темелите на нашата држава посебно.

Слободите и правата на човекот се дисперзирани во областа на културата, економијата, социјалата, политиката, безбедноста и други делови на општествениот систем. Повредата на било кој дел од овие слободи и права остава последици пред се по животот на поединецот, организациите и системот глобално. Меѓутоа, најтешки повреди и загрозување на слободите и правата се оние кои се извршени од страна на државниот присилен апарат – полицијата, разузнавањето, контраразузнавањето, одбраната. Со етаблирањето на приватниот сектор за безбедност во рамките на безбедносниот се поставува и прашањето за односот на приватните обезбедувачи кон слободите и правата на човекот и граѓанинот. Експлицитноста и имплицитноста на ова прашање доаѓа до израз со развојните тенденции на овластувањата на приватното обезбедување и посебно со нивно надополнување со овластувања кои имаат репресивен карактер. Дотолку повеќе што станува збор за област која од една страна се развива континуирано и со интензивно темпо, а од друа страна многу ретко се поставува прашањето за одговорноста на субјектите на приватното обезбедување. Затоа, академската, научната, стручната и експертската јавност денес, повеќе од било кога е исправена пред предизвикот да ги истражува и овие прашања, да навлезе во нивната етиологија, феноменологија, да ги дијагностицира проблемите и прогнозира идните движења со цел да се понудат модели со кои ќе се зајакне концептот на слободите и правата и во оваа мошне сензитивна област. "Поаѓајќи од онтолошката природа на правото како единство на метајуридичката и општествента супстанција, идеите на правото (надискуствено право) и правната стварност (искуственото, позитивното право), основните човекови

[221] Козарев А., Парламентарна контрола и надзор над безбедносниот сектор во Република Македонија, Скопје, 2012 година, стр. 133.

слободи и права не се некоја дистанцирана цел од него, вредност, туку се интерполирани во самото битие на правото и претставуваат материјален критериум за неговата исправност. Антропоцентричната смисла и цел на евроинтегративниот проект се изразува низ осмислување на концептот на човековите слободи и права како отворен и динаминче концепт, чијашто внатрешна движечка енергија ја создава постојаното испреплетување на нормативното и стварното: првото како одредување на повисоки стандарди врз идејата за ограничување на човековите слободи и права единствено со еднаквите слободи и права на другите и со интересите на демократското општество; и второто како создавање реални и ефективни правни и општествени механизми за остварување и заштита на слободите и правата врз постулатите и принципите на демократската правна држава."[222]

1. Слободите и правата – национална рамка за нивна заштита и гарантирање

Слободите и правата на човекот и граѓанинот претставуваат уставна вредност во нашиот правен поредок затоа што се загарантирани пред се со највисоките правни норми во уставно-правниот поредок. Уставните норми поради своето највисоко значење и регулација се посебно значење преку заштитата на човековите слободи и права остваруваат заштита и на вкупниот вредносен систем во нашето општество. "Вредносниот систем на правото покрај останатото се карактеризира со бројни правци и елементи на човековата свест и се оддраз на кокретната стварност, реалност со која е опкружен човекот. Со зголемувањето на диференцијацијата во нормативниот систем и со проширувањето на лепезата на интересите, вредностите стануваат се поапстрактни за на тој начин да можат да опфатат што повеќе и поразновидни содржини, дури и по цена на самите тие вредности да станат уште понеопределени."[223] Покрај уставните норми, слободите и правата на човекот и граѓаниот се заштитени и со бројни законски и подзаконски акти кои ја одразуваат нивната вистинска смисла и значење, преку:

1) Гарантирање на единствен, целосен и неселективен третман на слободите и правата на уставно и легислативно рамниште.
2) Подредување на меѓународните механизми за мониторинг и супранационална заштита на основните слободи и права, по пат на ратификација на меѓународните конвенции за човековите права и прифаќање на надлежноста на меѓународните тела и судски инстанции.
3) Обезбедување внатрешни правни механизми за превенција на повредите на човековите слободи и права (вклучувајќи ефикасен ситем на безбедност и одбрана, спреување на корупцијата, ефикасно функционирање на омбудсманот, ефикасна управа итн.) и

---

[222] Камбовски В., Предговор, Европските стандарди за човековите права и нивната имплементација во правниот систем на Република Македонија, Зборик од научна расправа, Скопје 2008 година, стр. 9-10.

[223] Pusić E., Društvena regulacija, Zagreb, 1989 godina, str. 198. (Во овој контекст, авторот наведува дека настануваат вредности-стандарди, односно такви вредносни поими кои, од самиот почеток, дури и со свесна интенција на оние што нив ги сиздаваат, немаат определен содржина, туку едноставно, тие означуваат само позитивна оценка за определен начин на однесување, односно определен став, без оглед на која содржина се однесува.).

4) Проширување на овластувањата на судот во заштитата на интегралниот и универзален корпус на оносновни слободи и права.[224]

Националната заштита на слободите и правата на човекот и граѓанинот има неколку димензии:

- Нормативна димензија;
- Институционална димензија.

Уставот на Република Македонија ги определува како темелна вредност чија заштита на највисоко хиерариско ниво се остварува преку Уставниот суд односно како "значајна уставна институција затоа што директно (непосредно) уставот тоа го утврдува, односно го предвидува неговото постоење и ја утврдува неговата уставна позиција во системот."[225] Судот ја штити уставноста и законитоста како орган на Републиката воопшто, а преку системот на такстативно набројување на надлежностите во член 110 од Уставот ги штити слободите и правата на човекот и граѓанинот што се однесуваат на слободата на уверувањето, совеста, мислата и јавното изразување на мислата, политичкото здружување и дејствување и забраната на дискриминација на граѓаните по основ на пол, раса, верска, национална, социјална и политичка припадност.

Следното национално ниво на заштита се остварува преку законската регулатива. Притоа, посебно значење имаат одредбите од lex specialis законите кои се однесуваат на полициската, одбранбената, разузнавачката и безбедносната област. Во однос на предмет на научен интерес на овој труд, неопходно е да се истражи регулативата која се однесува на вршење на приватното обезбедување и одредбите за заштита на слободите и правата од евентуални повреди при примената на нивните репресивни овластувања. Законот за приватно обезбедување[226] во член 48 содржи конкретна норма за почитување на угледот и достоинството на граѓаните и обем на примена на овластувањата:

- При примената на овластувањата работниците за обезбедување се должни да ги почитуваат угледот и достоинството на граѓаните, како и основните човекови права и слободи.
- Примената на овластувањата мора да биде пропорционална на потребата поради која истите се применуваат.
- Со примената на овластувањата не смее да се предизвикаат поголеми штетни последици од оние кои евентуално би настапиле, доколку работниците за обезбедување не би ги примениле овластувањата.

Кодексот на професионална етика на вршителите на дејноста обезбедување на лица и имот нормира заштита и унапредување на интересите на државата и заедничкото право на слобода, еднаквост, рамноправност и законитост, правилно и човечно спроведвуање на законите, секогаш со тенденција на решавање на споровите на мирољубив начин, воздржувајки се од примена на насилство и непотребна сила. [227]

---

[224] Камбовски В., цит. труд, стр. 131.

[225] Мукоска-Чинго В., Уставно судство (теорија и практика), Скопје, 2002 година, стр. 227.

[226] Објавено во Сл. Весник на РМ, бр.166 од 26.12.2012 година.

[227] http://obezbeduvanje.org.mk/%D0%BA%D0%BE%D0%B4%D0%B5%D0%BA%D1%81-%D0%BD%D0%B0-%D0%BF%D1%80%D0%BE%D1%84%D0%B5%D1%81%D0%B8%D0%BE%D0%BD%D0%B0%D0%BB%D0%BD%D0%B0-%D0%B5%D1%82%D0%B8%D0%BA%D0%B0-%D0%BD%D0%B0-%D0%B2%D1%80%D1%88%D0%B8/, 2004.2018 година.

Како составен дел на националната рамка за оваа заштита, се јавува и кривично-правната, која е од материјална и процесна природа: материјалното казнено законодавство во Глава XV ги содржи инкриминациите односно групацијата на кривичните дела против слободите и правата на човекот и граѓанинот:[228]

- Повреда на рамноправноста на граѓаните, Член 137;
- Повреда на правото на употреба на јазикот и писмото, Член 138
- Присилба, Член 139
- Противправно лишување од слобода, Член 140
- Грабнување, Член 141
- Мачење и друго сурово, нечовечно или понижувачко постапување и казнување, Член 142
- Малтретирање во вршење на службата, Член 143
- Загрозување на сигурноста, Член 144
- Нарушување на неповредливоста на домот, Член 145
- Противзаконито вршење претрес, Член 146
-Повреда на тајноста на писма или други пратки, Член 147
- Неовластено објавување на лични записи, Член 148
-Злоупотреба на лични податоци, Член 149
- Спречување на пристап кон јавен информатички систем, Член 149-а
- Неовластено откривање тајна, Член 150
- Неовластено прислушкување и тонско снимање, Член 151
- Неовластено снимање, Член 152
- Повреда на правото на поднесување правно средство, Член 153
- Спречување на печатење и растурање печатени работи, Член 154
- Повреда на правото на штрајк, Член 156
- Повреда на авторско право и сродни права, Член 157
- Повреда на правото на дистрибутерот на техничко посебно заштитен сателитски сигнал, Член 157-а
-Пиратерија на аудиовизуелно дело, Член 157-б
- Пиратерија на фонограм, Член 157-в.

Процесното казнено законодавство се одликува со важни процесни одредби за почитување на човековите слободи и права во претходната постапка, главниот претрес и при извршувањето на кривичните санкции. Така, во член 12 ст. 2 од Законот за кривична постапка[229] е наведено дека доказите прибавени на незаконит начин или со кршење на слободите и правата утврдени со Уставот на Република Македонија, законот и меѓународните договори, како и доказите произлезени од нив, не можат да се користат и врз нив не може да се заснова судската одлука. Постојат и други заштитни одредби на слободите и правата на обвинетиот, оштетениот и на другите учесници во кривичната постапка, а кои се дел од клучните цели на кривично-процесната наука: “да се поврзуваат теоретските и практичните знаења и сето

[228] Пречистениот текст ги содржи следните измени и дополнувања на законот објавени во „Службен весник на Република Македонија" број 80/99, број 4/2002 година, број 43/2003, број 19/2004, број 81/2005, број 60/06, број 73/06, број 7/08, број 139/08, број 114/09, број 51/11, број 135/11 , 185/11, број 142/12, број 166/12, број 55/13, број 82/13, број 14/14, број 27/14, број 28/14, број 115/14 и број 132/14.

[229] Службен весник на РМ бр 150/2010 година.

тоа во функција на подобро функционирање на кривичната постапка и остварување на слободите и правата на човекот и граѓанинот."[230]

2.Структура на репресивни овластувања на припадниците на приватното обезбедување

Покрај превенцијата како една од карактеристиките на приватнотно обезбедување, со последните коренити реформи во многу овластувањата на приватните обезбедувачи добија репресивен карактер, со нивно приближување до оние на полициските службеници. Законот за приватно обезбедување како lex specialis во член 1 определува дека предметот на негова регулација се и овластувањата на работниците за приватно обезбедување, меѓутоа во истиот не е дадена конкретна дефиниција за овој поим.

Овластувањата кои ги применуваат работниците за приватно обезбедување ги имаат следните карактеристики:

1.законска заснованост: што подразбира пропишување со нормите на правниот поредок со кои се гарантира исполнетост на определени стандарди при примената на овие овластувања;

2.целна заснованост: тие се применуваат исклучиво за остварување на дејноста на приватното обезбедување;

3.рамка на примена на овластувањата: во точно дефиниран простор, услови и ситуации кои се утврдени со договор за вршење на оваа дејност, со што се гарантира забрана на самоволие и анархија;

4.превентивна димензија на овластувањата: давање значење на проактивната во однос на реактивната примена на овластувањата преку конкретна примена на надлежности од т.н. секундарна ситуациона превенција;

4.репресивна димензија: доаѓа до израз во примената на овластувања со кои се навлегува во сферата на човековите слободи и права преку нивно ограничување во одреден простор и време кои се прецизно нормирани. Во тој контекст потребно е да се наведе дека и во тие случаи мора да се води сметка за баланс помеѓупазарниот критериум и јавниот карактер на оваа дејност која е детерминирана од критериумот за општествена безбедносна одговорност;

5.дефанзивна (одбранбена) репресија: претставува посебна карактеристика која извира од општиот репресивен концепт.[231]

Овластувањата во областа на приватното обезбедување се реализираат во контекст на:

1) Општото политичко опкружување и власт;
2) Правното опкружувње;
3) Технолошкиот развој;
4) Демографските фактори;
5) Социо-културното опкружување во смисла на обичаите, навиките, културата, традицијата и слично.[232]

---

[230] Козарев А., Ибиш Е, Практикум по казнено процесно право, Скопје, 2016 година, стр 9.

[231] Мамути Р., „Криминалитет поврзан приватното обезбедување и неговите реперкусии врз деловното работење на современите компании", (магистерски труд), Европски универзитет, Скопје, 2018 година стр. 23.

[232] Modly D., Durakvić A., Što otežava ili onemogučava profesionalni rad ovlaštenih policijskih službenika, JU Opća biblioteka Tešanj, 2013 godina, str. 12-13.

Надлежностите во областа на приватното обезбедување такстативно се наброени во член 9 од Законот за приватното обезбедување. Постојат два начини на реализирање на приватното обезбедување и тоа: а) физичко и б) техничко.

Нормативната поделба ги опфаќа следните видови на физички овластувања од член 45 на законот и тие табеларно може да се претстават на следниот начин:

Овластувања на приватните обезбедувачи за физичко обезбедување
*врши проверка на идентитет на лица при влез во имотот што го обезбедува
*предупреди лице да се оддалечи од имотот што го обезбедува, ако лицето неовластено се задржува во него, односно да го предупреди лицето кое со своето однесување или пропуштање да стори нешто ја загрозува сопствената или безбедноста на другите или може да предизвика оштетување на имотот што се обезбедува;
*не дозволи влез на неповикано лице, како и да забрани неовластено снимање или внесување на средства и опрема за таа намена во имотот што го обезбедува
*задржи и предаде на полицијата лице затечено во вршење на кривично дело за кое се гони по службена должност, до доаѓањето на полицијата
*врши преглед на лица, предмети, возила и багаж
*употреби средства за присилба

Табела бр. 1: Приказ на видови овластувања во приватното обезбедување

Најмногу репресивноста на приватното обезбедување доаѓа до израз тогаш кога станува збор за примена на присилни средства од страна на приватните обезбедувачи и тоа (член 54 од законот):
1) физичка сила;
2) гумена палка;
3) средства за врзување на лица;
4) хемиски средства (спреј);
5) огнено оружје и
6) дресирано куче.

За правилна и законита примена на овие репресивни средства, законодавецот пропишал дека тие се применуваат само кога работникот за обезбедување не може на друг начин да одбие непосреден противправен напад насочен кон неговиот или животот на лицата кои ги обезбедува или непосреден противправен напад насочен кон уништување, оштетување или отуѓување на имотот што го обезбедува; пред примена на средствата за присилба, работникот за обезбедување е должен гласно да го предупреди лицето спрема кое ќе го примени средството за присилба; средствата за присилба може да се употребат ако целта на постапувањето не може да биде остварена на друг начин; работникот за обезбедување секогаш ќе употреби средство за присилба со кое со причинување на најмала штета ќе ја оствари целта; работникот за обезбедување е должен да престане со употребата на средството за присилба, веднаш штом ќе престанат причините поради кои дошло до негова употреба; за употребата на средствата за присилба, работникот на обезбедување ја известува полицијата веднаш, а најдоцна во рок од еден час од моментот на престанување на вршење на дејствието.

2.1. Употреба на огнено оружје

Приватните обезбедувачи имаат овластување во законска постапка да употребуваат огнено оружје во случај на нужна одбрана (одбивање на непосреден противправен напад за животот или објектот кои се обезбедуваат).[233] Преку дефинирање на случаи во кои е забранета употребата на огнено оружје се создава рамка односно се дефинираат границите во рамките на кои може да дејствуваат приватните обезбедувачи и тие се однесуваат на забрана за оваа употреба во следните случаи:
1) доколку со тоа се доведува во опасност животот на други граѓани;
2) против бремена жена чија бременост е видлива, дете и старец, освен ако овие лица со огнено оружје или со други опасни средства непосредно го загрозуваат животот на работникот за обезбедување или на лицето кое се обезбедува и
3) при обезбедување на јавни собири и други настани.

2.2.Употреба на дресирано куче

Во вршењето приватно обезбедување, дресирано куче се употребува заради одбивање на непосреден напад над работникот за обезбедување, како и непосреден напад над лицето или имотот што се обезбедува. (7) Дресирано куче се употребува во случаите кога: 1) се исполнети условите за примена на физичка сила или 2) се исполнети условите за употреба на огнено оружје.

2.3. Задржување

Законитоста за примена задржување се гарантира со доставување извештај (член 57 од законот) до Министерството за внатрешни работи на подрачјето каде што се извршени дејствијата најдоцна во рок од 24 часа од моментот на престанување на вршење на дејствието, како и за истото да го извести правното лице во кое е вработен во рок од еден час од моментот на престанување на вршење на дејствието, (исто така и правното лице е должно во рок од 24 часа да достави извештај до МВР за примена на дејствието.

2. Како да се постигне балансот помеѓу концептот на човековите слободи и права и (не)опходноста од примената на репресивните овластувања на приватните обезбедувачи?

Клучно прашање кое се поставува во средиштето на овој труд е следното: можна ли е рамнотежа помеѓу неопходноста од почитување, гарантирање и заштита на човековите слободи и права и неопходноста од примена на овластувањата на приватните обезбедувачи со посебен осврт на репресивните?

---

[233] Член 55 од Законот за приватното обезбедување: (2) За напад од ставот (1) точка 1 на овој член се смета секој физички напад на начин или со средство (огнено оружје, опасно орудие или друг сличен предмет со кој може да се загрози животот) кое претставува непосредна опасност по животот, напад кој го вршат две или повеќе лица, односно напад од очигледно физичко посилно лице или лице кое се служи со посебни вештини. (3) За напад од ставот (1) точка 2 на овој член се смета секое дејствие насочено кон уништување, оштетување или отуѓување на имотот што се обезбедува. (4) Пред употребата на огнено оружје, работникот за обезбедување гласно го предупредува лицето за намерата за употреба на огнено оружје.

За да се одговори на ова прашање важно е прејудицијално да се разгледа односот помеѓу јавниот и приватниот интерес кога станува збор за секторот на приватна безбедност и државниот интерес за остварување поголема безбедност на деловните субјекти. Овој сложен однос ги опфаќа следните карактеристики:

- Во приватната безбедност субјектите на безбедноста се координирани и субкоординирани со исходот на приватниот интерес (сопственичкиот, лична или имотна безбедност);
- Во приватното право субјектите на правото се координирани во правен однос, а во јавниот се субординирани;
- Во приватната безбедност главен извор од безбедносни потреби е интересот за лична или имотна безбедност;
- Во приватното право главвен извор на правниот однос претставува волјата на странките, односно договорот. Во приватната безбедност санкциите се регулираат со волјата на странката и граѓанското право и правата кои произлегуваат од него.[234]

Исто така, остварувањето на рамнотежата односно објаснувањето на односот помеѓу овие две потреби е детерминирано од природата на следните видови на приватното обезбедување:

1. Физичка заштита: обезбедување имот, ограничување на губиток и контрола на пристап до објекти и податоци
- Нискоризични работи;
2. Безбедносни услуги: активна превенција на криминалот, ограничени патролирања, примена на локално законодавство врз основа на договор со локалните власти
- Средноризични работи, параполициски работи кои добиваат полициски карактер;
3. Приватни истраги: граѓански и приватни истраги
- Набљудување, проверка на кандидати за прием во работен однос;
4. Корпоративна безбедност: заштита на сложени операции, превенција на криминал против корпорациите и интерни истраги
- Агенти кои се вработени во големи компании и
5. Криминалистички истраги: истражување на измами и сомнителни деловни трансакции
- Сложени работи, често бараат специјалистичка обука, воглавно се присутни во приватната сфера на безбедноста.

Без оглед што овие категории во достапната литература се опишуваат како разграничени облици на дејност, во практиката едноставно е невозможно да се направи разграничување, еден облик на дејност не вклучува елементи од другите, со нив поврзани работи.[235]

---

[234] Marković S., Privatna bezbednost – ljudska potreba I korporativni interes, Zbornik radova, Prvi međunarodni naučni skup, Privatna bezbednost - stanje I perspective, Novi Sad, 2008 godine, str. 227. (Според концепцијат ана природното право, во едниот и во другиот случај во прашање е приватно-економската сфра, имотот на проединецот (dominium), а јавно е тоа каде е во прашање јавната безбедност и јавнат авласт, потреба и интерес за безбедност со која се изразува државниот суверенитет (imperium). Оваа разликување во голема мерка ја изразува трајната суштина и основното обележје на проблемите помеѓу приватната безбедност и приватното право.

[235] Ибид, стр. 69.

Економската безбедност на деловното работење е важен фактор за успешност на компаниите кои пак имаат влијание врз економскиот развиток. Нивната безбедност е значајна функција и таа во современи услови се остварува пред се преку фунцијата менаџер за приватно обезбедување, а во современи услови и преку повисок облик на корпоративната пирамида – менаџер за корпоративна безбедност.

Приватната безбедност како дејност и организација се реализира во услови на актуелниот економскиот амбиент во нашата држава. Како дејност која по својата природа е дел од приватниот сектор во многу е детерминирана од националната економска политика, бизнис климата и дефинираните економски постулати на економскиот систем во целина. Кризата во економијата се рефлектира и врз функционирањето на приватната безбедност која постои на пазарот и каде се почитуваат пазарните законитости. Услугите на приватната безбедност ги користи бизнис заедницата односно деловните компании во секојдневното работење. Тие услуги се гаранција за безбедно деловно работење, а со тоа и за имплементирање на поволно деловно опкружување. Оваа поврзаност и детерминираност на овој систем во многу зависи од влијанието на економскиот развој, посебно за креирање на конкуретнта способност на приватните безбедносни институции.[236]

Секој баланс, секоја рамнотежа претпоставува определен комприс помеѓу задачата и целта. Изборот е клучен фактор на субјектите кои се вклучени во процесот на дејствување. Слободите и правата на граѓанинот се најрелевантен критериум за остварувањ ена овој баланс. Во таа смисла, Камбовски В., забележува дека аподиктичкото значење на човековата слобода и природните права има не само важни етички имплликации, туку претставува и последна одбрана пред опасностите на поп-културата и општата деградација на умот и на културата, што водат кон нов тоталитаризам и неслобода.[237] Психолошкиот аспект на овој проблем лежи во објаснувањето на менталните конфликти кога кај човекот се јавуваат спротивни мотиви и тоа конфликтот на двојно привлекување: овој конфликт во стварноста се состои во колебањето за кој мотив да се одлучиме од двата коишто не привлекуваат. Во овие ситуации, човекот може да стане нерешителен и да западне во конфликтна ситуација. Но, во еден момент, еден од мотивите (целите) станува попривлечен и субјектот се одлучува за него.[238]

Овој прашање несомнено е дека има и психолошка основа која е во функција на детекрирање на клучниот проблем: приватните обезбедувачи имаат обврска да ги гарантира човековите права и истовремено да ја гарантира безбедноста на имотот и лицата преку примена на репресивни овластувања, слично како што државата е должан да ја осигури националната безбедност, но и безбедноста на поединецот (хумана безбедност). И бидејќи државата е институција, а не човечки организам кај неа не може да зборуваме за мотиви, за ментални конфликти, но можеме аналогно да кажеме дека судирот во интересите за човековите права и безбедноста мора да биде решен во рамките на европските вредности, универзалните вредности, метаправни

[236] Козарев А., Влијанието на економскиот развој врз приватната безбедност во Република Македонија, Македонско меѓународно списание за маркетинг, бр. 7, Год. 4, 2018 година, Скопје, стр.30.
[237] Камбовски В., цит. труд, стр. 68.
[238] Јосифоски Д., Криминалистичка психологија, Скопје, 1995 година, стр. 193.

категории и општи (уставни) клаузули. Уште многу одамна Аристотел напишал дека доброто за кое државата тежнее е правдата, а тоа е од општа корист.[239] Нашиот правен поредок гарантира приватните обезбедувачи да ја гарантираат безбедноста на имотот и лицата за кои се надлежни, но и да дејствуваат за некои повисоки безбедносни цели спротивно на интересите и доброто на сите граѓани, наспроти јавниот интерес или јавно добро. Затоа, при објаснувањето на овој сложен однос потребно е да се тргне од поимот јавно добро, за чиешто определување претходно го објаснивме поимот добро. Јавното добро не е било каков интерес кој некоја група може да го има. Станува збор за заеднички интерес на сите индивидуи што нив ги идентификува на траен наин во една битна смисла така што тој делимично станува конститутивен за самиот идентитет на членовите на заедницата и може да претставува основа за подолгорочна солидардност. Јавниот интерес (јавното добро) на индивидуите како членови на политичката заедница, односно како граѓани на државата, а не како припадници на некоја друга заедница е решавање на битните проблеми од аспект на правдата.[240]

Заклучок

Развојот на приватното обезбедување и проширувањето на каталогот на овластувањата на приватните обезбедувачи се остварува во контекст на развојот на слободите и правата на човекот и граѓанинот во современа смисла. Меѓутоа, современа тенденција во областа на приватното обезбедување е нивните овластувања постепено да се приближуваат до полициските, кои пред се имаат репресивна димензија. Токму од оваа причина се наметна потребата да се проучи овој сложен однос, поставен преку прашањето како да се воспостави баланс меѓу овие две потреби, од кои едната – слободите и правата имаат наднационална заштита. За таа цел најпрвин се навлезе во суштината на концептот на слободите и правата на човекот и граѓанинот, механизмите на нивна заштита и правната регулатива како детерминанта за обезбедување на владеење на правото во областа на приватното обезбедување. Приватното обезбедување се спроведува со цел успешно и безбедно функционирање на современите корпорации. Независно дали се работи за обезбедување на имотот на правното лице или телесна заштита на сопствениците на правните лица, приватните обезбедувачи имаат непосредно влијание врз остварување на нивната мисија и визија. Компанијата која е позната во деловниот свет по својата безбедност, успешно реализирани безбедносни процедури и стандарди ужива интегритет и авторитет меѓу останати деловни партнери од земјата и пошироко. Меѓутоа, општ е заклучокот дека повредувањето на човековите слободи и права во текот на реализирање на приватното обезбедување во многу може да го загрози угледот на компанијата која е давател на овие приватни безбедносни услуги. Исто така, може да претрпи негативни последици и компанијата која се обезбедува затоа што таа може да стане несигурен деловен субјект во деловниот свет.

---

[239] Аристотел, Политика, Београд, 1970 година, стр. 3, 84.

[240] Правен живот, бр. 12/1996 година, Скопје,стр. 91.

Затоа е потребно да се зајакне контролата и надзорот над примената на овластувањата на приватните обезбедувачи од страна на надлежните државни органи, но и од страна на невладиниот сектор како вовед за целосна демократизација на овој безбедносен сектор.

Литература

1. Козарев А., Парламентарна контрола и надзор над безбедносниот сектор во Република Македонија, Скопје, 2012 година.
2. Камбовски В., Предговор, Европските стандарди за човековите права и нивната имплементација во правниот систем на Република Македонија, Зборик од научна расправа, Скопје 2008 година.
3. Pusić E., Društvena regulacija, Zagreb, 1989 godina.
4. Мукоска-Чинго В., Уставно судство (теорија и практика), Скопје, 2002 година.
5. Објавено во Сл. Весник на РМ, бр.166 од 26.12.2012 година.
6. Козарев А., Ибиш Е, Практикум по казнено процесно право, Скопје, 2016 година.
7. Мамути Р., „Криминалитет поврзан приватното обезбедување и неговите реперкусии врз деловното работење на современите компании“, (магистерски труд), Европски универзитет, Скопје, 2018 година.
8. Modly D., Durakvić A., Što otežava ili onemogučava profesionalni rad ovlaštenih policijskih službenika, JU Opća biblioteka Tešanj, 2013 godina.
9. Marković S., Privatna bezbednost – ljudska potreba i korporativni interes, Zbornik radova, Prvi međunarodni naučni skup, Privatna bezbednost - stanje i perspecktive, Novi Sad, 2008 godine.
10. Козарев А., Влијанието на економскиот развој врз приватната безбедност во Република Македонија, Македонско меѓународно списание за маркетинг, бр. 7, Год. 4, 2018 година, Скопје.
11. Јосифоски Д., Криминалистичка психологија, Скопје, 1995 година.
12. Аристотел, Политика, Београд, 1970 година.
13. Правен живот, бр. 12/1996 година, Скопје.
14. http://obezbeduvanje.org.mk
15. “Службен весник на Република Македонија”, бр 150/2010 година.
16. „Службен весник на Република Македонија" број 80/99, број 4/2002 година, број 43/2003, број 19/2004, број 81/2005, број 60/06, број 73/06, број 7/08, број 139/08, број 114/09, број 51/11, број 135/11 , 185/11, број 142/12, број 166/12, број 55/13, број 82/13, број 14/14, број 27/14, број 28/14, број 115/14 и број 132/14.

Милош Божиновски , самостоен инспектор
Министерство за внатрешни работи
milosh.bozhinovski@gmail.com

Компјутерски криминалитет и импликациите врз деловното работење во современите корпорации

АПСТРАКТ
Компјутерскиот криминал од година во година станува се повеќе софистициран и ефикасен. Нападите се повеќе се насочени кон корпорациите со цел да се стекнат со тајни податоци. Во овој труд се разработени информационите технологии во МВР во борба против компјутерскиот криминал, сигурноста и заштитата на информациските системи како и процесот на корпорациските истраги. Кражбата на тајните податоци е и понатаму главна причина за настанување на комјутерски инцидент во корпорациите. Компјутерските инциденти се повеќе се случуваат од страна на вработените во корпорациите, што укажува на тоа дека треба да се спроведат ефикасни и јасно одредени правила кои ќе ги заштитат материјалните и интелектуалните вредности на организацијата од кражби и уништување. Најдобрата форензичка пракса докажала дека најдобро е да се формира тим од професионалци: органот за истрага, обвинител, експерт во областа на информациони комуникациски системи, експерт во областа на пресметувачките мрежи, дигитални форензичари и др. по потреба. Во случај на компјутерски криминалитет често е пракса да се побара експертско сведочење или вештачење.

Клучни зборови: компјутерски криминал, сигурност и заштита на информациски системи, корпорациска истрага, безбедносна политика, неовластено собирање на податоци.

Вовед

Во последниве години, општествата ширум светот постигнаа огромен напредок во поглед на воспоставувањето на информатички општества. Информатичките и комуникациските технологии (ИКТ) сега преовладуваат во речиси сите аспекти на животот на луѓето. Потребата за воедначување и систематизирање на глобално ниво на материјалните и процесните норми од областа на компјутерскиот криминал и електронските докази, свој одраз најде во Конвенцијата за компјутерски криминал[241] на Советот на Европа (во понатамошниот текст: Конвенцијата). На Конвенцијата за компјутерски криминал подоцна се надоврзуваат и Конвенцијата за заштита на личните права при автоматизиран процес на обработка на личните податоци[242] со амандманите и Дополнителниот Протокол за авторизиран проток на лични подотоци надвор од државата[243], Дополнителен Протокол на Конвенцијата за компјутерски криминал за заштита од расизам и ксенофобија[244], Конвенција за

[241] Види: http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm
[242] Види: http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm
[243] Види: http://conventions.coe.int/Treaty/Commun/QueVoulezVous.
[244] . Види: http://conventions.coe.int/Treaty/en/Treaties/Html/189.htm

заштита на децата од сексуална експлоатација и сексуално злоставување[245] и Директивите на ЕУ.

1. Сигурност и заштита на информациските системи

Глобалните компјутерски мрежи создале можност за нови облици на криминал. Се појавија посебни, софистицирани, продорни, технички потковани, бескурпулозни, понекогаш освестољубиви поединци на кои тешко можеме да им се спротиставиме, а уште потешко да ги сопреме. Тие често сакаат публицитет за да бидат познати. Лесно шетаат низ сајбер просторот каде се чувствува како дома, па затоа не е лесно да се идентификуваат. Активностите им се олеснети благодарение на огромноста и јавноста на Интернетот. Последиците од електронскиот криминал или од таканаречените вируси, црви или тројанци се големи. Така на пример:

- ,,Во Австрија во 2003 година електронскиот криминал нанесол штета од 3,5 милиони долари, а вирусите, тројанците и црвите 2 милиони долари.
- Во Велика Британија во 2003 година електронскиот криминал нанесол штета од 128 милиони фунти, а вирусите, тројанците и црвите 27,8 милиони фунти."[246]

Безбедноста на информациските систем претставува низа мерки и постапки кои се превземаат за да се овозможи функционалност на информациските систем и интегритет на неговата содржина во сите вообичаени облици на неговото дејствување. Тоа е гаранција дека системот ќе обезбеди непречено извршување на сите операции, одвивање на деловните процеси и ќе ги исполни барањата кои поставуваме. Степенот на сигурност се одредува со квантитативни големини до кои се доаѓа со математички и статистички методи за проценка на ризикот и отпорноста на ризикот и отпорноста на ризични ситуации. За да може да се спроведе соодветна заштита на информациските систем, мора да се направи:

- Проценка на важноста на содржината со податоци која се прави врз основа на анализата на односот на државата кон одделните видови на податоци, според евиденцијата која се води во деловниот систем и врз основа на интересите на раководни структури во деловниот систем.
- Проценка на изворите и обликот на закани на содржината на податоци која се изработува на темелите на претходно споменатите проценки.

2. Тим за истрага на компјутерски криминал

Истрагата на случките кои претставуваат злоупотреба во IKT системите и истрагата на компјутерскиот криминал можат ефикасно да го вршат само високоспецијализирани кадри во рамките на интервентниот тим составен од вработени во нападнатата организација и во надлежните државни органи.[247]

---

[245] Види: http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?CL=ENG&NT=201

[246] Р. Христов., Методика на истражување на електронски криминал ., авторизирани предавања., 2015,Скопје.

[247] ОБСЕ, Прирачник за компјутерски криминал, Скопје, 2014.

Таков пристап единствено овозможува квалитетна истрага и квалитетен начин на собирање, соочување и на судот квалитетно вештачење на дигитални докази за извршниот компјутерски инцидент како и солидна подлога за праведно санкционирање за стореното кривично дело. Успешна и ефикасна работа на интервентниот тим бара и соодветна специјалистичка обука на високостручните кадри- членови на тимот на национално ниво или на ниво на организација. Искуството во информатичко развиените земји кажува дека истрагата треба да започне на корпорациско ниво, да се утврди карактер на инцидентот, дури после тоа се донесува одлука за повикување на званичните органи за истрага на компјутерски криминал. Улогата на независната истрага на незваничниот корпорациски орган е ограничена поради тоа што:

- Поголемиот број на организации не располагаат со соодветен капацитет (кадровски, машински и организациски) за истрага и форензичка анализа.
- Овие органи за истрага ги немаат сите законски овластувања за откривање на трагите на напаѓачот и за заплена на неговиот компјутерски систем како доказен материјал.

Добро решение е да се ангажира стручен консултант за иницијална истрага, аквизиција и форензичка анализа на дигиталните докази и да се води истрага со сопствени снаги, најмалку до моментот на утврдување на природата на инцидентот и донесување на одлука за вклучување/невклучување на званичните истражни органи, бидејќи сепак на крајот мораме да ги повикаме. Организацијата, може да формира свој интервентен тим за брзо реагирање и спроведување на истрага за компјутерскиот инцидент, а празнините во постојниот тим потребно е да се пополнат со придружни (помошни) членови – стручни консултанти, најчесто технички експерти во областа на заштитата на IKT системи или од областа на контролните системи за заштита.

3. **Корпорациска истрага на компјутерскиот инцидент**

Корпорациската истрага може да се смета за предистражна постапка како официјална истрага на компјутерскиот криминалитет. Корпорациската истрага која се спроведува во рамките на организацијата (корпорацијата) во која се случил комјутерскиот криминален инцидент. Започнува од моментот кога инцидентот е откриен. Таа се изведува со специјалисти од организацијата и према интерните правила и процедури кои се предвидени за вакви инциденти. Во моментот кога се случува комјутерски инцидент најкритична е брзината на реакцијата. Во почетната пракса на форензичката истрага на комјутерските докази се покажало дека податоците откриени во текот на првите седум дена се критични за откривање на овој период е многу пократок. Се мери во часови. Според праксата која се применуа во FBI (САД) предистражната постапка се изведува во следните 3 фази:

- Покренување на истрага,
- Одредување дали инцидентот претставува компјутерскиот криминал и
- Анализа на собрани дигитални податоци.

Процедурите кои се користат во текот на истрагата на компјутерскиот инцидент генерално ги содржата следните постапки:

- Проверка на евиденцијата, лог датотека, како и останатите информации за сомнителните.
- Испитување на информантите (лицата од кои можат да се добијат било какви информации)
- Контрола на сите фази од истрагата
- Припрема на органите за пребарување (лоцирање на компромитираниот компјутер)
- Претрес на ресурсите на сомнителните
- Прибирање и анализа на доказите.

Главно тежиште на званичната корпорациска истрага секогаш се насочува на сведоците и сомнителните. Најдобра комбинација во истрагата на комјутерскиот инцидент е заедничка тимска работа на званичните органи на истрагата одредени од страна на сопственикот на информацискиот систем и ИТ специјалисти. Не постои супersвезда во истрагата. Секој учесник има своја задача соодветно на својата специјализација и своето знаење. Праксата покажала дека ефикасни резултати се постигнуваат со 6- те Rossenblatt- ови чекори:

- Елиминација на очигледност,
- Поставување хипотези за извршениот напад,
- Реконструкција на кривичното дело,
- Откривање на траги од компјутерот на осомниченият,
- Анализа на изворниот, индиректниот или пак компјутерот кој е цел,
- Собирање на докази, [248]

После тоа треба да се предадат наодите и доказните материјали на корпорациите или пак на официјалните органи за истрага за понатамошпостапка.[249]

Заклучок

Кривичните дела од стопанскиот криминалитет првенствено ја загрозуваат безбедноста на корпорациите.Најчесто овој вид на криминалитет го извршуваат вработените во компаниите во договор со деловните партнери (работа на штета на компаниите, мито, корупција, измама, проневера, кражба, мито и корупција). Деструкциите, измената на податоци, прекин на работата на системските сервиси (DOS напади), шпионажата и неовластеното користење претставуваат напади изведени од хакери, кракери, вандали, комјутерски криминалци или е-терористи. За жал позади сите малициозни напади стојат луѓе, а не технологии. Луѓето извршуваат криминални дела и тоа секогаш со некаква причина (најчесто поради лична корист). Компјутерскиот криминал како главен мотив за своето делување има материјална добивка.[250]

[248] Milosavljevic M.,,,Istraga kompjuterskog kriminala", Beograd, 2009.
[249] Trivan D., Korporativna bezbednost, Beograd, 2012
[250] Petrović R. S., Kompjuterski kriminal, op. cit.

Свеста за корпоративна култура во македонското општество треба да се подигне на повисоко ниво со цел сопствениците на корпорациите да го заштитат деловното работење. Неопходно е да се направи сериозна анализа на безбедносните закани и ризици од компјутерскиот криминал во деловниот свет. Превземањето на мерки од безбедносната политика која ја дефинира дигиталната форензичка истрага на комјутерскиот инцидент се неопходни за превенција и заштита на информацијата и информационите системи во корпорациите. Особено значаен е аспектот на едукација и обучување на персоналот како и оспособување на носителите на КИС, во спротивставувањето на појавните облици како и идентификувањето на феноменолошките и етиолошките карактеристики на компјутерскиот криминал.

Литература

1. Benjamin S. Buckland, Fred Schrejer, Theodor H.Winkler.: Democratic governance challenges of cyber security: DCAF, Geneva, Switzerland, 2010.
2. Information and security: An International Journal.: Support to the Comprehensive approach. Sofia, 2011.
3. Revolution in the U.S. Information Infrastructure: Copyright 1995 by the National Academy of Sciences: USA.
4. Р. Христов.: Методика на истражување на електронски криминал: авторизирани предавања: Скопје, 2015.
5. Мајкл Д. Лајман., Гори В.Потер.: Организиран криминал: Магор, Скопје, 2009.
6. Milosavljevic M.: Istraga kompjuterskog kriminala: Beograd, 2009.
7. ОБСЕ: Прирачник за компјутерски криминал, Скопје, 2014.
8. Security in cyberspace, Staff statement, U.S. Senate, Permanent subcommittee on investigations, june 5, 1996, http://www.fas.org/irp/congress/1996_hr/s960605t.htm.
9. Trivan D.: Korporativna bezbednost; Beograd, 2012.

Борислав Зукиќ
ЕУРМ –Скопје
Тел: 070/513-577; Е-маил: borislav_zukik@yahoo.com

ИНТЕР-ЛАБОРАТОРИСКАСПОРЕДБАНАДИГИТАЛНИОТ ФОРЕНЗИЧКИ ПРОЦЕС ЗА АКВИЗИЦИЈА НА ДИГИТАЛНИТЕ ДОКАЗИ ОД ОПЕРАТИВНАТА (RAM) МЕМОРИЈА

АПСТРАКТ
Овој труд ги опишува стратегиите за стекнување и анализа на содржината на оперативната (RAM) меморија од референтните системи, ја потенцира потребата од интер-лабораториска форензичка соработка преку споредба на искуствата стекнати при аквизирање на доказите и техниките за анализана истите а со цел да се добие поголема глобална стандардизација на аквизицискиот процес и техниките за анализа на дигиталните докази. Во интер-лабораториската форензичка соработка е вклучена и анализирана целоснатапроцедура на званичната истрага, од испитување на местото на физичкиот криминал до анализата на аквизираните дигитални податоци.
Складираните податоци на меморијата со произволен пристап на компјутерите содржат суштински релевантни информации. Во случај на корпорациска или званична истрагааквизицијатана дигиталните докази е неопходна и од исклучителна важност за ефективна разрешница на истрагата на криминалните дејствија.Од друга страна пак, аквизицијата на содржината на оперативната (RAM) меморија може да биде предизвик доколку не се следат предефенирани процедури.

Клучни зборови: корпорациска истрага, дигитална форензика на RAM, лабораторија за дигитална форензика, компјутерски криминал.

INTER-LABORATORY COMPARISON OF DIGITAL FORENSICS PROCESS USED INDIGITAL EVIDENCE ACQUISITION FROM RANDOM ACCESS MEMORY (RAM)

ABSTRACT
This paper describes the strategies for acquiring and analyzing the contents of the operational (RAM) memory from a reference systems, emphasizing the need for inter-laboratory forensic collaboration by comparing the experiences gained through the digital evidence acquisition process and the techniques used for analyzing this evidenceand consequently, this may lead towards greater global standardization of the acquisition process and techniques used for digital evidence analysis. The inter-laboratory forensic co-operation involves and analyzes the full procedure of an official investigation, from the crime scene examination to the analysis of the acquired digital data.
The stored RAM memory data contains essentially relevant information. In the event of a corporate or official investigation, the acquisition of digital evidence is imperative and of exceptional importance for effective resolution of the investigation of criminal activity. On the other hand, the acquisition of RAM content can be challenging if no pre-defined procedures are followed.

Key words: corporate investigation, digital forensics of RAM, laboratory for digital forensics, cybercrime.

ВОВЕД

Овој труд ќе се фокусира на дигиталната форензика во живо а посебен осврт ќе биде даден на РАМ меморијата.Презентирана ќе биде ситуацијата на аквизиција на дигитални докази во случајот кога нападнатиот систем е составен дел од корпорациски десктоп компјутер кој е активен и е вклучен на струјно напојување. Во кратки црти ќе биде презентирана ситуацијата кога системот не е заклучен во моментот на аквизиција, или ИТ администраторот може да употреби административна лозинка за да влезе во системот без да дојде до рестартирање на истиот. Случајот кога системот е заклучен и шифриран исто така ќе биде елаборирaн врз база на практичните и теоретските решенија. Процедурите и алатките за аквизиција ќе бидат образложени во зависност од ситуацијата. Трудот ќе го завршиме со заклучни согледувања.

АКВИЗИЦИЈА НА ДИГИТАЛНИТЕ ДОКАЗИ

Дигиталната форензика во живо се фокусира на испарливите податоци кои привремено се задржуваат во РАМ меморијата на компјутерот кој е во работен режим. Во повеќето случаеви испитувањето на криминалното дејствие и дигиталната форензичка анализа започнува со пријава на компјутерскиот инцидент, или кривичното дело, до органите за корпорациска истрага или званичните органи за истрага. Пријавата до званичните органи за истрага може да се изврши и откако биде извршена корпорациската истрага, која го потврдила и идентификувала компјутерскиот инцидент и е потребно ангажирање на званичните органи за истрага. Секој подносител на барање очекува од органите за истрага да поседуваат високо ниво на знаење и експертиза.

Во основа имаме три општо познати сценарија со кои форензичарите се среќаваат при аквизиција на содржината на РАМ меморијата а кои ќе бидат елаборирани по комплексност:

1- Компјутерот има тврд диск, не е заклучен, или ИТ администраторот има можност да го отклучи со употреба на административна лозинка без потреба да го рестартира истиот.

1-1 Компјутерот нема тврд диск, не е заклучен, или ИТ администраторот има можност да го отклучи со употреба на административна лозинка без потреба да го рестартира истиот.

2- Компјутерот има тврд диск, е заклучен, лозинката е недостапна и ИТ администраторот нема можност да го отклучи со употреба на административна лозинка без потреба да го рестартира истиот.

2-1 Компјутерот нема тврд диск, е заклучен, лозинката е недостапна и ИТ администраторот нема можност да го отклучи со употреба на административна лозинка без потреба да го рестартира истиот.

3- Компјутерот е заклучен без можност од употреба на административна лозинка или лозинките од корисниците. Компјутерот нема ExpressCard, firewire, или thunderbolt.

3-1 DDR3 и DDR4 ладно подигнување на системот.

ПРЕМЕСТУВАЊЕ НА КОМПЈУТЕРОТ

Околностите во кои се изведува корпорациската истрага понекогаш диктираат да нападнатиот систем биде отстранет од просторијата во која се случило криминалното дејствие и биде преместен во контролирана лабораториска околина. Деталите нема да бидат елаборирани, меѓутоа ќе напоменеме дека литературата и лабораториите се слагаат дека следнава процедура треба да се почитува:

- Напојувајте го влезот на UPS од истото мрежно напојување како и целниот систем, може да се користи кабел за напојување со неколку приклучоци,
- Почекајте UPS-от да се синхронизира на електричната мрежа, обично се слуша звучен клик од внатрешните релеи на UPS-от,
- Излезниот поларитет и поларитетот на дестинацијататреба да се исти,
- Поврзете го излезот до дестинацијата со користење на точниот поларитет,
- Исклучете го кабелот за напојувањена компјутерот од sидниот штекер,
- Исклучете го UPS-от од електричната мрежа.

ПРИПРЕМИ ЗА ХАРДВЕРСКА АКВИЗИЦИЈА

Дигиталната форензикана RAM меморијата е поле кое се развива и кое допрва треба да достигне целосна зрелост.Таа е фундаментален дел од процесот на истрага за инцидентот, на пример, во ситуации кога по откривање на упад или инфекција со малициозен софтвер многу е важно да се прибератсите испарливи податоци кои инаку би можеле да се изгубат кога системот ќе се исклучи.Пример е листата на тековни системски сервиси и кориснички процеси, во моментоткористени драјвери и модули, дури и мрежни врски,рутирање и ARP табели.Сите овие податоци можат да се соберат со користење на алатки за аквизиција од компјутери кои се сеуште во работен мод, но исто така може да се спроведе и анализирање на RAM мемориската слика.Дополнителни докази како што се корисничката лозинка и декриптираните клучеви за шифрирање на податоците и фрагменти постојат само во RAM меморија. За пример напредните датотеки или малициозните програми кои ја користат единствено RAM меморијата не создаваат датотеки на тврдиот диск и истите можат да се откријат само од анализата на RAM меморијата. Модерните оперативни системи користатвиртуелна меморијата за управување со главната меморија. Windows ги заменува страниците во датотеката со датотека со екстензија „.sis“ која се наоѓа во главниот системски уред, додека пак UNIX и Linux ја користат swapпартициската анализа на датотеката со страница.Од корист е да спомнеме и дека за да се добие комплетен поглед на целата виртуелна меморија друг извор на докази е датотеката за хибернација каде што оперативниот систем ја зачувува целата содржина на RAM пред да замине во хибернација.Windowsја користи датотеката„hiberfil.sys“ и е лоциран во главниот системски диск, додека Linux генерално ги користи swap партициите, но исто така може да користи swap-датотека, а понекогаш и депонии на несреќи генерирани од оперативниот систем кога апликацијата ќе се урне може да бидат од интерес за

форензичарот, тие можат да бидат во форма на целосна депонија на меморија или мали депонии кои содржат повеќе ограничени групи на податоци. Пред да се започне со било каква аквизиција на содржината на тврдите дискови и РАМ меморијата неопходно е да се направи фотографска или видео евиденција на целиот компјутерски систем, да се идентификува хардверот, оперативниот систем, и софтверот кој е инкорпориран во компјутерот.

АКВИЗИЦИЈА НА РАМ МЕМОРИЈА

Првото сценарио на аквизиција на содржината на РАМ меморијата е готово идентично спроведено и документирано како во литературата, така и од страна на лабораториите за форензика. Истата процедура е применлива и во останатите две сценарија со исклучок на софтверските и хардверските решенија кои се достапни на форензичарите. Мора да нагласиме дека независно од методата или алатка која е избрана форензичкиот тим мора постојано да ги снима и документира сите чекори кои биле преземени при процедурата на екстракција на содржината на РАМ меморијата. Одредени отстапки се јавуваат во алатките кои се користат, меѓутоа тоа е ирелевантно доколку тие се прифатливи за јурисдикацијата во која се спроведува истрагата. Прв чекор секогаш е да се утврди дали компјутерот има некаква заштита во вид на лозинки и енкрипции. Најсовршено сценарио е кога компјутерот нема лозинка, или кога ја имаме лозинката. Во тој случај се пристапува кон екстракција на содржината од рамот. Оваа процедура мора да биде завршена пред да биде исклучен компјутерот. Вообичаено е форензичките решенија кои се користат да се во вид на апликации кои се складирани на УСБ апарат. По правило на истиот УСБ апарат се алоцира простор на кој ќе се направи РАМ меморискиот дампинг. Поради намалување на интеракцијата на форензичките алатки со РАМ меморијата најпожелно е да првично се знае типот на оперативен систем и самата хардверска конфигурација на компјутерот кој се испитува. Самите форензички алатки вообичаено имаат можност да го идентификуваат оперативниот систем и конфигурацијата на компјутерот, меѓутоа како и секоја апликација така и форензичката ја менува содржината на РАМ меморијата, а тоа во краен случај сакаме да го избегнеме. За Windows оперативните системи 32битните и 64бинтните општо прифатена алатка е FTK Imager[251]. Оваа апликација дава можност да се направи и форензичка копија на „pagefile“ датотеката од оперативниот систем.Пред да се почне било каква екстракција на РАМ меморијата треба да се направи снимка на дата и време од BIOS и на HASH вредностите на РАМ меморијата, една од апликациите која може да се користи е „md5sum“. За споредба, кога се прави слика од содржината на тврдиот диск HASH вредностите по правило не би требало да бидат сменети пред и после исклучувањето и отстранувањето на дискот, кај РАМ меморијата овие HASH вредности постојано се менуваат па собирањето на вредноста е од исклучителна важност пред да се направи дампингот и откако ќе се направат дампингот со цел да имаме важечки HASHвредности за копиите кои ќе послужат за анализа. Јурисдикцијата во која

[251]Email од Stephanie Corvese, Grant Thornton LLP до авторот, 9 Април 2018

оперира лабораторијата ја признаваат HASH вредноста како неоспорен доказ. Кога станува збор за Linux,Unix, или MACos вообичаено се користи Volatility, LiME, osxpmemили интегрираните алатки од командната линија „md5sum“или „mac_hash“. Овие апликациисе релативно мали и не нанесува преголеми дисторзии во РАМ меморијата која ја користат за извршување на операциите.Кај MACos аквизицијата на содржината од РАМ меморијата е возможна само доколку форензичарите користат администраторска лозинка. За да се дојде до административниот кориснички екран потребен е мек рестарт. Под нормални околности, некој би помислил дека рестартирањето на компјутерот ќе ја уништи можноста за собирање на RAM меморија. MACos компјутерите се различни и ова не е нужно правило. Тестирањата покажале дека може да има губење на меморијата, но износот на загуба не мора да биде значаен. Форензичарите треба да бидат свесни дека RAM меморијата на компјутерите на Apple е компресирана, така што просторот достапен на излезниот волумен треба да биде околу 50% поголем од основната RAM меморија инсталирана на системот. Потребен е HFS + волумен како дестинациски диск.За аквизиција на содржината на тврдиот диск без разлика на оперативниот систем е препорачливо да се користи друг УСБ диск со алоциран мемориски дел на кој ќе биде складирана сликата од дискот. Доколку тврдиот диск или УСБ дискот на кој е системот е криптиран најдобро е да за направи логичка аквизиција на истите пред да се прејде на РАМ меморијата. Се разбира сите УСБ дискови треба да се означат со налепници, заштитат и складираат. Аквизицијата на содржината на тврдиот диск е надвор од доменот на овој труд.

Кај второто сценарио се применуваат хакерски техники кои мора детално да се евидентираат и документираат со цел да бидат прифатени во јурисдикцијата каде оперира лабораторијата. Постандардни решенија за отклучување на заклучените компјутери се понудени во форма на картичка и уред (CaptureGUARD Express и CaptureGUARDGateway) кои се користат на Windows платформите (од XP, VISTA, па до WIN10). Овиерешенија се базирани наExpressCard картичка и уред кои можат да ја прикажат физичката меморија на компјутерот на кој се поврзуваат и истите спроведуваат аквизиција на содржината на РАМ меморијата без потреба да системот биде рестартиран или исклучен. Првата солуција создава депонирани датотеки во стандардниот WinDD формат, кој може да се користи со WindowsSCOPECyberForensicsUltimate или со други алатки за анализа на депонираните датотеки кои се компатибилни со WinDD. Недостаток е да и при користење на овие решенија содржината на самиот РАМ до некоја мерка се менува поради драјверите кои се инсталираат при користење на картичката и уредот. Поголем недостаток е фактот дека компјутерите со читач за Express Card, firewire, thunderbolt или слични „SerialBusProtocol 2“решенија стануваат се поретки и се заменети со УСБ технологија. Кога станува збор за Linux, вообичаено е да лозинките се „salt HASH“ заштитени и во поновите верзии се користиSHA256 и SHA512HASH, што ги прави тешки за откривање со „brute force“, „rainbowtables“ или „wordlists“. Процесот за РАМ мемориска аквизиција подразбира воспоставување далечинска врска со нападнатиот компјутер клиент преку SSH при што се остварува мемориски дампинг. За Linux и доколку се успее да се дојде до терминалната команда постои веројатност

дека напаѓачот има активирано некој „rootkit“што користи анти-форензички методи, тие или го поткопуваатпроцесот на аквизиција на содржината на РАМ меморијата при користење на LiME, или пак оперативниот систем се урива при користење на директното мемориско дампирањена„pmem“.После РАМ аквизицијата форензичката процедурата е иста како и во претходното сценарио.
Третото сценарио подразбира иновативни техники кои во целост не се еалборирани во стручната литература дали поради недостаток на информации или едноставно се дел од деловни тајни достапни само за најелитните форензични лаборатории или агенциите за безбедност. Во вој труд само ќе ги споменеме можностите кои се поткрепени во научни трудови од реномирани форензични лаборатории. Според трудовите издадени до денешно време, кога станува збор за Windows или Linux оперативните системи ова и не е некој предизвик доколку системот користи РАМ мемории од типот на DDR2 или постари модели на РАМ мемории. Имено може да се користи веќе докажаниот метод „ColdBootAttack“.Додека нападнатиот компјутер е во режим на работа се пристапува кон разладување на РАМ меморијата со индустриски спреј за ладење на облоги кој не спроведува електрична енергија.Спрејот ја намалува температурата на РАМ меморијата во толкава мерка што меморијата не ја губи мемориската содржина во временски интервал и до 10 минути. Компјутерот се исклучува од напојувањето, или за Linux може да се суспендира на РАМ на пример па исклучи. РАМ меморијата се вади и се приклучува на компјутер кој ќе се користи за аквизиција на РАМ содржината. Во компјутерот за аквизиција се вметнува вообичаено УСБ со апликација која ќе направи екстракција на содржината од оладената РАМ меморија при првичното подигање на системот. За напомена е дека суспендирањето на компјутерот на RAM меморија треба да се смета за опасно бидејќи понекогаш компјутерот не може правилно да продолжи, или може да побара BIOS лозинка.Недостаток е што повеќето BIOS-и на модерните компјутерски плочи ја бришат содржината на РАМ меморијата при првичното подигање.Кога станува збор за DDR3 и DDR4 мемориите мора да се земе во предвид дека самите мемории подлежат на поголема испарливост на податоците и имаат понапредни заштитни мерки во форма на шифрирање на податоците. Од друга страна пак докажана е ранливоста на LFSRенкрипцијата и фактот дека може да се пробие со само 50 битен знаенчист текст доколку станува збор за единичен РАМ модул, сосема е друга ситуацијата доколку се користат повеќе РАМ модула. Во полза на „ColdBootAttack“ е и фактот дека поновите РАМ мемории се понеосетливи на термичко распаѓање на податоците во споредба со постарите модели DDR2.

АНАЛИЗА НА ПОДАТОЦИТЕ

Следниве артефакти може да се очекуваат од процесот на стекнување и анализа на содржината на РАМ меморија: системски процеси, сервиси кои се користат, информации за таблата со исечоци, сесиите за прелистување (инкогнито сесии), лозинки, датотеки и мултимедија кои се користат, чатови / складирани податоци на активните апликации.

Податоците од минатото исто така може да се извадат од RAM-от, процесите кои биле користени од пред некој саат време па до месец дена зависно од тоа колку бил активен компјутерот. Анализата никогаш не смее да се спроведува на оригиналните дампинг дискови и материјали. Други алатки кои исто така се користат се AXIOM, COFFEE, BelkasoftLiveRamCapturer, Volafox, The Coroner's Toolkit, HashKeeper, CodeSuite, RegRipper, Windows Scope Cyber Forensics, Registry Recon, и XRY. Kaj Linux оперативните системи за да ја анализирате депонијата со на пример Volatility, треба да кре-ирате профил кој се совпаѓа со системот од каде што е дампирана меморијата: за да го направите ова, треба да компилирате C програма во системот и да користите „dwarfdump".Во случај да е потребно ресетирање на лозинката,декрипцијатана HASH датотеките е една од опциите, на пример со „sudosu",„Hashcat",или„oclHashcat" која пак користи предности од GPU за про-наоѓање на лозинките. Резултатите и анализата се документираат и се прави извештај.

ЗАКЛУЧОК

Имајќи ги во предвид изобилието на оперативни системи, компјутерски конфигурации, и решенија кои се достапни во моментов во светот предизвик е за дигиталните форензичари да одредат и да се согласат околу правилна процедура па и околу алатките кои би можеле да биде применувани при секој случај. Во извесни точки процедурата на аквизиција е стандардизирана кога зборуваме за RAM меморијата, меѓутоа како што веќе беше елаборирано во второто и третото сценарио процедурата може да наиде на пречки од типот јурисдикциони и правни пречки па се до немање соодветен кадар или опрема. Од друга страна пак малициозниот софтвер бележи се пософистициран развој на кој и самите дигитални форензичари и лаборатории немаат соодветен одговор. Само за пример ги наведуваме Spectre илиMeltdown малициозните алатки кои се стационирани во целост во RAM меморијата а ги искористуваат хардверските и софтверските грешки на Intel како и на другите процесори и самиот CPU cache од една страна и недостатоците во шифрирањето на DDR3 и DDR4 мемориите од друга страна. Потенцираме дека ова е еден од многуте примери кои може да бидат експлоатирани со употреба на обична JAVA скрипта на било кој интернет сајт било каде во светот. Овој пример е само еден во океанот од многу кој го наведуваме со цел да ја истакнеме потребата од поголема соработка помеѓу форензичките лаборатории во споделување на најновите техники и методи за аквизиција на содржината на RAM меморијата од живите системи во случаи кога компјутерот е целосно преземен од напаѓачот а вообичаените процедури наведени во овој труд па и пошироко сенекорисни а последиците може, а и се најчесто, глобални кога не се преземаат соодветни мерки како што го покажа случајот со WannaCry во 2017 година.

КОРИСТЕНА ЛИТЕРАТУРА

1. Bovet, D., &Cesati, M. UnderstandingtheLinuxKernel (3 ed.). Sebastopol. 2006.
2. Binnie, C. Linux Server Security: HackandDefend. 2016.
3. AccessData. (2016). PasswordRecoveryToolkitandDistributedNetworkAttack.

4. Kavrestad, J. Guide to Digital Forensics: A Concise and Practical Introduction. 2017.
5. Rochmadi, T., Riadi, T., Prayudi, Y.:LiveForensicsforAnti-ForensicsAnalysisonPrivatePortable Web Browser: InternationalJournalofComputerApplications. Vol. 164 – No 8 (2017)
6. Bauer, J., Freiling, C.: Lestweforget: Cold-bootattacksonscrambled DDR3 memory: DFRWS 2016 EuropeProceedingsoftheThirdAnnual DFRWS Europe - DigitalInvestigation. Vol 16 (2016)
7. Austin, T., Aga, T., Das, R., Yitbarek, S.: ColdBootAttacksareStillHot:SecurityAnalysisofMemoryScramblersinModernProcessors: 2017 IEEE InternationalSymposiumonHighPerformanceComputerArchitecture. (2017)
8. Schramp, R.: Livetransportationand RAM acquisitionproficiencytest : DigitalInvestigation. (2017)
9. Schatz, B., Cohen, M.: Advancesinvolatilememoryforensics: DigitalInvestigation. (2017)
10. Block, F., Dewald, A.: Linuxmemoryforensics: Dissectingtheuserspaceprocessheap: DigitalInvestigation. Vol. 22. (2017)
11. Case, A., KusumDas, A., Park, SJ., Ramanujam, J.: Gaslight: A comprehensivefuzzingarchitectureformemoryforensicsframeworks: DigitalInvestigation. Vol. 22. (2017)
12. Carbone, F. ComputerForensicswith FTK. 2014.
13. Skulkin, S. deCourcier, S. Windows ForensicsCookbook. 2017.
14. Johansen, G. DigitalForensicsandIncidentResponse. 2017.
15. Malin, H. LinuxMalwareIncidentResponse: A Practitioner'sGuidetoForensic. 2017.
16. Stephenson, P. Official (ISC)2® Guidetothe CCFP CBK. 2017.
17. Binnie, C. Linux Server Security: HackandDefend. 2016.

Роберт Вртески
Факултет за детективи и криминалистика
Европски Универзитет Република Македонија

Апстракт
Најголем мотив за истражувањето на оваа тема се различните видови на професиии кои произлегуваат при секодневното собирање на сите информации без оглед на тоа дали станува збор за повеќе или помалку издржани информации. Горенаведеното се поткрепува со фактот дека разузнавањето се извршува кога голем број на различни информации се собираат заедно, па откако ќе се сублимираат тие се обработуваат за да на крај се извлечат нови заклучоци во различни полиња од науката, културата, и образованието. Најнапред во ова истражување ќе зборуваме за историските, тековните и предиктивните погледи во работењето на бизнис разузнавањето, кое, често пати има за цел да го подржи донесувањето на крајните одлуки во бизнис околината. Проблематиката на ова ова истржување со состои од споредбена алнализа на успехот на големите и на малите претпријатија при работата со бизнис разузнавање. Целта на истражувањето е исто така, благоречено идентична со целта на деловното разузнавање а таа се состои од винстинска информација во вистинско време и на вистинско место за да може да се донесе вистинска одлука во малите и големите бизниси, и добивање на предност пред конкуренцијата.

Клучни зборови: информација, стратегија, профит, конкуренција, разузнавање.

Business intelligence

Abstract
The biggest motivation for this research paper on business intelligence are the vast types of professions that are developed from everyday information gathering, regardless of the sustainability of the information itself. The above said is supported with the fact that intelligence is created when a lot of different information are gathered together, sublimed, and after they are processed we can achieve new conclusions in the fields of science, culture and education. As an introduction in this research, we'll talk about past, present and future views of the business intelligence, that more than often has a primary goal to support decision making in the business environment. The main goal in this research is to compare the success of the business intelligence of the big and small businesses while managing the business intelligence. Also, the main goal of this research is supported by the fact that getting the right information in the right place and time can help small and big corporation to make the best decision for their businesses, and get a step ahead of the competition.

Keywords: Information, strategy, profit, competition, intelligence.

Вовед

Современ тренд претставува се позасиленото темпо за користење на услугите од приватните детективи во деловниот свет. Искуството покажува дека делониот успех во многу е детерминиран од деловната безбедност, односно од деловното безбедносно опкружување. Оваа услуга значи и повеќе финансии заради плаќање на истата од страна на деловните компании. Од друга страна, во деловната заедница преку обезбедување на поголема безбедност се придонесува за зголемување на интегритетот, угледот и довербата перципирана од остананите деловни субјекти. Може да се наведе дека не постои подрачје од бизнисот во кое нема свое место бизнис разузнавањето. Како што наведува д-р Г. Цветковски: "токму поради овој факт, големите реномирани компании формираат сопствен систем за деловна заштита на корпоративно ниво, исто како што секоја држава има безбедносно-разузнавачка служба на национално ниво. Малите и средни фирми кои не се во можност посебно да инвестират во оваа област или процениле дека тоа би бил нерационален задат, за оваа цел користат детективиски услуги, односно специјализирани консалтинг агенции. Со помош на нив се добиваат информации за сопственоста и менаџментот на конкретна фирма, предметот на дејност, факти, бонитет, биланси, индиректни врски меѓу лица и фирми и други сознанииja и податоци."[252]

Неспорноста на овие факти поврзани со реалноста на потребите на современите корпорации ја наметнува потребата да се даде одговор на следните прашања: дали овој современ тренд на користење на детективските услуги е присутен на исто рамниште во светот? Дали постојат диспропорции во оваа област на работење? Дали се исти надлежностите на приватните детективи воопшто и посебно во областа на деловното работење во различни држави?

Во обидот да се даде точен и прецизен одговор на овие прашања потребно е најпрвин да се навлезе во природата на бизнис разузнавањето, да се објасни неговата структура и значење, односот со јавниот безбедносен сектор итн. Сложеноста на овие прашања во многу е детерминирана од сложените односи во глобалното опкружување, тајноста во дејствувањето на приватните детективи, нивните специфични надлежности и контролата над нивната дејност.

1. Дефинирање на бизнис разузнавањето

За да се дефинира бизнис разузнавањето потребно е претходно да се определи природата на економската и деловната шпијунажа, под која се подразбира "функционално собирање податоци од економски, финансиски и друг деловен карактер за другии држави, општествени организации, економски и финансиски институции и компании заради заштита на сопствените интереси. Деловната шпијунажа ги опфаќа сите легални дејствија и процеси кои се спроведуваат со цел на компаниите да им се даде предност на пазарот во однос на конкуренцијата."[253] Неспорно е дека "економската шпијунажа претставува една од многуте важни полуги на корпоративната и

[252] Цветковски Г., Професија приватен детектив, "Панили", Скопје, 2011 година, стр. 259.

[253] Стојановиќ М., Павловиќ Д., Економска безбедност пословања, Београд, 2014 година, стр. 30-31.

вкупна национална моќ, затоа што силен стопански систем претставува и здрава и цврста основа на општествениот поредок на земјата, нејзината воена сила, потенцијал за одбрана, монетарна сила, политичка стабилност и јакнење на позицијата на владата на секоја земја како на внатрешен така и на надворешен план."[254] Современите ризици и закани во деловниот свет се поврзуваат со најразлични феноменолошки облици на економска односно деловна шпијунажа, на која се надоврзуваат етиолошките елементи и на тој начин преку синтеза се доаѓа до природата на бизнис разузнавањето кое е логична последица на оваа конкретна, непосредна и континуирана закана. Имено, бизнис разузнавањето во последно време забележува брз раст и се усредоточува кон собирање на податоци и информации, нивна обработка, анализа и предлагање решенија кои се корист на една современа корпорација или деловен субјект. "Сепак, неговата суштина е поседување на бизнис информации заради супериорност во однос на конкурентите и следствено на тоа, донесување правилни одлуки од страна на менаџментот на фирмата. Поедноставено, тоа значи способност да се соберат, обработат (анализираат) и употребат информации кои претставуваат клучен менаџерски ресурс во новите бизнис услови. Во светот овие работи се познати под името due diligence."[255] Бизнис разузнавањето претставува значајна содржина во работните задачи пред се на менаџерите за корпоративна безбедност кои се етаблирани во современите корпорации. За нивната работа од големо значење се информациите поврзани со деловното работење. Законската дефиниција на поимот информација кај нас го подразбира само она сознание кое го менува знаењето на приемачот, односно сознанието кое дава ново знаење, различно од претходното. Информацијата е сознание кое може да биде пренесено во која било форма. Од друга страна, нејзината безбедност може да се претстави на следниот начин:

Слика бр. 1 Информатичка безбедност

[254] Marković S., Osnovi korporativne i industrijske bezbednosti, USEE, Novi Sad, 2007 godina, str. 185.
[255] Цветковски Г., Професија приватен детектив, "Панили", Скопје, 2011 година, стр. 260.

Оттука, може да се забележи дека круцијално значење поврзано со бизнис разузнавањето има информацијата воопшто или деловната информација посебно. Затоа, обезбедувањето на точни деловни информации и нивна заштита се остварува преку структурите и инструментите на бизнис разузнавањето во денешно време.

2.Надлежности на македонските приватни детективи во областа на деловното работење

Приватната детективска дејност во нашата држава претставува дел од приватниот безбедносен сектор настанат после стекнувањето на македонската независност и самостојност. Развивана со бавно темпо и без осовременување на оваа дејност претставува една од посуштинските слабости со кои се карактеризира и по кои е препознатлива во јавноста. Постои перцепција дека оваа дејност повеќе се реализира конспиративно од лица кои ниту имаат лиценци и легитимации за детективи, ниту пак ги исполнуваат условите за нивно добивање. Од истражувањето на податоците во Централниот регистар каде што се регистрира оваа дејност може да се нотира дека:

Овие слабости имаат системски карактер и придонесуваат за бавното професионално развивање на дејноста на приватните детективи.

И покрај оваа реална состојба, законската омеѓеност на приватната детективска дејност е клучна детерминанта за нејзино етаблирање во економскиот систем на државата. Специјален закон за вршење на оваа дејност претставува Законот за детективска дејност, донесен во 1999 година.[256] Во член 12 од законот е дефинирана природата на податоците и информациите кои може приватниот детектив да собира, а како позначајни и поврзани со бизнис работењето може да се наведат следните:

- за обезбедување на доказни материјали во врска со кривични дела или сторители на кривични дела. Понекогаш во текот на работењето доаѓа до извршување на кривични дела (кражби, измами, деловна шпијунажа итн.) заради што се јавува потребата правните лица да се обратат до приватните детективи за прибирање на овие податоци и информации и тоа од повеќе причини: прво, брзината на дејствување на приватните детективи, второ, конспиративноста во нивното работење, трето, односот кој се воспоставува на релација приватен детектив – корисник на услуга кој припѓа на бизнис заедницата итн.;
- за лица кои се исчезнати или сокриени, за пишувачи на анонимни писма или за причинители на материјална штета. Не ретко во текот на извршувањето на бизнис задачите поедини лица, посебно во делот на менаџерското раководење се соочуваат со писмени закани од одделни

[256] Овој закон е менуван и дополнуван со следните закони: Законот за изменување и дополнување на Законот за детективска дејност („Службен весник на Република Македонија“ бр. 66/07), Законот за дополнување на Законот за детективска дејност („Службен весник на Република Македонија“ бр. 86/08), Законот за изменување и дополнување на Законот за детективска дејност („Службен весник на Република Македонија“ бр. 51/11), Законот за изменување и дополнување на Законот за детективска дејност („Службен весник на Република Македонија“ бр. 164/13), Законот за изменување и дополнување на Законот за детективска дејност („Службен весник на Република Македонија“ бр. 148/15), Законот за изменување и дополнување на Законот за детективска дејност („Службен весник на Република Македонија“ бр. 193/15) и Законот за изменување и дополнување на Законот за детективска дејност („Службен весник на Република Македонија“ бр. 55/16)

вработени кои од најразновидни побуди се одлучуваат да пристапат кон таков облик на комуникација. Исто така, се случува некој вработен да исчезне под сомнителни околности и во тие случаи, покрај ангажманот на полицијата се јавува потребата да се ангажираат приватни детективи кои со примена на нивните надлежности придонесуваат за расветлување на настанот и откривање на неговиот предизвикувач;

- за откривање на идентититет на лице и негово живеалиште, односно престојувалиште. Постојат ситуации кога определено лице вработено во една приватна компанија да доставува лажни податоци за својот вистински идентите или неговото живеалиште односно престојувалиште. Посебно овие ситуации се среќаваат при спроведување на првично интервју за вработување кога определени факти не се поклопуваат со одредени статусни состојби. Во тие ситуации приватниот детектив може да им помогне на приватните компании да ги елиминираат евентуалните сомнежи и да ја откријат вистината во погоден момент.

- за украдени или изгубени предмети. Кражбата на одредени предмети односно нивното губење може да предизвика дополнителни финансиски трошоци за компаниите. Со цел нивно спречување или пак откривање во благовремен период, услугите на приватните детективи се голема корист;

- за односот на работниците спрема заштитата на деловната тајна.

- за успешноста и деловноста на правни лица.

3.Улогата на бизнис разузнавањето во заштитата на деловната тајна

Под поимот деловна тајна се подразбира збир на податоци и информации кои се користат во работењето, а кои припаѓаат на деловните субјекти, доведуваат до економска корист и обезбедуваат одредени предности над конкуренцијата.[257]

Деловната односно трговска тајна претставува комплекс од податоци и информации што се користат во деловното работење на компаниите односно деловните правни лица чиј што степен на тајност е во функција на остварување економска предност и бенефит за една корпорација. Правото на заштита на деловната тајна има национална и меѓународна димензија. На национално ниво, деловната тајна е предмет на нормирање во одделни одредби од Законот за работни односи[258] (член 35) каде е определено дека работникот не смее да ги искористи за своја сопствена употреба или да ги предаде на трето лице податоците што се сметаат за деловна тајна на работодавачот, кои како такви со посебен акт ќе ги определи работодавачот и кои му биле доверени на работникот или со кои бил запознат на друг начин. Исто така, работникот е одговорен за издавање на деловна тајна, ако знаел или би морал да знае за таквото својство на податоците. Притоа, секој работник кој доаѓа во контакт со материјали, информации и податоци кои се класифицирани е должен да ја чува тајната на истите. За таа цел, претставниците на работниците и сите експерти што им помагаат, не смеат на работниците или на трети страни да им откриваат какви било информации кои

[257] Katilić T., Uvod u zaštitu intelektualnog vlasništva u Republici Hrvatskoj, CARnet, Zagreb, 2006 godina, str. 50.

[258] Службен весник на РМ бр. 167/2015 година.

се од деловен интерес на работодавачот, а кои јасно им биле кажани во доверба. Оваа обврска продолжува да важи и по завршувањето на нивниот мандат. Во одредени случаи и според условите и ограничувањата утврдени со закон, може да се утврди дека работодавачот не е обврзан да пренесе информации или да се консултира кога природата на тие информации или консултации е таква што според објективни критериуми сериозно би го нарушила или би го довела во прашање функционирањето на работодавачот.

На меѓународно ниво постојат механизми за заштита на деловната тајна при што се прави разлика помеѓу деловна тајна и доверлива информација. Во отсуство на национална нормативна дефиниција на поимот деловна тајна, би можеле да се послужиме со критериумите кои се содржани во член 39 од Договорот за трговските аспекти на правата од интелектуална сопственост на Светската трговска организација и тоа:

1) Информацијата да е тајна, односно да не е општо позната или да е достапна до кругови кои вообичаено се занимаваат со соодветниот вид на информации;

2) Информацијата да има комерцијална вредност и

3) Друштвото да преземало чекори за да ја здржи тајната со пропис или одлука.

Бизнис разузнавањето преку своите експоненти – приватните детективи имаат посебни надлежности во заштитата на деловната тајна, каде што влегуваат: бизнис планови, бизнис стратегии, маркетинг планови, клиенти итн. За да се определи заштита на деловната тајна потребно е најпрвин да се пропише со пропис кои документи, материјали или акти го имаат тоа својство. Затоа што не постои повреда на работниот ред и дисциплина со неовластено соопштување на деловна тајна, доколку претходно работодавачот во посебен акт не определил кои факти, исправи, податоци и документи се прогласени за деловна тајна.[259]

Натаму, во Кривичниот законик на Република Македонија е обезбедена заштита на деловната тајна – оддавањето и неовластеното прибавување на деловна тајна. Во член 281 од КЗ на РМ, е инкриминирано дека тој што на неповикано лице ќе му соопшти, ќе му предаде или на друг начин ќе му ги направи достапни податоците што со закон се прогласени за деловна тајна, како и тој што прибавува вакви податоци со намера да ги предаде на неповикано лице, ќе се казни со затвор од една до пет години. Тој што на неповикано лице ќе му ги соопшти, ќе му ги предаде или на друг начин ќе му ги направи достапни податоците што со пропис или со одлука на надлежен орган на управување се прогласени за деловна тајна, ако оддавањето на овие податоци предизвикало или можело да предизвика потешки штетни последици, како и тој што прибавува вакви податоци со намера да ги предаде на неповикано лице, ќе се казни со затвор од три месеци до три години. Ако податоците се од особена важност или ако оддавањето, односно

[259] Рев. 3 бр. 239/2014 од 14.10.2015.

прибавувањето на податоците е извршено заради нивно изнесување во странство, ќе се казни со затвор од една до десет години.

Заштита на деловната тајна има и меѓународна димензија, а изворите за тоа се наоѓаат во актите на Европската унија, како што е Директивата на ЕУ 2016/943 за заштита на неоткриени знаења и искуства и трговски информации (деловни тајни) од незаконско прибавување, користење и употреба од 08.јуни 2016 година.

Во Законот за детективска дејност посебно е определена надлежноста на приватните детективи да истражуваат дали работниците во една компанија ја заштитуваат деловната тајна односно да прибираат податоци за тоа каков е нивниот однос кон оваа прашање. Затоа ова прашање по својата природа влегува во поширокаата област на economic espionage, под што опфаќа "употреба на илегални, тајни, принудни или измамнички начини и методи да се дојде до одредени информации за деловните субјекти во приватниот сектор."[260] Во поглед на штетните последици кои корпорациите и националното стопанство ги имаат поради дејствувањето на индустриската/деловната шпијунажа, во стручната литература постојат различни мислења, првенствено поради спорот за тоа дали штетите од овој вид можно е да се согледаат во целина.[261]

4.Улогата на бизнис разузнавањето во остварувањето на заштита на податоци за успешноста и деловноста на правни лица

Бонитетот на правните лица отсекогаш претставувал предизвик и интерес за бизнис заедницата. Имено, срцевината на деловниот свет се засновува врз бројни договори, меморандуми кои ги склучуваат деловните субјекти, а на чие потпишување односно официјализирање му претстои проверка на податоците за деловниот партнер. Во оваа сфера деловната интелигенција има посебни надлежности кои се реализираат преку афинититети и способностите на приватните детективи во истражувањето на непосредната и поширокаата деловна околина, а сето тоа со цел да се олесни процесот на донесување на одлуки од страна на менаџментот. Тој процес се состои во следните клучни елементи:

- собирање на податоци и нивна анализа;

- согледување на ситуацијата и проценка на ризик;

- поддршка во донесувањето на одлуки.[262]

Изработката на безбедносната проценка за потребите на деловниот клиент е работа на менаџерот за корпоративна безбедност, кој исто така може да ги користи услугите на бизнис разузнавањето и тој процес најчесто опфаќа:

[260] Potter H. Evan, (ed.), Economic Intelligence and National Security, Carleton University Press & The Center for Trade Policy and Law, Ottawa, 1988, pp. 11-14.
[261] Trivan D., Detektivska delatnost, Beograd, 2014 godina, str. 135.
[262] Цветковски Г., цит. труд, стр. 261.

1) Проценка на можните извори (носители) на загрозување на безбедноста во корпорациите;
2) Проценка на можните облици (начини) на загрозување на безбедноста во корпорациите;
3) Проценка на можните места на загрозување на безбедноста во корпорациите и
4) Анализа на ризикот.[263]

Деловното работење на компаниите не е само прашање на желба за добивка, туку во исто време и прашање на финансии кои треба да ги вложат сопствениците во градење на деловна структура и клима која ќе биде насочена кон јакнење на интегритетот на вработените, нивниот етички однос на податоците и сознанијата поврзани со секојдневното работење, а кои понекогаш имаат и суптилна природа. Приватните детективи како сервис на корпоративната безбедност можат во многу да придонесат за унапредување на овие тековини во деловниот свет и тоа на неколку нивоа:

- Утврдување на ризици и закани за деловното работење;
- Изготвување елаборати за безбедносна проценка во тесна комуникација со топ-менаџерите на корпорациите, преку развивање сопствена методологија за изработка на модел во контекст со менталитетот и природата на корпорацијата;
- Анализа на актуелната состојба поврзана со безбедносните појави поврзани со деловното работење и опкружување;
- Развивање на безбедносни мерки односно заштитни активности. Така доколку се "неразвиени безбедносните заштитни мерки, во ситуација кај изворите на загрозување да постои позитивна проценка дка проблемите може да ја реализираат својата замисла, тогаш веројатно е дека ќе се случи загрозување на безбедноста на корпорацијата. Доколку после правилната безбедносна проценка мерките за обезбедување целосно се воспоставени, кај носителите на загрозување ќе се развие убедување дека не е можно да се спроведе замисленото, и ќе дојде до откажување од злонамерното дејствување."[264]
- Корпорациско предвидување на идните закани и нивните носители, со изготвување на анализа на ризиците, како завршна фаза од безбедносната проценка која во зависност од ранливоста на имотот и лицата и работењето на корпорациите и заканите, дава оценка за прифатливоста на ризикот, непосредно влијае на степенот и начинот на заштита и обезбедување на корпорациите.[265]

Заштитата на деловното работење на корпорациите е исто така една од стратешките цели на менаџментот е детерминирана и од квалитетното утврдување на нивоата на ризици кои ја загрозуваат безбедноста на работењето, проценка на нивната фрекфенција итн.

[263] Драгишић З., Безбедносни менаџмент, Службени гласник, Београд, 2007, стр.47-52.
[264] Мандић Г., *Систем обезбеђења и заштите,* Факултет цивилне одбране, Београд, 2004,стр.42
[265] United States Bureau of Diplomatic Security, Vital Installation Security Training Course, Philippines, 2002.

5.Улогата на планирањето во бизнис разузнавањето

Планирањето на бизнис разузнавањето е неопходно заради обезбедување на систематичност и деловен поредок во кој точно ќе се знае кои се целите кои треба да се постигнат, улогата на деловните субјекти во постигнувањето на овие цели, јакнењето на сигурноста во работењето итн. Во областа на корпоративната тероија, планирањето најчесто се дефинира како "мисловно-творечка активност која претходи на извршувањето на секоја задача од делокругот на безбедноста на корпорацијата, а опфаќа утврдување на целите и пронаоѓање најдобар начин за нивно остварување."[266] Планирањето:
А) обезбедува правец
Б) ја намалува несигурноста
В) трошоците се сведуваат на најмала мерка и
Г) се утврдуваат стандарди кои се применуваат во контролата.[267]
Планирањето во областа на бизнис разузнавањето е сложен процес фокусиран кон остварување на целите на стратешко, тактичко и оперативно ниво и затоа плановите може да се поделат на ист начин. Ако бизнис разузнавањето има за цел подигнување на нивото на безбедност во деловното работење тогаш, одделните планови се во функција на јакнење на безбедносните аспекти на бизниост, ресурсите, програмите. Имајќи ја во вид конспиративноста на овој облик на разузнавање планското работење претставува императив со детерминирачно значење за неговата ефикасност. Имено, неспорно е дека приватните детективи извршувајќи сериозна корпорациска дејност. Затоа тие мора да водат грижа пред се за тајноста на своето работење, што претставува иманентна карактеристика и на општиот облик на разузнавање каде има "значење на фундамент за разузнавачката дејност."[268]
На овој начин може да се нотира дека планирањето на бизнис разузнавањето треба да биде насочено кон идентификување на субјектите, моделите, просторната и временска димензија на актуелните безбедносни ризици и закани. Со тоа се остварува благовремена и правилна проценка и предвидување на идните закани, како и формулирање на стратешки документи кои се во функција на идно превентивно дејствување преку прибирање на податоци и информации од значење на бизнис разузнавањето.
ЗаклучокИстражувањето на одредени современи аспекти на бизнис разузнавањето само го потврдува неговото значење и вредност за современиот деловен свет. Кога станува збор за деловното разузнавање тогаш природно е да има синтеза помеѓу теоријата и практиката затоа што само на тој начин може да се обезбеди да се разбере суштината на еден многу витален сегмент од деловното работење.
Основите на бизнис разузнавањето мора да се засновуваат врз начелото на законитост затоа што во спротивност ќе се поткопа интегритетот на деловниот субјект во целина.
Ефикасното бизнис разузнавање има за цел зголемување на безбедноста во деловното работење. Затоа денес, во светот овој облик на разузнавање има

[266] Hunger i T.L.Wheelen, Strategic Management, 7, Upper Saddle River, NJ: PrenticeHall,2000.
[267] Стевановић О., Руковођење и командовање, Полицијска академија, Београд, 1999, стр.96.
[268] Masleša R., Obavještajne teorije, hrestomatija, Sarajevo, 2010 godina, str. 146.

приоритетно значење во функционирањето на врвниот менаџмент на една современа корпорација. По својата природа може да се заклучи дека бизнис разузнавањето ги има карактеристиките на општото разузнавање, а тоа се согледува во однос на тајноста на работењето, но се разликува од истото според својата корпорациска заснованост.

Во нашата држава многу малку е познат овој модел на разузнавање и токму поради тоа компаниите се препуштени сами да се борат со современите безбедносни ризици и закани, како што се сајбер криминалот, економските деликти, имотните деликти итн. "Свеста за корпоративна безбедност во Република Македонија Македонија сеуште не е на високо ниво, поради што компаниите трпат загуби. Меѓутоа, иако скромно, постепено голем број домашни компании ја согледуваат потребата од ангажирање на професионалци за корпоративна безбедност."[269]

Затоа е неопходно потребно во иднина да се вложат напори пред се за развивање на парадигмата за бизнис разузнавањето прилагодена на нашите услови, со консекветно почитување на странските искуства во оваа област, од една страна и развивање на свеста кај приватниот сектор за поголемо користење на услугите на бизнис разузнавањето. Дотолку повеќе што ваков "вид на услуги бараат често и странски фирми кои приватните детективи ги ангажираат по пат на деловна преписка преку Интернет, а финансиските средства по завршената истрага, уредно ја плаќаат на сметката на детективот."[270]

Литература

1.Цветковски Г., Професија приватен детектив, "Панили", Скопје, 2011 година.
2.Стојановиќ М., Павловиќ Д., Економска безбедност пословања, Београд, 2014 година.
3.Marković S., Osnovi korporativne i industrijske bezbednosti, USEE, Novi Sad, 2007 godina.
4.Katilić T., Uvod u zaštitu intelektualnog vlasništva u Republici Hrvatskoj, CARnet, Zagreb, 2006 godina.
5.Potter H. Evan, (ed.), Economic Intelligence and National Security, Carleton University Press & The Center for Trade Policy and Law, Ottawa, 1988.
6.Trivan D., Detektivska delatnost, Beograd, 2014 godina.
7.Драгишић З., Безбедносни менаџмент, Службени гласник, Београд, 2007.
8.United States Bureau of Diplomatic Security, Vital Installation Security Training Course, Philippines, 2002.
9.Hunger i T.L.Wheelen, Strategic Management, 7, Upper Saddle River, NJ: PrenticeHall, 2000.
10.Стевановић О., Руковођење и командовање, Полицијска академија, Београд, 1999 година.
11.Masleša R., Obavještajne teorije, hrestomatija, Sarajevo, 2010 godina.
Службен весник на РМ бр. 167/2015 година.
Рев. 3 бр. 239/2014 од 14.10.2015.

[269] Цветковски Г., оп. цит. стр. 260
[270] Ибид, стр. 260.

Јелена Ванева
Факултет за детективи и криминалистика
Европски Универзитет Република Македонија

Улогата на полицијата во откривање на имотните деликти (кражба, тешка кражба)

Апстракт
Имотниот криминалитет претставува посебен облик на криминалитет што се состои од кривични дела што се насочени против имотот и имотните права на граѓаните и правните лица. Извршителите на овој вид кривични дела настојуваат за себе или за друг да присвојат имотна корист, а со тоа и некому да предизвикаат материјална штета. Кривичните дела против имотот се појавиле уште од најстари времиња, односно со самата појава на сопственоста. Имотните деликти со посебен акцент на кражбите и тешките кражби се најчест облик на криминалитет во Република Македонија. Голема улога во откривањето и докажувањето на овие имотни деликти имаат и органите за внатрешни работи како основни органи за откривање на кривичните дела во склоп на нивната превентивна и репресивна активност со примена на соодветни мерки и активности со цел да се спречи и намали бројката на извршување. Заедничкиот интерес на МВР и приватното обезбедување во Македонија придонесуваат во одржувањето на приватната и државна сопственост и сузбивање на имотниот криминалитет.

Клучни зборови: имотни деликти, кражба, тешка кражба, полиција, приватно обезбедување

Abstract
Property crime is a special form of criminality consisting of crimes that are directed against property and property rights of citizens and legal entities. The perpetrators of this type of crime endeavor to assign a property benefit to themselves or to others, and with that to cause end material demage. Criminal acts against property have arisen since the earliest times, that is, with the very appearance of ownership. Real estate with special emphasis on the theft and heavy thefts are the most common form of criminality in the Republic of Macedonia. The organs of internal affairs as the main organs for detecting crimes in their preventive and repressive activity with the application of appropriate measures and activities in order to prevent and reduce the number of execution have a major role in the detection and proving of these property deeds. The joint interest of the Ministry of Interior and private security in Macedonia contribute to the maintenance of private and state property and the suppression of property crime.

Keywords: property delicts, theft, heavy theft, police, private security

Вовед

Безбедноста во заедницата станува актуелна тема на јавни, политички и научни дебати, кои сè повеќе ја актуализираат превенцијата на криминал како прашање на полицијата и на казненоправниот систем. Таа ги обединува владините агенции, практичарите, научните работници и граѓаните да работат заедно за да ги подобрат условите кои придонесуваат за безбедност во заедницата, бидејќи заканите за безбедноста се сè поприсутни во нашето опкружување. Ниедно општество, вклучително и македонското општество, не е отпорно на процесите на распаѓање и редефинирање на општествените вредности на заедништво, солидарност и кохезија на граѓаните и на заедниците. Наспроти тоа, големите градови станаа места за преживување и наместо безбедни места за живеење и движење станаа сиви, материјални светови во кои насилството и криминалот се присутни појави кои го стеснуваат безбедниот простор за движење и творење[271].

Имотниот криминал е феномен кој е стар колку и самата човечка цивилизација. Со појавата на вишок на вредности, кои се одразуваат во секој имот, од самиот почеток, го прилекувало вниманието на луѓето кои се склони кон девијантно однесување, кои се обидувале да присвојат имот за кој знаат дека не им припаѓа. Овој вид на криминал секогаш беше забранет во сите слоеви на општеството[272].

Обемот на имотниот криминал постојано се зголемува без оглед на ефектот на казнената политика врз сторителите. Така увидувајќи го ова во последно време многу криминолози и пенолози во прв план ги стават современите принципи на т.н принципи на ресторативна правда во борбата против имотниот криминалитет.

Целта на овој труд е да се потенцира значење и улогата на полицијата во откривањето на имотните деликти како што се кражбата и тешката кражба.

1. Историско-правна димензија на имотниот криминалитет

Историско набљудувано, во првобитната родовска и племенска зедница немало имотни криминалитети како негативна општествена појава во правна смисла. Постоеле само поединечни, издвоени случаи на кршење на општествените правила на животот и општествената дисциплина.[273] Меѓутоа и првобитните човечки колективи на таквите негативни појави различно реагирале. Таа реакција на членовите на првобитните човечки заедница зависела од тоа дали недозволивото однесување е извршено внатре во фамилијата, спрема некој нејзин член, или помеѓу членовите на различните семејства на една поширока општествена група. Оттука како реакција на недозволивото однесување на поединците или групата се разликуваат: прогонство од заедницата, освета или подмирување во вид на средства за надомест за причинета штета (композиција) како форма на приватна реакција

[271] Стефановска В., Гогов Б., Улогата на заедницата и на полицијата во превенција на криминалитетот:состојби во градот Скопје, Факултет за безбедност, Скопје, 2015, Стр. 4

[272] Богоевич Р., Основне криминолошке карактеристике и пенолошка обележја учинилаца имовинског криминалитета, Универзитет у Нишу, Ниш, 2016, стр.10

[273] Н. Срзентић, А. Стајић, Љ. Лазаревић, Кривично право СФРЈ, Општи део, Савремена администрација, Београд, 1994. године, стр.16.

на недозволиво однесување, или како почетоците на казнување во вид на „ултимативните форми на неодобрување од надворешната група[274]“.

Имотниот криминалитет се појавува како револт на одредени луѓе, или група на луѓе спрема одредени општествено-економски услови на живот. Како тие услови се менувале во текот на историјата, така се менувало и сфаќањето за имотниот криминалитет и односот спрема одредени негови облици. Меѓутоа без оглед на тоа што имотниот криминалитет со текот на врмето ги менувал своите облици и видови на појавување, тој никогаш не ја менувал својата суштина. Зголемувањето на обемот на овој вид на криминалитет доведувал до промена во санкционирањето на неговите причинители. Со настанокот на првите робовладетелски држави, почнува и период на јавно реагирање на појавата на имотниот криминалитет. Државата тогаш постепено почнала да врши трансформација на мерките на првобитната општествена реакција во кривично првниот систем на казната[275]

2. Полициски мерки и активности на сузбивање на имотниот криминалитет

Планирањето и преземањето на криминалистичко полициските мерки и активности на сузбивање на имотните кривични дела, претпоставува правовремено доаѓање до сознанија за припремање или извршување на делата. Меѓутоа за жал ретки се случаевите да се дознае за припремањето, бидејќи во последно време се потешко е да се обезбедат т.н „соработници и информатори“ од криминалната средина. Најчест начин на сознание за извршеното имотно кривично дело е пријавата од страна на оштетениот, по што веднаш се почнува со трагање по извршителот. Покрај ова познати се уште и начините на сознание на основа на информативните криминалистички дејности, сознанија за самите полициски службеници, пријава на инспекциските или некои државни служби, по пат на анонимна пријава на граѓаните, јавно преговарање од средствата за информирање и сл. Не е непознато во полициската и криминалистичката практика и затекнувањето на делото како начин на сознание за извршениот имотен деликт.
Благовремената добиена потполна информација за видот и локацијата на извршеното имотно кривично дело, овозможува брзо излегување на полициските службеници на местото на настаните и брзо преземање на одредени полициски мерки и активности.[276]
Стручно оспособениот и посветен на работата полицаец, може и во наизглед во безизлезните ситуации да ги воочи знаците на сомнителното однесување, кои укажуваат на спремност на лицата да направат имотен деликт, или околност да извршат деликт. Полицаецот кој со тоа е и добар познавач на приликите на одреден терен или во одредена средина може да го запази и

[274] R.R. Korn, L.W. McCorkle., Criminology and Penology, Holt, Rinehartand Winston, New York, 1959, p.359
[275] Д. Јовашевиќ, Кривично право, Општи део, Номос, Београд, 2010. године, стр. 25-27.
[276] М. Жарковиќ, Криминалистика, ВШУП Земун, Београд, 1999. године, стр. 2012

правилно да го протолкува отстапувањето на вообичаената состојба а притоа и на соодветен начин да реагира[277].
Меѓутоа ако немаме некои особени сознанија за извршеното имотно кривично дело, тогаш мораме да ги следиме утврдените принципи за работата како што се добро познатите индиции и правно релавантните факти.
До индиција најчесто се доаѓа со разговор, следење и останати оперативно тактички мерки, со увид на лице место, со преглед на телото и облеката на обвинетиот и со истражен експеримент, претрес на станот, слободниот простор и лицето, со вештачење, испитување на сведоци, испитување на обвинетиот итн[278]. Секако имајќи го во предвид движењето на извршителот на кривичното дело, посебно треба да се истакне прегледот и претресот на превозните средства[279].
Првичните доказни вредности на индицијата предизвикуваат спорови во процесната теорија и практика. Поради тоа иницијалниот доказ не е ништо друго туку еден вид на мозаик во кој секој составен дел претставува еден сегмент од вкупната слика а дури и сите заедно претставуваат мисловна целина.
Правно релевантните факти ги утврдува судот со примена на одредени истражни работи, и врз основа на нив се гради кривичната постапка.
Разјаснувањето на приватниот имотен деликт, ќе биде најуспешно ако полицијата е веднаш на местото на настанот. Кога неспоредно ќе се дојде на местото на настанот, тогаш исчезнуваат сите сомнежи и шпекулации за тоа што навистина се случило. Правилното обезбедување на местото на настанот[280] подразбира дека тоа мора да остане непроменето до доаѓањето на екипата за увид. Кога правилно ќе се обезбеди лицето на местото на настанот, тогаш се собираат потребните известувања, за најуспешно да дојдеме до одговорот: како е направено кривичното дело и кој е сторителот? Колку е пократка временската разлика од моментот на сознанието за имотно-кривичното дело до извршувањето на увидот, успехот е поверојатен, бидејќи се намалува можноста за уништување и оштетување на трагите, било од страна на оштетениот, било од страна на осомничениот, или од трети лица или во однос на атмосферските прилики.[281]
По доаѓањето на екипата за увид полициските службеници се запознаваат со мерките и активностите кои се преземале до нивното доаѓање. Целата на увидот е собирање на материјални докази, или индиција за фактите кои се однесуваат на извршеното имотно крвично дело, или одговорност за негово извршување, или тие факти да се разјаснат или да се утврдат трагите, или да се провери вистинитоста на другите докази.
Познатата криминалистичка поговорка кажува дека „човекот го запазува само она што живее во неговиот мисловен свет“. Сведувањето на сложената

[277] В. Кривокапић, М. Жарковић, Б. Симоновић, Криминалистичка тактика, ВШУП Земун, Београд, 2005. године, стр. 47
[278] В. Водинелић, Криминалистика, Савремена администрација, Београд, 1984. године, стр. 188
[279] Б. Симоновић,Криминалистика, Правни факултет у Крагујевцу, Институт за правне и друштвене науке, Крагујевац,2004. године, стр. 284.
[280] М. Бошковић, Б. Бановић, Криминалистика методика,ВШУП Земун, Београд, 2001 године, стр. 107
[281] А. Петровић, Криминалистичка методика, ВШУП, Београд, 1981. године,стр. 590

поврзаност само на генеричка врска значи типизирање и систематизирање, постапки на докажување[282].
За извршување на имотното кривично дело, посебно е важен увидот на местото на извршување на тоа дело, чии предмет може да бидат ствари, лица како и самото место.
Посебен вид на увид претставува реконструкцијата на настаните, која често се врши во врска со имотните кривични дела. Реконструкцијата на настаните се состои во проверување на изведените докази или утврдување на фактите кои се значајни за разјаснување на имотното кривично дело, повторување на одредени активности или ситуации во услови на приближно исти на оние во кои се извршиле и активностите на кривичното дело. Реконструкцијата на настаните не е доказно средство, туку само еден вид на проверка на веќе собраните докази.

3. Кражбата и тешката кражба според македонскиот законик

Кривичен Законик на РМ

Кражба Член 235

(1)Тој што од друг ќе одземе туѓ подвижен предмет со намера противправно да го присвои, ќе се казни со парична казна или со затвор до три години. (2)Ако вредноста на украдениот предмет е помала и сторителот одел кон тоа да присвои предмет од таква вредност, ќе се казни со парична казна или со затвор до една година. (3)Гонењето за делото од став 2 се презема по приватна тужба. (4)Обидот за делата од ставовите 1 и 2 е казнив. (5)Како кражба се смета и одземање од туѓа шума дрвја чие количество е поголемо од еден кубен метар со намера за противправно присвојување.

Тешка кражба Член 236

(1)Ако кражбата е сторена: 1)со кршење или провалување во затворени простории, со совладување препреки или на друг начин совладување поголеми пречки, 2)од страна на повеќе лица здружени заради вршење кражба, 3)на дрзок начин, 4)од страна на лице кое кај себе имало некакво оружје или опасно орудие заради напад или одбрана, 5)за време на пожар, поплава или слична несреќа иб)со искористување на немоќта или несреќата на друг, сторителот ќе се казни со затвор од една до десет години. (2)Со казната од став 1 ќе се казни сторителот на кражба на предмети од значителна вредност. (3)Ако украдениот предмет е: добро под привремена заштита или културно наследство, сторителот ќе се казни со затвор најмалку четири години. (4)Ако вредноста на украдениот предмет е мала и сторителот одел кон тоа да присвои предмет од таква вредност, ќе се казни со парична казна или со затвор до три години.
Кражба – според одредбите од македонскиот Кривичен законик, забележуваме дека се пропишува една основна и една привилегирана форма

[282] В.Водинелиќ, Криминалистика, Откривање и доказивање, први том, Факултет за безбедност и општествена заштита, Скопље, 1985. стр. 451.

на работа. Исто така, за основната форма на работа, се предвидува казна, односно парична казна или казна затвор до три години.
Македонскиот законик предвидува привилегирана форма на кривично дело кражба. За привилегираната форма на кражба во македонскиот законик, алтернатива е парична казна или казна затвор до една година.
Исто така во македонски законик, се наведува дека кражбата се смета за одземање, заради присвојување, на пример на повеќе од еден кубен метар на туѓи шумски дрва.
Тешка кражба - Во македонскиот законик, се пропишани два основни облика и една посериозна форма на кривично дело. Меѓутоа, во овој кривичен дел, Македонскиот Законик, предвидува и привилегирана форма.
За основните форми на делата во македонскиот законик е пропишана построга казна, т.е. од една до десет години затвор.
Понатаму, Македонскиот законик предвидува потешка форма на затворање од најмалку четири години, што исто така може да се смета за сериозна казна во споредба со некои други закони во регионот. Имено, ако се земе предвид дека не е пропишана посебна максимална казна за оваа сериозна форма на работа во македонскиот кодекс, пропишаната казна затвор значи апсолутен приоритет во однос на износот на казните што се наметнуваат во споредба со претходно споредената кривично законодавство.
Исто така, во Кривичниот законик на Република Македонија не се споменува организирана криминална група, а само во основната форма на работа се спомнуваат повеќе лица поврзани со кражба.
Така Македонскиот законик, во ова од кривичното дело, исто така, предвидува привилегирана форма за која е забрането казнување (со парична казна или затвор до три години), што се состои во фактот дека сторителот добил мало нешто и дека имал намера да ја примени таквата мала вредност.
Така кривично правните карактеристики на тешката кражба опфаќаат:

- Законско битие на делото
- Активниот субјект-извршителот
- Пасивниот субјект-жртвата
- Објектот на заштита
- Субјективната страна на делото
- Соучесништвото и соизвршителството
- Поттикнувањето и помагањето.

Така според член 236. Ст. 1 од Кривичниот законик на Р.М тешка кражба постои доколку кражбата е сторена:

- Со кршење ли провалување во затворени простории, со совладување препреки или на друг начин на поголеми пречки;
- од страна на повеќе лица здружени заради вршење кражба;
- на дрзок начин;
- -од страна на лице кое кај себе имало некакво оружје или опасно орудие
- заради напад или одбрана;
- - за време на пожар, поплава или слична несреќа;
- со искористување на немоќта или несреќата на друг, при што сторителот ќе се казни со казна затвор од една до десет години.

Поимот на тешката кражба се поклопува со општиот поим на кривичното дело кражба, со тоа што овде се работи за квалифициран облик со оглед на начинот на извршување, учество на повеќе лица во извршувањето, околностите под кои е извршена кражбата и објектот на дејствие. Дејствието на извршување може да се реализира на повеќе начини. За сите облици заедничка карактеристика е што со нивното преземање за одземање на предмет заради присвојување започнува дејствието на присвојување во рамки на тешката кражба. Ако делото остане во оваа фаза постои облик на кривичното дело кражба.

4. Улогата на приватното обезбедување

Овластените приватни обезбедувачи имаат должност да работат врз законот (начелото на легалитет) и притоа законот да го применува спрема сите граѓани на еднаков начин и пред законот да бидат рамноправни.
Денес неспорно е дека современите држави се исправени пред нови безбедносни предизвици кои бараат конципирање на заштитни системи и механизми кои ќе овозможат спречување и редуцирање на насилството односно загрозувањето на населението и неговите добра. Во таа смисла, императивно потребно е постојано да се прилагодува и доградува системот на безбедност кој е проектиран на начин што секогаш остава можност за неопходно перманентно иновирање, односно безбедносниот систем е многу еластичен на имплементацијата на нови потребни решенија.
Појавата на приватната безбедност во Република Македонија следува неколку години после стекнувањето на нејзината независност и отпочнување на патот кон Европската унија и НАТО-алијансата. Почетоци на приватната безбедност во Република Македонија се поврзуваат со донесување на Законот за обезбедување на лица и имот на 14 декември 1999 година.
Она што е значајно за приватното обезбедување е дека може да има голема улога во заштита од имотните деликти. Со постојаниот пораст на барањето на услугите од агенциите за приватно обезбедување се зголемува и сигурноста на граѓаните и на нивниот имот и се зголемува нивната заштита од имотни деликти. Така приватното обезбедување денес има се поголема улога во заштитата од имотните деликти. Воедно се овозможува надзор на одредени имоти како и поставување на лица за приватно оебзбедување со кои се зголемува сигурноста од имотните деликти и тешките кражби на многу објекти.

5. Учество на кражбите во вкупниот број на кривични дела против имот во Р.М во периодот од 2006-2016

Според Државниот завод за статистика може да се состави следната табела од осудени полнолетни лица за кривични дела против имотот.

Табела 1 Осудени полнолетни лица за кривични дела против имотот

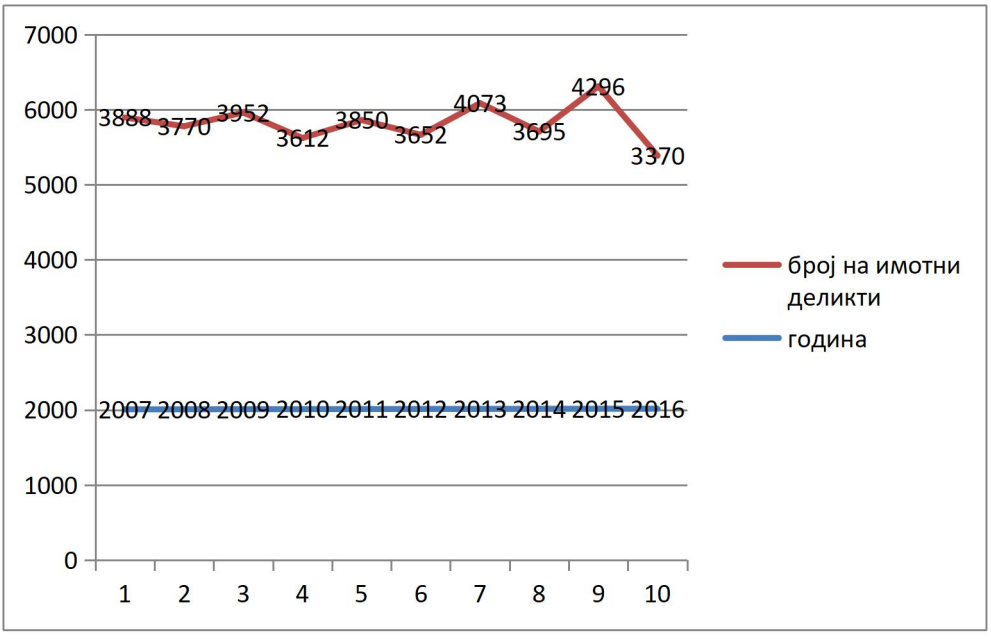
Осудени полнолетни лица за кривични дела против имотот									
2007	2008	2009	2010	2011	2012	2013	2014	2015	2016
3888	3770	3952	3612	3850	3652	4073	3965	4296	3370

Извор: ДЗС

Така во табелата 1 имаме податоци од 2007 до 2016 година за осудените полнолетни лица за кривичните дела против имотот каде спаѓаат и кражбите. Па така може да се забележи дека најмногу осудени полнолетни лица има во 2015 година, а најмалку во 2016 година, и нема некој голем процент на зголемување или намалување, пред се се слични со бројките на осудени полнолетни лица за кривични дела против имотот од 2007-2016 година.

Податоците можеме да ги прикажеме и графички на графикон 1.

Графикон 1 Број на осудени полнолетни лица за кривични дела против имотот



6. Превентивни мерки

Општо превенцијата во борбата против криминалот значи плански и организирани мерки со кои се настојува да се остранат или барем во нивното дејствување да се намалат причините за криминалитетот. Поправилно е да се каже дека превенцијата не е намалување на причините на криминалитетот туку избегнување, предупредување на настанување на некои штетни појави, а тоа може да се постигне со отстранување на самите причини или намалување на нивното дејствување[283].

Така полицијата е таа која има огромна улога во превенцијата на имотните деликти, како и со тешките кражби. Па од неопходно значење е информирањето на јавноста за штетноста на оваа појава, која може да ја зајакне свеста кај населението за заштита на нивниот имот и намалување на имотните деликти воопшто. Основните облици на превенција особено на домовите од провални кражби се однесуваат на конкретни мерки кои треба да се преземаат од страна на општеството, државата и државните институции, а како најосновни се следниве:

- да се иницираат трибини со граѓаните во урбаните заедници и да се зголеми едукацијата на истите,
- да се дистрибуираат фалери до сите урбани заедници од градот,
- да се зголеми осветлувањето од страна на локалната самоуправа во оние делови на градот каде истата е слабо осветлена,
- да се зголеми соседскиот соживот, а во текот на летото домот кога во истиот нема да биде никој да биде надгледуван од соседот или од некој близок роднина.
- да се постават тајмери кој ќе се палат во одредено време во ноќта и ќе остават впечаток дека во домот има некој;
- да се обрне внимание на заклучувањето на влезните врати, вратите од гаражата и прозорците особено во приземјето, истите да бидат адекватно заштитени итн...

Значи со соработка и заеднички активности со граѓаните за одреден временски период може да дојде до намалување на стапката на криминалот, да се зголеми безбедноста на граѓаните.

Заклучок

Од овој труд можеме да дојдеме до конкретни заклучоци дека кражбите и тешките кражби се реалност во нашата држава и пошироко. Но полицијата е тука која има голема улога во откривањето на овие кражби и нивно решавање како и во спречувањето на нивната појава. Нивниот придонес е огромен, но исто така може да се спомене и улогата на приватното обезбедување. Приватното обезбедување од ден на ден има се поголема улога бидејќи голем број на граѓани одлучуваат да ги заштитат своите имоти од тешки кражби преку одреден вид на приватно обезбедување. Тоа е во пораст последните години и продолжува да се развива во иднина.

---

[283] Арсова Е., Кривично-правни, криминолошки и криминалистички карактеристики на кривичното дело тешка кражба- со посебен осврт врз провалите на каси – УГД, Штип, 2017, Стр.92

Она штое значјано за тешките кражби и сите дела против имот на граѓаните е да се преземаат превентивни мерки кои ќе помогнат во намалување на овие деликти и кои ќе помогнат на неутрализирање на оваа појава. Така преку поголема едукација на граѓаните и преземање на повеќе заштитни мерки, тие би можеле да се заштитат од овие деликти кои значајно може да влијаат на нивниот имот и безбедност.

Литература

[1] R.R. Korn, L.W. McCorkle., Criminology and Penology, Holt, Rinehartand Winston, New York, 1959, p.359

[2] А. Петровић, Криминалистичка методика, ВШУП, Београд, 1981. године,стр. 590

[3] Арсова Е., Кривично-правни, криминолошки и криминалистички карактеристики на кривичното дело тешка кражба- со посебен осврт врз провалите на каси – УГД, Штип, 2017, Стр.92

[4] Б. Симоновић,Криминалистика, Правни факултет у Крагујевцу, Институт за правне и друштвене науке, Крагујевац,2004. године, стр. 284.

[5] Богоевич Р., Основне криминолошке карактеристике и пенолошка обележја учинилаца имовинског криминалитета, Универзитет у Нишу, Ниш, 2016, стр.10

[6] В. Водинелић, Криминалистика, Савремена администрација, Београд, 1984. године, стр. 188

[7] В. Кривокапић, М. Жарковић, Б. Симоновић, Криминалистичка тактика, ВШУП Земун, Београд, 2005. године, стр. 47

[8] В.Водинелић, Криминалистика, Откривање и доказивање, први том, Факултет за безбедност и општествена заштита, Скопље, 1985. стр. 451.

[9] Д. Јовашевић, Кривично право, Општи део, Номос, Београд, 2010. године, стр. 25-27.

[10] М. Бошковић, Б. Бановић, Криминалистика методика,ВШУП Земун, Београд, 2001 године, стр. 107

[11] М. Жарковић, Криминалистика, ВШУП Земун, Београд, 1999. године, стр. 2012

[12] Н. Срзентић, А. Стајић, Љ. Лазаревић, Кривично право СФРЈ, Општи део, Савремена администрација, Београд, 1994. године, стр.16.

[13] Стефановска В., Гогов Б., Улогата на заедницата и на полицијаво превенција на криминалитетот:состојби во градот Скопје, Факултет за безбедност, Скопје, 2015, Стр. 4

Slavica Markovska
European University Republic of Macedonia

Corporate security towards cooperative Intelligent Transport Systems and Services

Abstract
This paper aims to introduce the importance of the essence related to the corporate and contemporary security of Intelligent Transport Systems and Services.
This specifics and new tools for preventing, protecting and defending has become high level priority which is part of serious consideration by the systems.
In this particular issue, the emphasizing of Intelligent Transport Systems and Services are subject of researching and presentation of corporate security framework of functionality.

Having in mind the expanded mobility of free movement of goods, people and capital, the intelligent transport systems and services need highly professional level of secured and monitoring as well. The security is more than important.
The Modern vehicles equipped with driver assistance systems can “feel” (by sensors), “see” (by cameras) and – in future – “speak” (by communication systems).
The new technology of cooperative Intelligent Transport Systems and Services enables communication between vehicles and traffic infrastructure. It is based on the principle that cooperative parties, stations, i.e. in vehicles, exchange information among each other in terms of standardized message sets.
Services and applications being subject to competition between companies cover up-to-date traffic information, improved safety by avoiding accidents and reducing injury severity, increased efficiency by supporting a consistent traffic flow, foresighted driving and enhanced driving comfort.
The innovation of such a protected transport and services are based and strictly connected with a daily achievements, technical and informatics facilitation tools.
These movements produce expected impacts in order to facilitate the free movement as well as to implementing new and updated technology.
Additionally, all above mentioned segments depend of funding sources, human resources and capacities for such an implementation and protection.
The content of this abstract intends to promote the new and contemporary approach towards the high quality corporate protection. In reality, the cyber threat to these systems is very real. Nation states, cybercriminals, cyber-terrorists, malicious insiders, and even unscrupulous operators all have their motives, whether it’s making money, causing chaos and disruption.
So, the Corporate security protection is more than necessary.

Key words: Corporate security, services, technology, protection

Introduction
The Corporate security is contemporary protected system which has been designed and created to protect safety framework for the management, operation and functionality of the Intelligent Transport Systems and Services.

Intelligent Transport Systems (ITS) can be defined as holistic, control, information and communication upgrade to classical transport and traffic systems, which enables significant improvement in performance , traffic flows, efficiency of passenger and goods transportation:

- safety and security of transport,
- ensures more comfortable travelling for passengers,
- reduces pollution, etc.

ITS presents a crucial breakthrough by changing approaches and trends in transport and traffic research and technology aiming to solve escalating problems of congestions, pollution, transport efficiency, safety and security of passengers and goods..[284]

ITS replaced previously used concept for transport problem solving, which had already been exploited. Increasing transport related problems in all major cities, centers or airports, raise the need for new approaches and new solutions. Direct benefits from ITS deployment can be analyzed based on different sets of factors so called categories of ITS benefits. In literature ITS benefits are classified into the following categories:

- Safety,
- Flow efficiency,
- Productivity and cost reduction,
- Environment benefits.[285]

Beside the measurable benefits, many other advances can also be noticed, including new business opportunities, increase of employment; improvement of regional/urban/national technology status etc.

Among common users and stakeholders, the following groups can be recognized: end users, network operators, system owners (stakeholders), service providers, tour operators, local authorities, civil government, etc. There are many approaches to measuring influences and benefits of new projects related to ITS development and deployment.

Designing effective and usable ITS solution includes a possibility for estimating the ITS benefits using suitable methods, such as:

- Method for physical impact measurement
- Benefit analysis method
- Cost – effectiveness analysis (C/E)
- Benefit – cost analysis (B/C

An ITS Architecture is important for a number of reasons:

- it ensures an open market for services and equipment,
- it ensures consistency of information delivered to end-users;
- it encourages investment in ITS since compatibility is ensured;
- it ensures inter-operability between components,
- it permits an appropriate level of technology independence and allows new technologies to be incorporated easily;

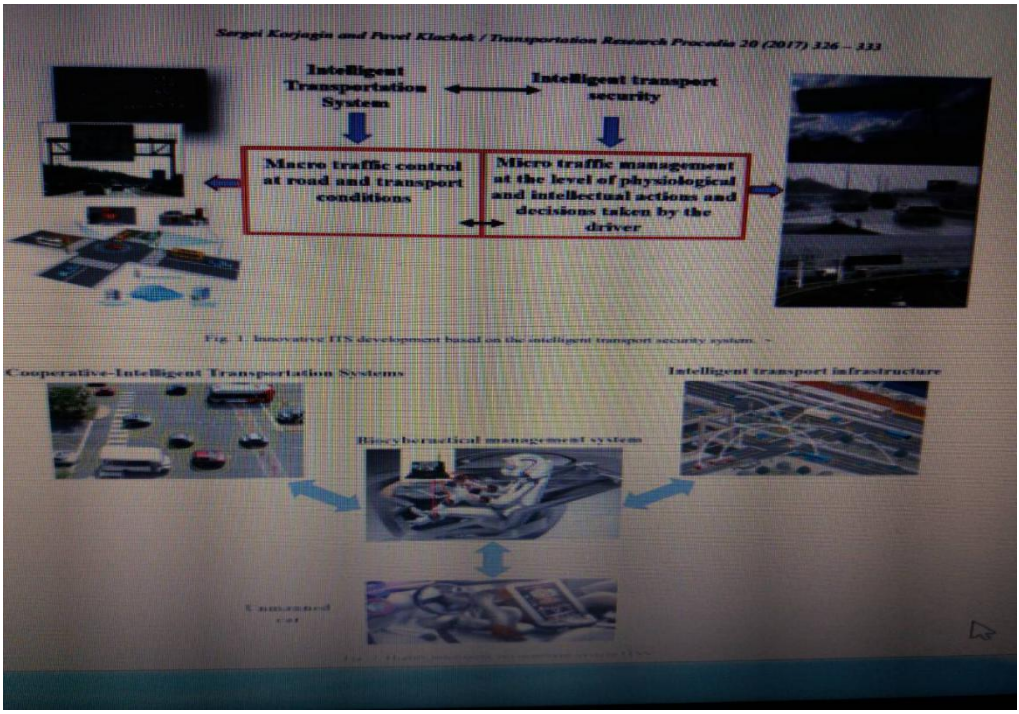
[284] Bošnjak, I., Intelligent Transportation Systems 1, Faculty of Transport and Traffic Sciences, Zagreb, 2006 (in Croatian)
[285] Intelligent Vehicle Highway Systems: The State of the Art, JHK and Associates, New York, NY, March 1993,

– it provides the basis for a common understanding of the purpose and functions of the ITS, thus avoiding conflicting assumptions.[286]

1. The new technology of Cooperative Intelligent Transport Systems

The Intelligent Transportation System[287] is intended for effective management of traffic streams, increase in traffic capacity of the street and road network, traffic jams prevention, reduction of delays in traffic flow, improvement of traffic safety, informing the road users about the emerging road and transport situation and options of the optimal traffic route, ensuring uninterrupted flow of the land urban passenger transport.[288]

Figure 1 Cooperative Intelligent Transport Systems



1.1. Additional requirements on deployment -Governance and regulation

Within the framework of the requirements on deployment the issue of Governance and regulation, the regulatory prerequisites for the innovation is more than important to be introduced. [289]

[286] Škorput, P., Real-time incident management system, M.Sc. Thesis, Faculty of Transport and Traffic Sciences, Zagreb, 2009 (in Croatian)

[289] https://eu-smartcities.eu/sites/default/files/2017-10

Especially strategies, architectures, services and processes related to road authorities, road operators, cities and automotive industry need to be commonly developed, tested and standardized European-wide for visualising the benefits towards sustainable mobility enabled by cooperative ITS.
Deployment of cooperative ITS in Europe needs to build-up on standards and profiles commonly agreed by all (investing) stakeholders.
The legal framework should be harmonised where necessary for enabling minimum performance and quality as well as transparent responsibilities and liabilities cross border and seamless in all road networks.

Stakeholders to involve
In practice the different stakeholder that need to be mobilised to successfully introduce the technology in the urban area, such as households, specific professional bodies, corporations, specific authorities (transport authority), etc,
The main goal is to identifies the different stakeholder that need to be mobilized to successfully introduce the technology in the urban area, such as households, specific professional bodies, corporations, specific authorities (transport authority), etc,

1.2. Expectations

The innovative approach is capable of transforming the existing transportation system radically having turned it into a highly intelligent environment. It means that it will not only bring mortality and injury rate on roads to nothing but will also:
- increase social mobility,
- improve environmental situation;
- give impulse to development of new services in different fields.

Moreover, the application solutions can become harmonious ITS development not only in the field of ensuring traffic safety but also become a basis for development of the unified environment for solution of the problems of transport infrastructure management ensuring essential improvement of characteristics of the traffic management in the urbanized territory.
Application of such systems will enable to raise the traffic management level:
- to improve characteristics of the street and road network,
- to improve location of the traffic management facilities,
- to optimize the process of traffic control on all traffic phases reducing transport delays, improving traffic safety.

2. Competition- Services and applications (up-to-date traffic information)

Information technology is revolutionizing products. Once composed solely of mechanical and electrical parts, products have become complex systems that combine hardware, sensors, data storage, microprocessors, software, and connectivity in myriad ways.
These “smart, connected products”-made possible by vast improvements in processing power and device miniaturization and by the network benefits of ubiquitous wireless connectivity have unleashed a new era of competition.

Smart, connected products offer exponentially expanding opportunities for new functionality, far greater reliability, much higher product utilization, and capabilities that cut across and transcend traditional product boundaries.
The changing nature of products is also disrupting value chains, forcing companies to rethink and retool nearly everything they do internally.
These new types of products alter industry structure and the nature of competition, exposing companies to new competitive opportunities and threats. They are reshaping industry boundaries and creating entirely new industries. In many companies, smart, connected products will force the fundamental question, "*What business am I in?"*
Smart, connected products raise a new set of strategic choices related to how value is created and captured, how the prodigious amount of new (and sensitive) data they generate is utilized and managed, how relationships with traditional business partners such as channels are redefined, and what role companies should play as industry boundaries are expanded.
The phrase "*internet of things*" has arisen to reflect the growing number of smart, connected products and highlight the new opportunities they can represent. Yet this phrase is not very helpful in understanding the phenomenon or its implications.
The internet, whether involving people or things, is simply a mechanism for transmitting information. What makes smart, connected products fundamentally different is not the internet, but the changing nature of the "things." It is the expanded capabilities of smart, connected products and the data they generate that are ushering in a new era of competition.
Companies must look beyond the technologies themselves to the competitive transformation taking place. [290]

2.1. The Third Wave of IT-Driven Competition

Twice before over the past 50 years, information technology radically reshaped competition and strategy; we now stand at the brink of a third transformation. Before the advent of modern information technology, products were mechanical and activities in the value chain were performed using manual, paper processes and verbal communication.
The first wave of IT, during the 1960s and 1970s, automated individual activities in the value chain, from order processing and bill paying to computer-aided design and manufacturing resource planning. .
The productivity of activities dramatically increased, in part because huge amounts of new data could be captured and analyzed in each activity. This led to the standardization of processes across companies And raised a dilemma for companies about how to capture IT's operational benefits while maintaining distinctive strategies.
IT is becoming an integral part of the product itself. Embedded sensors, processors, software, and connectivity in products (in effect, computers are being put inside products), coupled with a product cloud in which product data is stored and

[290] James E. Heppelmann Michael E. Porter,**How Smart, Connected Products Are Transforming Competition,** NOVEMBER 2014 ISSUE

analyzed and some applications are run, are driving dramatic improvements in product functionality and performance. Massive amounts of new product-usage data enable many of those improvements.
Another leap in productivity in the economy will be unleashed by these new and better products. In addition, producing them will reshape the value chain yet again, by changing product design, marketing, manufacturing, and after-sale service and by creating the need for new activities such as product data analytics and security. This will drive yet another wave of value-chain-based productivity improvement. The third wave of IT-driven transformation thus has the potential to be the biggest yet, triggering even more innovation, productivity gains, and economic growth than the previous two.

3. Key to innovation

Smart Cities Stakeholder Platform Cooperative Intelligent Transport Systems and Services
The Modern vehicles equipped with driver assistance systems can "feel" (by sensors), "*see"* (by cameras) and in future "*speak"* (by communication systems). The new technology of cooperative Intelligent Transport Systems and Services (C-ITS) enables communication between vehicles and traffic infrastructure. It is based on the principle that cooperative parties (ITS stations, i.e. in vehicles, road side units) exchange information among each other in terms of standardised message sets.
The receiving ITS station analyses the incoming data and makes use of them, resulting in a selforganisation principle on local level. Services and applications being subject to competition between companies cover up-to-date traffic information, improved road safety by avoiding accidents and reducing injury severity, increased efficiency by supporting a consistent traffic flow, foresighted driving and enhanced driving comfort.
By involving public transport, bicyclists and pedestrians, intermodal and environmental capabilities, autonomous driving and further functions will be addressed in a second step when C-ITS has reached a sufficient market penetration.[291]
At European level required to promote the adoption of key innovations, such as the removal of regulatory barriers or recommendations on the focus of the Horizon 2020.
It is important to stress that this document is not a set of technical proposals or a full evaluation of the innovation, but aims to assist the cities to identify potential solutions and understand their context and implementation needs. It does not exempt or substitute a detailed cost/benefit analysis and implementation plans for cities that wish to introduce the innovation.
The Stakeholder Platform cannot take any responsibility for inaccuracies or missing information or specific problems in the implementation of the proposed Key Innovations or other Solution Proposals. [292]

[291] Key to Innovation Integrated Solution Cooperative Intelligent Transport Systems and Services (C-ITS) Karl-Oskar Proskawetz (ITS /D) Stefan Klug, Bernd Beckert (Fraunhofer ISI/D) December 2013 2.0
[292] This includes a description of the main EU support instruments, such as the Risk Sharing Financing Facility,Solution proposals are published on the web site: www.eu-smartcities.eu/ solutionproposals

Description of a Key Innovation
A key objective of the Smart Cities Stakeholder Platform is to identify Key Innovations (KIs) for the development of Smart Cities. The selection of an SP as KI is based on the following criteria:
- applicability,
- simplicity,
- affordability,
- usability,

The extent to which it addresses technology integration and if the potential impact is significant.
Selected SPs will then be enhanced based on the following aspects:
- Premises for the technology development and up-take
- (e.g. problems, what the technology is intended to achieve, other unforeseen benefits for the smart cities); ν Potential integration with other technologies and sectors, including use of ICT;
- If necessary, enhancing the information from the SP on the urban environment in which the technology can be applied;
- Key pre-requisites for the applicability of the key innovation, such as the required enabling environment;

Instruments and market conditions needed to reach commercial viability.
The innovation of such a protected transport and services are based and strictly connected with a daily achievements, technical and informatics facilitation tools

4. Mobility of transport

Intelligent Transport Systems (ITS) are vital to increase safety and tackle Europe's growing emission and congestion problems. They can make transport safer, more efficient and more sustainable by applying various information and communication technologies to all modes of passenger and freight transport.
Moreover, the integration of existing technologies can create new services. ITS are key to support jobs and growth in the transport sector. But in order to be effective, the roll-out of ITS needs to be coherent and properly coordinated across the EU.
The European Commission is working with Member States, industry and public authorities to find common solutions to the various bottlenecks for deployment. Through financial instruments the European Commission supports innovative projects in ITS and through legislative instruments it ensures that ITS are rolled out consistently.
In the coming years, the digitalisation of transport in general and ITS in particular are expected to take a leap forwards.
As part of the Digital Single Market Strategy, the European Commission aims to make more use of ITS solutions to achieve a more efficient management of the transport network for passengers and business. ITS will be used to improve journeys and operations on specific and combined modes of transport. The European Commission also works to set the ground for the next generation of ITS

solutions, through the deployment of Cooperative-ITS, paving the way for automation in the transport sector. Following an invitation of the European Commission, industry representatives and public authorities have today agreed on a further developed shared vision on the interoperable deployment of Cooperative Intelligent Transport Systems (C-ITS) towards cooperative, connected and automated mobility (CCAM) in the EU.[293]

5. Funding Models and Funding Schemes

The classification of terms has been developed structure in order to enable structured analysis as well as Funding framework: the institutional, legal, organisational and budgetary framework within which the funding scheme operates

- **Funding model**: (generic) funding from a given funding provider (national, regional, local, operator, commercial etc) with a given funding method (grant, subsidy, competition, reinvestment of revenue, sponsorship or other financial tool / incentive).
- **Funding scheme**: (specific) a funding programme for specific purposes and policy goals, using a selected funding method, involving one or more funding agencies or partners as the funding provider (single agency, multi-partner, composite arrangements, Joint Venture)
- **Funding conditions:** the funding provider may impose qualifying criteria, such as specific eligibility criteria, a satisfactory business case (e.g. a cost-benefit analysis), conformance to national standards or to a system architecture
- **Funding source**: the funding provider will draw on one or more sources of funding for the funding scheme, for example through taxation, borrowing, income or revenue. Some of the funding sources that are available are listed below but are not explored further:[294]

6. EU Legislation

The EU's new approach to funding peace and security. The link between security, peace and development is recognized by both security and development communities. However, the practical implications of this nexus still pose challenges – especially in the light of a rapidly evolving security environment.
While the EU's assistance for peace and security comes in different forms for instance through budgetary support or under common security and defense policy-the existing rules of financing under the EU budget exclude activities aimed at enhancing cooperation with the defense sector and the military in third countries.
Regulation (EU) No 230/2014
Regulation 230/2014 of 11 March 2014 establishing an instrument contributing to stability, responding to crises or emerging crises to prevent conflicts. [295]

---

[293] Intelligent Transport: sector issues further guidance towards cooperative, connected and automated mobility in the EU https://ec.europa.eu/transport/themes/its/news/2017-09-22-intelligent-transport-sector-issues-further-guidance-towards-cooperative_en2/09/2017

[294] FUNDING Final Report, TREN/G4/FV-2008/475/02 Study regarding guidelines for public funding of Intelligent Transport Systems, Final Report Issue 03 Date 25 May 2011

[295] Briefing EU Legislation in Progress , http://www.europarl.europa.eu

7. Intelligent transport systems achievements

In many respects today's vehicles are already connected devices. However, in the very near future they will also interact directly with each other and with the road infrastructure.
This interaction is the domain of Cooperative Intelligent Transport Systems (C-ITS), which will allow road users and traffic managers to share information and use it to coordinate their actions.
This cooperative element enabled by digital connectivity between vehicles and between vehicles and transport infrastructure is expected to significantly improve road safety, traffic efficiency and comfort of driving, by helping the driver to take the right decisions and adapt to the traffic situation.
Communication between vehicles, infrastructure and other road users is also crucial to increase the safety of future automated vehicles and their full integration in the overall transport system. Cooperation, connectivity, and automation are not only complementary technologies; they reinforce each other and will over time merge completely.[296]
Therefore, the European Commission has on 30th of November 2016 adopted a European Strategy on Cooperative Intelligent Transport Systems (C-ITS), a milestone initiative towards cooperative, connected and automated mobility. It also involves continuous coordination, in a learning-by-doing approach, with the C-ROADS platform, which gathers real-life deployment activities in Member States.

- COM (2016) 766 - A European strategy on Cooperative Intelligent Transport Systems, a milestone towards cooperative, connected and automated mobility
- Press release: "Commission presents a Strategy towards cooperative, connected and automated mobility"
- Memo: "An EU strategy on cooperative, connected and automated mobility"
- Opinion of the European Economic and Social Committee.

Figure 1 Intelligent transport systems achievements

[296] Cooperative, connected and automated mobility (C-ITS) https://ec.europa.eu/transport/themes/its/c-its_en

Benefits of ITS technology
Intelligent transport systems have the potential to provide key benefits for businesses and road users.

- **Safety.**

ITS can be used to divert traffic and alert emergency services the moment an incident occurs.

- **Efficiency**

Travel time and point of arrival become more reliable through the monitoring of real-time data.

- **Reduced costs.**

Smoother, predictable traffic flow brings considerable cost benefits to both individual drivers and transport and supply industries through improved fuel consumption, reduced vehicle wear, less time spent in transit and more reliable delivery.

- **Productivity.**

Traffic congestion causes flow-on delays in supply chains and increases the cost of business. ITS can increase productivity through improving the capacity of current infrastructure, as well as through monitoring of vehicular performance and driver fatigue. When supported by ITS, trucks should be less likely to break down, and drivers less likely to have fatigue-induced accidents.

- **Environmental performance.** Less congestion and stop-start driving will result in a reduction in fuel consumption and greenhouse gas emissions compared with 'normal' driving conditions.[297]

The objective of the Intelligent Transport Systems is to facilitate the convergence of investments and regulatory frameworks across the EU, in order to see deployment of mature C-ITS services in 2019 and beyond.
This includes the adoption of the appropriate legal framework at EU level by 2018 to ensure legal certainty for public and private investors, the availability of EU funding for projects, the continuation of the C-ITS Platform process as well as international cooperation with other main regions of the world on all aspects related to cooperative, connected and automated vehicles.

8. Future of Intelligent Transport Systems

Corporate Intelligent transport systems (ITS) help to improve safety and enhance the efficiency and sustainability of transportation networks.
Intelligent transport systems (ITS) take that vehicular technology a little further, combining it with rapidly expanding internet of technology to benefit all users and modes of transport, regardless of their level of sophistication. [298] When applied to transport and infrastructure, these technologies create a smooth flow of information between systems for improved safety, productivity and environmental performance.

[297] Global Heavy Vehicle Leaders Summit, May 2016
[298] Viva Energy, 2016://www.vivaenergy.com.au/driven/innovation/the-future-is-intelligent-transport

ITS also includes the more specific 'cooperative intelligent transport systems' (C-ITS) applications.
Cooperative ITS technology enables real-time communication between individual vehicles, or between vehicles and roadside infrastructure. For instance, C-ITS can warn a driver that a collision has just happened or is imminent, and even alert the driver to a vehicle which is braking hard but may be out of sight.

9. Expectations

The further expectations are focusing more to the possibilities of achieving maximally effective and efficient corporative development, implementation and protection of the real-time traffic incident management system. It emphasizes the special significance on the timely incident detection.
The efficient management of available information, data exchange as well as intelligent real-time decision-making can reduce the consequences of traffic incidents, especially, prevents secondary incidents. Advanced inventive technologies and the approach based on the intelligent transport system paradigm, significantly improve the system performances.
The main performance characteristics taken into consideration are response time and reduction of harmful consequences from incidents.
The future work should study the possibilities of different realisations of the algorithm for traffic flow variables estimation. Therefore, a promising approach is based on the implementation of neuro-fuzzy estimators, which may include also the incident detection algorithms. Such systems will lead in the future to technologies based on the today already proven approach to the decision support system i.e. expert systems.
Special effort should be directed also to the study of the possibility of predicting the incident. Some past researches have shown that in some situations an incident can be predicted (forecast) with fairly sufficient probability. In that case, the final results referring to the Corporative security as well as prevention of the incident itself can be of great significance.

Cyber threat

Nation states, cybercriminals, cyber-terrorists, malicious insiders, and even unscrupulous operators all have their motives, whether it's making money, causing chaos and disruption.
Corporate security protection
The world of mobility is undergoing nothing less than a technological revolution. Such technologies pose significant issues, most notably cyber security.
Hacking of connected vehicles and traffic signals regularly hits the headlines and news. How this issue will evolve, and how the automotive, public transport, maritime, aviation, and other sectors of mobility react will be critical.
The Intelligent Mobility will be a whole new Cyber security proposition. The future isn't just an extension of the current issues. As demands for integrating technology into mobility become insatiable, Intelligent Mobility will be a whole different proposition to securing current transport systems. It is one that we need to understand quickly if we are to remain safe.

This proposition is characterised by the following elements:

Deep levels of integration across all mobility sectors and new forms of mobility. .

- Decentralised control of customer and operational choices.
- Autonomy as standard, but with humans.
- New business models and services emerging.

Mobility companies, governments, academics, cyber security practitioners and people using our mobility systems every day face new challenges. The current research indicated that even securing existing systems whilst maintaining levels of services is a huge challenge.

Intelligent Mobility brings more challenges, not just related to technology. New Corporative security governance structures crossing mobility sectors will need to be in place, sharing intelligence and solutions between traditionally conservative sectors. [299]

References

- Bošnjak, I.*, Intelligent Transportation Systems 1*, Faculty of Transport and Traffic Sciences, Zagreb, 2006,
- Prof. Sadko Mandžuka*, Intelligent Transport Systems*, Department Faculty of Transport and Traffic Sciences University of Zagreb, Zagreb, 2015.
- Sergei Korjagin, and Pavel Klachek, 12th International Conference "*Organization and Traffic Safety Management in large cities",* Innovative Development of Intelligent Transport Systems Based on Biocybernetical Vehicle Control Systems, 28-30 September 2016, St. Petersburg, Russia,
- James E. Heppelmann Michael E. Porter, *How Smart, Connected Products Are Transforming Competition,* NOVEMBER 2014 ISSUE
- Key to Innovation Integrated Solution Cooperative Intelligent Transport Systems and Services (C-ITS) Karl-Oskar Proskawetz (ITS /D) Stefan Klug, Bernd Beckert (Fraunhofer ISI/D) December 2013 2.0,
- www.eu-smartcities.eu/ solutionproposals
- FUNDING Final Report, TREN/G4/FV-2008/475/02 Study regarding guidelines for public funding of Intelligent Transport Systems, Final Report Issue 03 Date 25 May 2011,
- James Gleave, a Foresight Analyst at Transport Systems Catapult and owner of consultancy Transport Futures, discusses cyber security in intelligent mobility and provides steps on staying secure. https://www.intelligenttransport.com/transport,
- Viva Energy, 2016://www.vivaenergy.com.au/driven/innovation/the-future-is-intelligent-transport,

[299] James Gleave, a Foresight Analyst at Transport Systems Catapult and owner of consultancy Transport Futures, discusses cyber security in intelligent mobility and provides steps on staying secure. https://www.intelligenttransport.com/transport

Костовски Кристиан
Факултет за детективи и криминалистика – ЕУРМ
email: kostovski.kristian@gmail.com

Работните организации и информатичката безбедност

Апстракт
Хакерите постојано бараат начини за упад во компјутерските мрежи. Некои тоа го прават тоа за чиста возбуда од надмудрување на безбедносните системи во компаниите, додека други се платени да пробиваат во компјутерски мрежи со цел за пристап до важни податоци. Хакерството познава многу форми, од пробивање на лозинка и тројански вируси, до психолошка манипулација со таргетот и компромитирање на мрежниот администратор. Иако целосната заштита на сопствениот систем од искусните хакерски тимови претставува предизвик, спроведувањето на безбедносните мерки може значително да ја намали можноста за хакирање на системот.

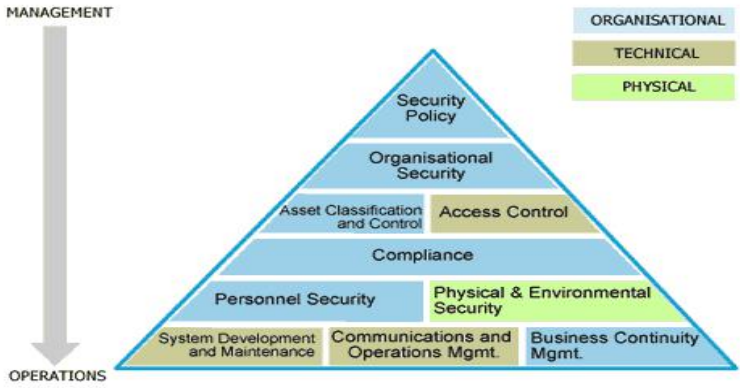
Клучни зборови: Компјутерски мрежи, Лозинка, Криптирање, Манипулација.

Бизнисите се подложни на многу видови закани – измами, кражби, хакерски напади, па дури и терористички дејствија. Обврска и одговорност на сопственикот на едно претпријатие е да инвестира во соодветни безбедносни системи за заштита на персоналот, инвентарот, финансиските инструменти и документацијата. Потребно е да се проценат потенцијалните закани на кои е изложен бизнисот, со цел да се воспостават правилни процедури за справување со заканите. Развивањето на безбедносниот план ќе зависи од видот на бизнисот.

Со континуираниот раст на хакерските напади врз податоците и останатите закани по мрежната безбедност, трошоците за информатичката безбедност минатата година достигнаа 90 милијарди американски долари.

Повеќето компании почнуваат да се подготвуваат за безбедносните прашања откако веќе е предоцна. Денешните хакери се попаметни и поинформирани од кога било. Работодавците треба да спречат проблеми многу поголеми од вирусите, малверите и рансомверите: тие мораат да бидат свесни и за надворешните закани, и за внатрешните проблеми. Со оглед на овие факти, денеска информатичката безбедност преставува еден вид на култура кон која треба сериозно да пристапиме.

Слика 1: Безбедносен менаџмент



Со оглед на тоа што безбедноста денес претставува прашање од најголем интерес за извршните одбори кои внимаваат на влијанието на безбедноста врз бизнисот, лица одговорни за безбедност на информациите (Chief information security officer) сега имаат место меѓу оние кои ги донесуваат одлуките. Ова е добрата вест за лицата одговорни за информатичката безбедност кои сакаат да придонесат и да ја поддржат заедничката стратегија. Лошата вест за нив е дека, додека дискусијата за безбедноста станува сè постратешка за бизнисот, довербата во нивната способност за идентификување и спречување на заканите е многу мала.
Компјутерите на кои работат вработените се составен дел од работната организација. Ако нешто тргне наопаку со тие компјутери или пак со мрежата, додека ИТ тимот или трети лица испитуваат и го решаваат проблемот, ние ќе се соочиме со потенцијални загуби во продуктивноста. Превенцијата е клучна кога станува збор за компјутерска безбедност, а постојат неколку едноставни работи кои можат да се направат за заштита на компјутерските системи од натрапници и случајни инфекции:

Софтверска заштита
Кога станува збор за компјутерска безбедност, добрите анти-вирусни софтвери се првата линија на одбрана. Секој компјутер во мрежата треба да биде опремен со антивирус, антиспајвер и фајервол софтвер. Заштитата на компјутерот со антималвер софтвер нема да ги спречи сите инфекции, но ќе ги спречи повеќето од нив. Треба да се обезбеди ажурирање на антивирус и антиспајвер софтверот и редовно да се врши скенирање на компјутерите.

Постојани ажурирања
Секој компјутер има оперативен систем, а секој оперативен систем има безбедносни дупки. Како што се откриваат овие безбедносни дупки, компанијата која е одговорна за оперативниот систем објавува ажурирања за нивно популнување. Без разлика дали се користи Linux, Windows или OS X, од суштинска важност е оперативниот систем на секој компјутер да се одржува во

чекор со најновите решенија за хардверските или софтверски грешки и безбедносните дупки. Ажурирањето на оперативниот систем треба да се направи веднаш штом новите ажурирања станат достапни.

Редовни резервни копии
Ниту еден безбедносен систем не е сигурен. Дури и со најдобрите практики за заштита и персонал кој е добро упатен во веб безбедноста, компјутерите на работната организација би можеле да завршат со некаква инфекција. Затоа треба да се има копија на сите важни информации во мрежата и да се постави распоред за редовно копирање. Треба да се запомни дека резервната копија е корисна само кога истата секогаш се ажурира со менувањето на информациите. Резервна копија од податоците треба да се прави најмалку еднаш месечно, со цел за ограничување на загубите во случај на инфекција.

Ограничување на системот
Ова може да се нарече и заклучување или безбедносно засилување и вклучува активности како конфигурирање на софтверот за оптимална употреба, деактивирање на непотребен софтвер кој може биде основа за некои едноставни напади, и конфигурирање на оперативниот систем за оптимална безбедност. Обично процесот на ограничување на системот се изведува во фазен пристап за повторливо зголемување на бројот на одбранбени слоеви и намалување на изложените површини за напад.

Управување со плаќања
За обезбедување на најдоверливи и најпотврдени инструменти и услуги против измами со пари, најдобро е да се работи со банките и компаниите кои управуваат со платежните картички. Согласно договорите со банките или компаниите кои управуваат со платежните картички, работната организација може да има одредени обврски во однос на безбедноста, па истата треба да биоде сигурна дека ги знаете своите должности. Системите за плаќања треба да бидат изолирани од останатите, помалку безбедни програми, а за обработка на плаќањата и за сурфање на интернет не треба да се користи ист компјутер.

Едукација на вработенитеМногу безбедносни пробивања или компјутерски инфекции не се резултат на недостаток на софтверот, туку на недоволните безбедносни постапки од страна корисниците. Вработените треба да се едуцираат за навики за безбедно прелистување на интернет за да им се помогне за донесување на правилни одлуки при користењето на опремата на компанијата. Вработените треба да бидат запознаени со фишинг измамите, опасните прилози на електронската пошта и неограничените веб-страници, и, при користење на уредите на работната организација, треба да бидат ограничени на користење на мрежата само за потребите на работата или одобрено користење на истата.

Кориснички сметки
Заканите по сајбер-безбедноста на компанијата не се само од далечина – исто така можни се и физичките нарушувања на безбедноста. На секој вработен треба да му се даде посебна корисничка сметка и лозинка, така што само овластените лица ќе можат да пристапат до системите. Корисничките сметки, исто така, даваат можност за одредување на одобренијата за секој корисник, што, пак, овозможува подетална контрола на она што вработените можат, односно не можат, да го прават при користење на нивните компјутери. Од сите вработени треба да се бара, пред напуштање на своите работни места, да ги заклучат или да се одјават од своите системи.

- **Употреба на лозинки**

Вообичаени, какви што се, лозинките остануваат еден од најефикасните начини за спречување на хакирањето. Секоја компанија треба да започне со спроведување на сериозна поликтика за употреба на лозинки. Лозинките, обично, треба да бидат составени од минимум осум безбедни знаци – комбинација од алфанумерички знаци и големи и мали букви. Како мерка на безбедност, лозинките треба да се менуваат неколку пати во една година. Копија од сите лозинки треба да се чува на друго безбедно место, како што е сефот на компанијата, во случај администраторот да е недостапен или неспособен за работа.

- **Креирање на акционен план за мобилни уреди**

Мобилните уреди создаваат големи безбедносни и менаџерски предизвици, особено ако содржат доверливи информации или можат да пристапат до деловната мрежа. Од корисниците на истата треба да се побара да ги заштитат своите уреди со лозинки, да ги шифрираат своите податоци и да инсталираат безбедносни апликации, за да се спречи криминалците да крадат информации додека телефонот е поврзан на јавни мрежи. Треба да се воспостават и процедури за известување за изгубена или украдена опрема.

Управување со компјутерски мрежи
Повеќето хакери ги искористуваат дупките во мрежата на компанијата. Дури и со добра технологија, лошо управуваната компјутерска мрежа сè уште ќе биде ранлива за нападите. Компаниите треба да воспостават оддели за безбедност на информациите кои ќе ги надгледуваат сите активности поврзани со обезбедувањето на мрежите и податоците на компаниите. Ваквиот оддел треба да биде вклучен во сите активности на компанијата, со цел бидат покриени сите можни нарушувања. Безбедноста не е производ туку филозофија, па сите вработени во компанијата треба да бидат едуцирани за слабостите на мрежите, за да можат да бидат внимателни во секое време кога ќе работат со податоци на компанијата или ќе користат ресурси поврзани со Интернет.

Ангажирање на етички хакери за тестирање на системот
Етичките хакери се од голема корист кога една компанија сака да спречи софистицирани напади. Таквите хакери вршат напади на високо ниво и тестови за пенетрација со согласност на компанијата. Целта на овие тестови е

да се идентификуваат слабите точки во системот, така што истите ќе можат да бидат пополнети за да се спречат надворешни напади. Некои компании рутински спроведуваат внатрешни тестови, меѓутоа тие не можат да бидат толку ефикасни и исцрпно изведувани како оние од страна на етичките хакери.

Други мерки

Без разлика дали станува збор за мал бизнис или голема компанија, губењето на податоци може да претставува голем неуспех. Постојат неколку други мерки кои, за подобра безбедност, можат да се имплементираат на мрежно администраторско ниво. Тие вклучуваат конфигурирање на фајервол за одвраќање на непреченото навлегување на можните натрапници; употреба на VPN (виртуелна приватна мрежа) или SSH (безбедна школка) клучеви за автентикационите процедури; користење на смарт картички и други напредни технологии; и, ажурирање на сите системи. Можат да се следат и хакерските форуми. Постојат онлајн хакерски форуми кои информираат за напредокот во хакерската технологија. Со учество на вакви форуми можат да се следат хакерските активности и да се откријат сите нови методи. Ова, од своја страна, ќе помогне за задржување на системите на компанијата безбедни.

Заклучок

Безбедносната политика е основа врз која се гради ефективна безбедност. Како и секоја друга основа, таа мора да биде добро дизајнирана и воспоставена. Проблемите со безбедноста се појавуваат во многу секојдневни активности, иако понекогаш може да е тешко да се направи разлика помеѓу безбедносниот напад и обичниот човечки или технолошки дефект. За жал, паметните напаѓачи ја сфаќаат ваквата забуна и прават нивниот напад да изгледа како едноставна, случајна грешка.

Заканата е дејствие кое може да предизвика штета. Ранливоста е слабост преку кој може да настане штета. Овие два проблема се комбинираат: едната без другата не предизвикува штета, но заканата која ја искористува ранливоста значи штета. За контролирање на таквата ситуација, може или да се спречи или намали заканата, или да се ограничи ранливоста.

Користена литература:

1. MCGlobalTeck – Bridging the gap betwean mission, technology & security.
2. Billy Max - Professor of mechanical engineering, SANS: IEEE Transactions and Business Solutions websites, 2014.
3. Daniel Kehrer, Founder & Managing Director of BizBest Media Corp, 2013.
4. Sam Kassoumeh - SecurityScorecard

Феџри Шаини
Факултет за детективи и криминалистика
Европски универзитет - Република Македонија

Аспекти на одговорноста во областа на приватното обезбедување во Република Македонија

Апстракт
Одговорноста претставува базичен критериум за квалитетно и ефикасно работење во областа на приватното обезбедување. Законот мора да се почитува од секој припадник на агенциите за приватно обезбедување и никој не може да биде привилигиран за сторените прекршоци и кривични дела. Одговорноста во приватното обезбедување се јавува во неколку облици: дисциплинска одговорност, материјална одговорност, кривична одговорност итн. Видот на одговорноста зависи од природата на повреда на одредбите од законот и другите акти со кои се регулира дејноста на приватното обезбедување. Етичката одговорност претставува предизвик кон која се стреми современиот човек и овој облик на одговорност мора да важи и за приватното обезбедување. Авторот на трудот настојува да го постави прашањето за одговорноста во оваа област на работење како детерминанта за отчетност и јакнење на капацитетите на приватното обезбедување.

Клучни зборови: безбедност, контрола, закон, отчетност, одговорност

Responsibility Aspects of Private Security in the Republic of Macedonia

Abstract
Responsibility is the basic criterion for quality and efficient operation in the area of private security. Law must be obeyed by every single member of the private security agencies and no one can be privileged for committing offenses and crimes. Responsibility in private security occurs in several forms: disciplinary responsibility, material liability, criminal responsibility, etc. The type of responsibility depends on the nature of the violation of the provisions of the law and the other acts that regulate the activity of the private security. Ethical responsibility is but a challenge for the modern person, and this form of responsibility must also apply to private security. The author of the paper seeks to raise the question of the responsibility in this working area as a determinant of report and of strengthening the private security capacities.

Keywords: security, control, law, report, responsibility.

Вовед
Прашањето за одговорноста како начело во функционирањето на институциите на општествениот систем воопшто отсегаш го окупирало вниманието на академската заедница. Затоа кон истражувањето на оваа подрачје се разликуваат неколку пристапи: социолошки, етички, казнено-правен, морален итн. Притоа, секој од наведените пристапи се засновува врз парадигми кои се иманентни за нивната природа, со настојување секој од свој

аспект да го објасни феноменот како што е одговорноста. Паралелно со ова, треба да се наведе дека после распадот на поранешните социјалистички држави и создавање на новите демократии, одговорноста добива нова димензија и посебно место во агендата на носителите на политичката власт. Меѓутоа, ова издигнување на површината на интересните сфери најчесто е поставувано во погрешен правец. Зошто? Најпрвин затоа што за одговорното односно неодговорното работење на институциите редовно во практика се истражува после промена на власта. Значи, многу ретко, во изолирани случаи, се практицира оценување на одговорноста на носителите на власта и тоа од многу индикативни причини. Второ, не постои изградена демократска свест за контрола и надзор над законитото и професионално работење на службениците и раководните лица како во јавниот, така и во приватниот сектор. Притоа, "неопходно е да се истакне дека приватната безбедност, како значајна современа безбедносна област со сите свои противречности, динамика на развој и детерминзмот, исто така влијае и на промената на самиот концепт за безбедност и на безбедносниот сектор"[300].Трето, невладиниот сектор во изминатиот период исто така, не е обединет околу создавање стратегија за надзор над работењето на власта и посебно над приватниот сектор. Дотолку повеќе, што "цивилното општество насекаде, па со тоа и во Македонија, претставува движечка сила, поради што е потребна поголема подготвеност за прифаќање на критиките и на заложбите што ги прават граѓанските организации, имајќи став дека заедничка определба на сите е подобрување во сферата на човековите права."[301] "Групите во рамките на граѓанското општество како што се академските институции, Think Thanks, НВО за човекови права и НВО насочени кон политички прашања, можат активно да се борат и да имаат влијание врз одлуките и политиката кои се однесуваат на секторот за безбедност."[302]

Четврто, прашањето за одговорност или неодговорното работење најчесто се решава во текот на кривичната постапка со широка јавна промоција на одделни случаи со цел да се поентира во јавноста и најчесто за дневно – политички потреби. Меѓутоа, не треба да се заборави дека улогата на кривичното законодавство е пред се репресивна, иако има и превентивна димензија и дека неговиот систем се активира тогаш кога сите останати општествени социјални и првентивни мерки не дале ефект во борбата против криминалитетот.

Кога станува збор за одговорноста на припадниците на приватното обезбедување веднаш се појавува перцепцијата дека во јавноста многу малку се зборува за овој феномен, иако има случаи во кои се евидентни незаконити постапки или непрефесионално однесување. Индикативно е што во јавноста ова прашање воопшто не е застапено, а во научните кругови ретко се среќаваат текстови со објаснување на неговата природа, етиологија,

---

[300] Kozarev A., Privatna bezbednost u Republici Makedoniji – aktuelno stanje I perspective, Zbornik radova, Prvi međunaraodni naučni skup: Privatna bezbednost – stanje I perspective, Novi Sad, 2008 godina, str. 169.

[301] Томшиќ-Стојковска А., Улогата на цивилното општество во сферата на чеовековит права, Зборник од научната расправа: Европските стандарди за човековите права и нивната имплементација во правниот систем на Република Македонија, МАНУ, Скопје, 2008 година, стр. 375.

[302] Центар за демократска контрола на вооружените сили, Интер - парламентарна унија, Прирачнчик за парламентарци бр. 5, 2003 година, стр. 36.

феноменологија. Од овие причини, се наметна потребата се проучат одредени аспекти на прашањето за одговорноста и одговорното работоење во областа на приватното обезбедување и на тој начин да се даде конкретен придонес во јакнење на неговите капацитети, интегритет и доверба како кај граѓаните, така и кај деловната заедница кои се корисници на нивните услуги дефинирани со закон и подзаконски акти.

1.Демократијата, одговорноста воопшто и одговорноста како начело на работење во областа на приватното обезбедување

Демократските системи се одликуваат со начелата на одговорно, транспарентно и отчетно работење во целина. Системот на поделба на власт всушност и се заснива на односите на рамнотежа на власта, при што одговорноста на секој носител на власта е прашање кое е природно сврзано со системот. Дал[303], своевремено власта ја дефинира како "однос помеѓу актерите, во кој еден актер принудува друг да дејствува на начин на кој инаку би дејствувал". Сартори[304], пак, вели: "власта наредува, командува, наложува. Демократскиот систем на власт, барем на теоретска основа се смета за антипод на авторитарните односно тоталиттарните системи. Но, и демократијата како политички систем се темели на владеење. Од другите режими се разликува дотолку: што во неа дејствувањето на власта е јавно; јазот помеѓу водачот и водените е најмал." "Карактеристика на демократската власт, е значи, тоа што таа е отворена, толерантна и подготвена за предизвикот на слободната конкуренција, во која постои континуиран, институционално овозможено и правно гарантирано влијание на општеството врз формирањето и спроведувањето на државната политика.[305] Имено, "работата и дејствувањето на државните органи е јавно и е предмет на критичко вреднување, па оттаму и е подложно на механизмот на правна одговорност, што ќе рече дека државните органи и службеници се одговорни за своите противуставни или противзаконски акти и постапки."[306]

Според Светската Банка: доброто владеење го карактеризираат предвидливо, отворено и посветено креирање на политика, бирократија исполнета со професионална култура која делува за унапредување на јавното добро, владеење на правото, транспарентни процеси и силно граѓанско општество кое учествува во јавните работи. Лошото владеење (од друга страна) се карактеризира со произволно креирање на политика, бирократија која не е отчетна, неспроведени или неправилни правни системи, злоупотреба на извршната моќ, граѓанското општество кое е не вклучено во јавниот живот и распространета корупција.[307]

"Одговорноста и отчетноста се однесуваат на начинот на практицирање на власта од нејзините носители, а пред се на спроведувањето на уставните и

[303] R.A.Dahl, Modern Political Analysis, Englewood Cliffs, 1963, p. 68.
[304] Sartori Dj., Demokratija šta je to? Podgorica, 2001, str. 168 – 172..
[305] Radonjić R., Demokratija, Podgorica, 2004 godina, str. 54-55.
[306] Бајалџиев Д., Вовед во правото, Држава, Книга прва, Скопје, 1999 година, стр. 374.
[307] Светска Банка, Владеење: Искуствата на Светска Банка, 1994 година.

законските овластувања и надлежности од страна на носителите на јавни овластувања."[308] Меѓутоа, овие сложени и суштински прашања се поставуваат и во врска со функционирањето на приватниот безбедносен сектор заради следното:

1. Дејноста приватно обезбедување претставува дејност од јавен интерес;
2. Приватните обезбедувачи имаат законски овластувања со репресивен карактер;
3. Услугите на приватното обезбедување се повеќе завземаат место во работењето на компаниите и со тоа стануваат фактор за нивната безбедност;
4. Приватната безбедносна индустрија вработува голем број на лица кои извршуваат дејност приватно обезбедување и се наоѓа на трето место после полицијата и војската;
5. Дејноста на приватно обезбедување е надвор од демократска контрола.

Затоа се наметнува потребата од системско омеѓување на дејноста приватно обезбедување со начелото на одговорност. Тоа може да се постигне преку утврдување на детерминантите за одговорноста и одговорното работење, како што се следните:

- Имплементирање на одреден тип безбедносна култура за приватната индустрија за безбедност која ќе извира од фундаментот на општата безбедносна култура. На овој начин ќе се овозможи да се развие свеста кај поединците кои се носители на овластувања за вршење на приватното обезбедување. Безбедносната култура е основа за ефикасност, отвореност и демократичност на приватната безбедност како дејност од јавен интерес;
- Развивање на механизми на внатрешна и надворешна контрола над функционирањето на приватната безбедност, со што содржински ќе се создадат услови за развивање на начелото на одговорност и одговорно работење;
- Начелото на одговорност создава претпоставки за почитување на човековиет слободи и права во врска со примената на овластувањата на приватните обезбедувачи, владеењето на правото и правната држава.

"Внатрешната контрола на работата и однесувањето на припадниците на приватното обезбедување мора да се засили, како и секојдневната едукација. Се разбира, за овој дел од работата потребно е посебно да се едуцираат кадри со повисоко образовно ниво. Контролата на полицијата би морала да биде континуирана, а по потреба и вонредна, воочените пропусти брзо и ефикасно да се санкционираат, со задолжително давање стручна помош на менаџментот на агенциите, но и на поедини припадници на физичкото обезбедување."[309]

---

[308] Козарев А., Парламентарна контрола и надзор над безбедносниот сектор во Република Македонија, Скопје, 2011 година, стр. 56.

[309] Škondrić V., Ovlaščenja agancija za obezbedzenje lica I imovine I privatnih detektiva, Zbornik radova, Prvi međunaraodni naučni skup: Privatna bezbednost – stanje I perspective, Novi Sad, 2008 godina, str. 388.

2. Нормативна уреденост на начелото на одговорност во областа на приватното обезбедување

Основата на нормативната уреденост на начелото на одговорност ја сочинуваат одредбите од Законот за приватно обезбедување. Никулците на начелото на одговорност се евидентни уште во првите одредби на овој закон. Имено, во дефинирањето на целите на приватното обезбедување преку превентивна-репресивна концепција се наведува дека правните лица кои имаат дозвола за приватно обезбедување преземаат мерки и активности утврдени со овој закон заради спречување и откривање на штетни појави и противправни дејствија кои ги загрозуваат телесниот интегритет и достоинството на личноста и имотот што се обезбедува. Натаму, преку определување на недозволените работи поврзани со приватното обезбедување исто така посредно се поставува прашањето за одговорност доколку некое правно лице кое има дозвола за приватно обезбедување обезбедуваат лица и имот кои врз основа на посебни прописи ги обезбедуваат надлежни државни органи; доколку вршат работи поврзани со наплата на долг или пак, применуваат оперативни методи и средства кои со закон не се дозволени или за чија примена врз основа на посебни прописи се овластени само надлежни државни органи.

Начелото на одговорност во областа на приватното обезбедување има две димензии:

А) одговорност на правните лица и

Б) индивидиална одговорност на приватниот обезбедувач.

Одговорноста за нивното законито постапување произлегува од извшрениот надзор од страна на овластени службени лица на Министерството за внатрешни работи, како облик на надзор над законитоста на работењето затоа што овие лица конкретно го надзираат спроведувањето на одредбите од Законот за приватно обезбедување и на прописите кои се донесени врз основа на овој закон.

Исто така, покрај овој модул, овластени службени лица на Министерството за внатрешни работи редовно ја надзират работата и на Комората за приватно обезбедување и тоа најмалку еднаш во календарската година.

Предмет на полициискиот надзор опфаќа:

1) утврдување дали и како се спроведува овој закон и прописите донесени врз основа на овој закон;

2) проверка на евиденцијата на склучените договори од членот 6 став (1) од овој закон;

3) преглед на деловните простории, техничките средства и уреди и возилата кои се употребуваат во вршењето на работи на приватно обезбедување;

4) проверка на начинот на чување и носење на огненото оружје, како и на оспособеноста за ракување и употреба на огненото оружје и

5) проверка на начинот на примена на овластувањата на работниците за обезбедување.

По потреба овластените службени лица на Министерството преземаат и други мерки и активности со кои се врши надзор.[310]

[310] Член 67 од Законот за приватното обезбедување.

Врз основа на извршениот надзор се сочинува записник и кај најтешки мерки кои може да ги примени Министерството за внатрешни работи се јавуваат следните:
А) одземање на дозволата за обезбедување ако правното лице кое врши обезбедување на лица и имот доколку:
1) повеќе не ги исполнува условите за издавање дозвола за обезбедување утврдени со овој закон и
2) не ги отстрани недостатоците во рокот утврден со решението од членот 68 став (2) од овој закон.[311]
Министерството ги известува Комората и Централниот регистар на Република Македонија за одземањето на дозволата за обезбедување на правното лице веднаш по конечноста на решението.
Б) Одземање на јавните овластувања на Комората, доколку не ги отстрани недостатоците во рокот предвиден со решението од членот 68 став (2) од Законот за приватното обезбедување. Во случај на одземање на јавни овластувања на Комората, јавните овластувања ги врши Министерството, сé до отстранувањето на недостатоците од страна на Комората.[312]

3.Видови одговорност во областа на приватното обезбедување

"Општиот поим на одговорноста во правото има различни значења (Hart, на пример, разликува четири: одговорна позиција, одговорност за последицата со сопствените постапки, одговорност како обврска за исполнување определени правни должности и одговорност во смисла на пресметливост, капацитет на одговорност). По дефиниција одговорноста имплицира, натаму, двостран однос меѓу два субјекта: тој што одговара и тој пред кого се одговара! Никој не може за своите постапки да одговара пред самиот себеси, освен ако под тоа не се подразбере одговорност пред сопствената совест!"[313]
Одговорноста на субјектите на приватното обезбедување е сложена и повеќеслојна:
- Морална;
- Етичка;
- Прекршочна;
- Дисциплинска;
- Кривична.
Нормативната рамка која се однесува на одговорноста во областа на приватното обезбедување подразбира и:
- Општа одговорност за штета (граѓанско-правна одговорност – Закон за облигационите односи, ЗПО);
- Одговорност за сторени прекршоци (прекршочна одговорност – Закон за прекршоци итн.);
- Одговорност за кривични дела (Кривичен законик, Закон за кривична постапка).

[311] Член 69 од Законот за приватното обезбедување.
[312] Член 70 од Законот за приватното обезбедување.
[313] Камбовски В., Казнено право, Култура, Скопје, 2004 година, стр.523.

3.1. Морално – етичка одговорност

Камбовски В., наведува дека "уште старите Римјани го дефинирале правото како ars aequi et boni, внесувајќи го во неговата дефиниција етичкиот критериум за доброто! Постои суштествена разлика и во системот на санкции: внатрешни санкции, врз кои се потпира моралот, и формални санкции со кои располага казненото право (кан: правото го регулира надворешното, а моралот внатрешното однесување!)."[314]

Морално-етичкиот дигнитет на приватните обезбедувачи е предмет на оценка ушт при утврдувањето на исполнетост на условите за добивање лиценца за обезбедување. Во член 22 од Законот за приватно обезбедување, покрај останатите услови се бара лицето да не е осудено со правосилна судска пресуда или против него да не се води постапка за кривично дело. Тоа значи, се бара лицето кандидат да ги почитува нормите на правниот поредок преку однесување кое го пави достоен за вршење на оваа дејност.

Понатаму, моралнио и етички лик на приватниот обезбедувач е фундиран со доследно почитување на одредбите од Кодексот на професионалната етика на вршителите на дејноста обезбедување на лица и имот, кој определува дека секој припадник на оваа дејност:

- својата работа ќе ја врши согласно Уставот и законите на Република Македонија, грижејќи се за заштита и унапредување на интересите на државата и заедничкото право на слобода, еднаквост, рамноправност и законитост.
- законите ќе ги спроведува правилно и човечно, секогаш со тенденција на решавање на споровите на мирољубив начин, воздржувајќи се од примена на насилство и непотребна сила. Во вршење на работата секогаш ќе се води од правилата на професијата, моралот и етиката. Никогаш нема да дозволи неговите лични чувства, предрасуди, политички убедувања и стремежи, омразата, љубовта, пријателските или роднински врски да влијаат врз донесување на неговите одлуки и извршување на неговите должности и обврски.
- свесност дека единствено е одговорен за стандардите и нивото на професионалноста во вршење на дејноста обезбедување на лица и имот и секогаш ќе тежнее достојно да ја извршува својата професија, гордо стоејќи зад службената легитимација и бранејќи ја довербата која преку неа му ја доделува македонската држава и јавност.
- личниот живот ќе го води чесно и ќе се однесува на начин кој нема да го дискредитира, службата во која работи или странките со кои поради природата на работата, секојдневно има контакти. Секогаш ќе се обиде да ги задржи присебноста во расудувањето, спокојот и самоконтролата.
- гарантира дека секогаш ќе ги почитува и со цело тело, душа и свест ќе ги исполнува сите изјави кои во оваа прилика ги прифаќа како дел од него и неговото постоење, затоа што да се работи на обезбедување значи да се постои за друго човечко битие, за државата.

[314] Камбовски В., Казнено право, Култура, Скопје, 2004 година, стр.20-21.

3.2.Прекршочна одговорност

Прекршочните одредби за дејноста приватно обезбедување се содржани во Глава XI од Законот за приватното обезбедување. За сторените прекршоци предвидени се следните глоби:

А) за одговорното лице во правното лице во зависност од видот на прекршокот, може да се изрече:

(1) глоба во износ од 400 до 500 евра во денарска противвредност;
(2) глоба во износ од 1. 500 до 1. 800 евра во денарска противвредност;
(3) глоба во износ од 1. 200 до 1. 500 евра во денарска противвредност;

Б) за прекршочна одговорност на правното лице, кое во зависност од видот на прекршокот може да се изрече:

1) прекршочна санкција забрана на вршење на дејност приватно обезбедување во траење од шест месеци до пет години;
2) глоба во износ од 900 до 1. 000 евра во денарска противвредност
3) глоба во износ од 3. 500 до 4. 000 евра во денарска противвредност;
4) прекршочна санкција забрана на вршење на дејност приватно обезбедување во траење од шест месеци до пет години.

В) за физичко лице во зависност од видот на прекршокот, може да се изрече

(1) глоба во износ од 600 до 700 евра во денарска противвредност.
(2) глоба во износ од 900 до 1. 000 евра во денарска противвредност;
(3) забрана за вршење на дејност обезбедување на лица и имот во траење од една до пет години.

Феноменологијата на прекршоци е разнолика и опфаќа:

а) ***за физички лица***: 1) на барање на правното лице за приватно обезбедување на ја врати легитимацијата за обезбедување (член 25 став (6)); 2) на барање на овластено службено лице на Министерството не го даде на увид налогот за носење на огнено оружје, дозволата за носење на оружје, како и огненото оружје што го носи (член 29 став (3)); 3) врши работи на одржување на јавниот ред на јавни собири и други настани без работна облека и без елеци со светлоодбојни ленти на кои има натпис „Обезбедување“ (член 38); 4) во вршењето приватно обезбедување не носи легитимација за обезбедување (член 46 став (1)); 5) не ја покаже легитимацијата за обезбедување во случај кога се повикува на вршење на приватно обезбедување или не ја покаже легитимацијата за обезбедување на барање на овластено службено лице на Министерството (член 46 ставови (2) и (3)) и 6) во рок од 24 часа не поднесе писмен извештај за задржувањето, односно употребата на средства за присилба (член 57 став (1)); 7) при вршење на физичко обезбедување носи огнено оружје и муниција спротивно на членот 29 ставови (4) и (5) од овој закон; 8) носи сопствено огнено оружје за време на вршење на физичко обезбедување на лица и имот (член 30); 9) веднаш не ја извести полицијата, доколку примената информација во центарот за обезбедување и надзор укажува дека се врши кривично дело за кое се гони по службена должност (член 33 став (5)); 10) работите на обезбедување на јавни собири и други настани ги врши со употреба на огнено оружје (член 38 став (4)); 11) при

вршење на физичко обезбедување применува овластувања за кои не е овластен согласно со членот 45 став (1) од овој закон; 6) применува овластувања спротивно на членот 45 став (2) од овој закон; 7) не постапи по наредба на овластено службено лице на Министерството (член 47 став (1)); 12) изврши задржување на лице спротивно на членот 52 од овој закон; 13) употреби средства за присилба спротивно на членот 54 од овој закон и друго.

б) ***за правни лица***: 1) не го извести Министерството за настанатата промена во однос на основачот, адресата, називот или одговорното лице во правното лице кое има дозвола за приватно обезбедување, во рок од осум дена од денот на настанатата промена (член 17 став (2)); 2) во рокот утврден со закон не ја извести Комората дека престанало да ја врши дејноста (член 19); 3) не ја одземе легитимацијата за обезбедување, односно не ја достави за поништување до Комората во пропишаниот рок, или не ја извести Комората во пропишаниот рок за неисполнување на еден од условите утврдени членот 25 став (2) од овој закон од страна на работникот за обезбедување и не ја огласи легитимацијата за неважечка (член 25 ставови (4) и (5)); 4) не изведе задолжително контролно гаѓање најмалку еднаш годишно (член 31 став (1)); 5) нема дежурство од 24 часа во Центарот за обезбедување и надзор (член 33 став (3)); 6) врши работи на одржување на јавниот ред на јавни собири и други настани со работници за обезбедување кои не носат работна облека и немаат на себе елеци со светлоодбојни ленти на кои има натпис „Обезбедување“ (член 38) и 7) работната облека не е во согласност со членот 58 ставови (3) и (6) од овој закон и друго.

3.3.Кривична одговорност

Поимот казнена одговорност е идентичен со поимот на вина. И двата се законски поими! КЗМ зборува за кривична одговорност (чл 11 ст. 1): кривично е одговорен сторителот кој е пресметлив и што кривичното дело го сторил со умисла или небрежност! Повлекувањето на знак на равенство меѓу поимот на казнена одговорност и поимот на вина е резултат на современото сфаќање за казнената одговорност заснована врз начелото на вина (иако во теоријата може да се сретне стојалиштето според кое тоа не се идентични поими: поимот казнена одговорност е синтетички поим кој покрај вината ги вклучува и стие други објективни и субјективни претпоставки за казна. Современото казнено право успешно се спротивставува на реставрирањето на објективната одговорност, но од друга страна е неспорно дека прифаќањето на казнената одговорност на правните лица, заснована врз концепцијата на претпоставена одговорност, значи прво официјално раздвојување на ови епоими (правното лице може да се огласи за казнено одговорно, но не и за виновно, зашто второво подразбира исклучително субјективна одговорност на поединецот како сторител на казнено дело!).[315]

Казнената одговорност посебно е значајна за приватното обезбедување како дејнсот од јавен интерес, затоа што се работи за овластувања кои имаат делумно репресивен карактер – вклучени се можности за примена на сила.

[315] Камбовски В., Казнено право, Култура, Скопје, 2004 година, стр.524.

Оттука, важни се општите кривично правни институти на материјалното казнено право од една страна, но и законските инкриминации кои се содржани во КЗ (познато како казнено право посебен дел). Меѓу првите посебно влегуваат следните институти: а) противправноста како елемент на кривичното дело: противправниот напад исполнува обележја на некое казнено дело; противправното обезбедување може да доведе до противправни напади на имот затоа што приватното обезбедување. Противправноста е елемент на дејствието на напаѓачот спрема лицето или имотот кој е предмет на обезбедување, но може да биде и елемент на дејствието што го превзема субјектот на приватното обезбедување. Дејствијата на приватните обезбедувачи при примената средствата за присилба претставуваат prima facie противправни дејствија.

Во случаите на нужна одбрана versus одбраната на обезбедуваниот субјект т.е. објект, кај насоченоста на нападот се јавуваат две ситуации: а) напад насочен кон животот на работникот за приватно обезбедување или кон животите на лицата кои ги обезбедува или кон имотот и б) напад кон сторителот на делото во нужна одбрана или кон трето лице (т.н. нужна помош). Во ситуации на приватното обезбедување кога ќе дојде до пречекорување на овластувањата во оваа област, пречекорувањето на границите на нужната одбрана се однесува на:

- Нужноста и интензитетот (интензивен ексцес) – правно релевантно;

- Времетраењето на одбраната (екстензивен ексцес) – правно ирелевантно.

Од аспект на законските инкрминации под кои би можеле да се подведат евентуални незаконити постапки и кривично-правни релевантни однесувања на приватните обезбедувачи, може да се наведат следните:

Заклучок

Проучувањето на одговорноста на феномен претставува сложен предизвик за секој истражувач воопшто. Не постои област од општественото живеење која може да функционира во отсуство на начелото на одговорно, отчетно работење. Тоа е логична последица на фактот што ниту една компанија, систем не е имун од конкретни, но и идни злоупотреби поврзани со деловното работење. Ниту дејноста приватно обезбедување како дејност од јавен интерес чии што припадници (приватни обезбедувачи) не може да биде ефикасно без консеквентна примена на начелото на одговорност. Самата природа на овластувањата со кои располагаат приватните обезбедувачи, посебно оние со репресивен карактер и со кои се ограничуваат одредени човекови слободи и права ја наметнува потребата да се издигне одговорноста како приоритет на деловниот свет. Каков модел на одговорност ќе постои во многу зависи од интересот на менаџерите и сопствениците на компаниите. Тоа пак е поврзано со стилот на управување – авторитарен, демократски, нивна комбинација итн.

Одговорноста на приватните обезбедувачи е повеќедимензионална и ги опфаќа: моралната, етичката, прекрошочната,казнената и други видови на одговорност.

Таа се наметна како детерминанта за успешно извршување на дејноста на приватното обезбедување. Одговорноста во многу зависи од моделот на контрола кој постои, затоа што тие се поврзани едни со други. Независно од оваа симбиоза, заклучокот е дека отсуството на одговорност води кон анархија односно ситуации на злоупотреби на овластувањата на приватните обезбедувачи. Најголемата штета од овие ситуации ја има слободите и правата на човекот и граѓанинот, правната држава и интегритетот на правните лица за приватно обезбедување.

Литература

1. Kozarev A., Privatna bezbednost u Republici Makedoniji – aktuelno stanje I perspective, Zbornik radova, Prvi međunaraodni naučni skup: Privatna bezbednost – stanje I perspective, Novi Sad, 2008 godina.
2. Томшиќ-Стојковска А., Улогата на цивилното општество во сферата на чеовековит права, Зборник од научната расправа: Европските стандарди за човековите права и нивната имплементација во правниот систем на Република Македонија, МАНУ, Скопје, 2008 година.
3. Центар за демократска контрола на вооружените сили, Интер - парламентарна унија, Прирачнчик за парламентарци бр. 5, 2003 година.
4. R.A.Dahl, Modern Political Analysis, Englewood Cliffs, 1963.
5. Sartori Dj., Demokratija šta je to? Podgorica, 2001.
6. .Radonjić R., Demokratija, Podgorica, 2004 godina, str. 54-55.
7. Бајалџиев Д., Вовед во правото, Држава, Книга прва, Скопје, 1999 година.
8. Светска Банка, Владеење: Искуствата на Светска Банка, 1994 година.
9. Козарев А., Парламентарна контрола и надзор над безбедносниот сектор во Република Македонија, Скопје, 2011 година.
10. Škondrić V., Ovlaščenja agancija za obezbedzenje lica I imovine I privatnih detektiva, Zbornik radova, Prvi međunaraodni naučni skup: Privatna bezbednost – stanje I perspective, Novi Sad, 2008 godina.
11. Камбовски В., Казнено право, Култура, Скопје, 2004 година.
12. Закон за приватното обезбедување.

Кристијан Ѓорѓиоски
Факултет за детективи и криминалистика,
Европски Универзитет – Република Македонија

Улогата на Дирекцијата за безбедност на класифицирани информации и корпоративната безбедност

Апстракт
Заштита на информациите е од клучно значење за ефикасното деловно работење. Економската безбедност и деловното работење се поврзани и затоа е потребно да се подигне свеста кај корисниците на класифицираните информации. Индустриската шпионажа претставува сериозна закана за економскиот систем во целина. Сето тоа ја наметнува потребата од преземање на мерки за подигнување на безбедносната свест како што се: почитување на воспоставените безбедносни политики и процедури, почитување на административните и безбедносните зони, пријавување на сомневања за безбедносни нарушувања итн. Тоа значи дека информациите мора да бидат достапни исклучиво на лицата кои поседуваат безбедносен сертификат, да се почитуваат пропишаните мерки за безбедност на класифицирани информации и одржување на тајноста на информацијата и нејзино ограничување од слободна циркулација во јавност. Во овој процес важна улога има Дирекцијата за безбедност на класифицирани инфорамции како институционална основа за имплементација на системот за заштита на класицифицирани информации.

Клучни зборови: безбедност, заштита, информација, институција, мерки и активности.

Abstract
Information protection is a crucial for effective business operations. Economic security and business operations are linked and therefore it is necessary to raise awareness among users of classified information. Industrial spying is a serious threat to the whole economic system. There is a need to take measures to raise awareness of security, such as: respecting established security policies and procedures, respecting administrative and security zones, reporting suspicions of security disorders, etc. This means that information must be accessible exciusively for the holders of a security certificate, to observe the prescribed security measures for classified information and to maintain the confidentiality of the information and its restriction of free circulation in the public. In this process, the Directorate for Security of Classified Information have an important role as an institutional basis for the implementation of the system for the protection of classified information.

Keywords: security, protection, information, institution, measures and activities

Вовед

Информација од интерес за Република Македонија е секоја информација или материјал изготвен од државните органи, орган на единицата на локалната самоуправа, јавно претпријатие, јавна установа и служба, правно и физичко лице, како и странски државни органи, странски 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 човекот и граѓанинот.[316] А пак, класифицирана информација е информација којашто се заштитува од неовластен пристап или употреба и којашто се определува со степен на класификација. Државните органи, организациите, институциите и другите правни лица се должни да создадат услови неопходни за заштита на класифицирани информации и да преземат мерки за елиминирање на негативните последици ако дојде до откривање на класифицираните информации.

- **Дирекција за безбедност на класифицирани информации**

Се со цел да се приближи кон НАТО и ЕУ, Р. Македонија започнала со размена на класифицирани информации. По потпишувањето на Безбедносната спогодба меѓу Р. Македонија и НАТО во 1996 година, во рамките на Министерството за одбрана е формирана Службата за реципрочна безбедност за заштита на информации што се разменети меѓу РМ и НАТО. За безбедна дистрибуција на класифицираните информации до крајните корисници во Службата е формиран Централен регистар, а во Министерството за внатрешни работи и во Министерството за надворешни работи подрегистри.

Р.Македонија презеде активности за промени во безбедносниот сектор поврзани со класифицираните информации и се донесе Законот за класифицирани информации кој влезе во сила на 5 Март 2004 година. За истите надлежна е Дирекцијата за Безбедност на класифицирани информации како самостоен орган на државната управа со својство на правно лице. Согласно Законот, беа донесени неколку уредби и тоа: Уредба за административна безбедност на класифицирани иформации, Уредба за физичка безбедност на класифицирани информации, Уредба за индустриска безбедност на класифицирани информации и Уредба за информатичка безбедност на класифицирани информации.

Дирекција за безбедност на класифицирани информации е основана за спроведување на утврдената политика за заштита на класифицираните информации и меѓународните стандарди за реализирање на размената на класифицирани информации во согласност со меѓународните договори, за вршење инспекциски надзор на спроведуавањето на одредбите на Законот за класифицирани информации и на другите прописи од областа на класифицираните информации, како и за вршење други работи утврдени со законот. За ефикасно и координирано извршување на правата и обврските кои се однесуваат на класифицираните информации во сите корисници на класифицирани информации се определува овластено лице кое треба да

[316] Закон за класифицирани информации (10 фев. 2004)

поседува соодветен безбедносен сертификат. Безбедносен сертификат е документ кој овозможува физичките или правните лица да имаат право на пристап и користење на класифицирани информации во извршувањето на работните обврски. Постојат два вида безбедносни сертификати кои што ги издава Дирекцијата и тоа: безбедносен сертификат за физичко лице и безбедносен сертификат за правно лице. Безбедносните сертификати може да се издадат за ракување со национални, со НАТО или со ЕУ класифицирани информации. Дирекцијата за безбедност на класфицирани информации издава национални безбедносни сертификати до највисокиот степен "Државна тајна".

- **Надлежности на ДБКИ**

Надлежности на Дирекцијата, по својата природа можат да се поделат во три групи: на примените информации;

- надлежности со надворешна димензија коишто се однесуваат на вршењето контрола на начинот на којшто се чуваат и се заштитуваат класифицираните информации што Р.Македонија им ги има отстапено на користење на странски држави и на меѓународни организации како и надлежностите коишто се однесуваат на учеството на Р.Македонија во евроатлантските структури и иницирањето меѓународни договори;

-други надлежности коишто се однесуваат на развивање планови за заштита на класифицирани информации во вонредни состојби, како и обука на корисниците на класифицираните информации преку организирање разни советувања, семинари и одделни консултации[317].

Дирекцијата за безбедност на класифицирани информации ги врши работите што се однесуваат на:

- обезбедува континуирано спроведување на меѓународните стандарди и нормативи во преземањето на мерките и активностите за заштита на класифицираните информации;
- вршење контрола на начинот на којшто се чуваат и заштитуваат класифицираните информации коишто Р.М. им ги има отстапено на користење на странски држави и меѓународни организации, како и надлежностите коишто се однесуваат на учество на Р.М. во евроатлантските стурктури и иницирањето склучување на меѓународни договори;
- останати надлежности коишто се однесуваат на развивање планови за заштита на класифицирани информации во вонредни состојби, како и обука на корисниците на класифицираните информации преку организирање на разни советувања, семинари и поединични консултации;
-врши координација на активностите во обезбедувањето заштита на класфицираните информации со државните органи и институциите кои вршат размена на класифицирани информации со странски држави и меѓународни организации;

[317] http://www.dbki.gov.mk/

- учествува во изготвување на планови и програми на Р.Македонија за членство во меѓународни организации од областа за обезбедување заштита на класифицираните информации;
-предлага мерки за унапредување на заштита на класифицирани информации;
-покренува иницијативи за склучување меѓународни договори со странски држави и меѓународни организации од областа на размената на класифицирани информации;
- врши други работи утврдени со Законот за класифицирани информации и друг закон.

- Организација на Дирекцијата за безбедност на класифицирани информации

Во дирекцијата се формирани организациски единици во коишто се вршат работи и задачи во доменот на: административната безбедност на класифицирани информации, физичката безбедност на класифицирани информации, безбедноста на лица корисници на класифицирани информации, индустриската безбедност на класифицирани информации и информатичката безбедност на класифицирани информации, како и во доменот на општите, нормативно-правните работи и меѓународната соработка. Во Дирекцијата се формирани и организациски единици надвор од секторите коишто во согласност со позитивните законски прописи за организација и работа на органите на државната управа треба да бидат со ваква позиционираност. Во овие организациони единици со кои што раководат раководители кои што директно одговараат на функционерот што раководи со органот, се вршат работи и задачи во доменот на финансиските прашања и човечките ресурси.

Корпоративна безбедност

Корпоративната безбедност може да се одреди како збир на работи со кои се обезбедуваат лицата, имотот и работењето во самите компании. [318]Во поширока смисла на зборот во корпоративната безбедност влегуваат безбедносните предизвици, ризици и опасности, како и конкретните појави со кои се загрозува безбедноста на корпорацијата. Всушност корпоративната безбедност е одговорна за сите безбедносни процеси во деловниот субјект. За успешна имплементација на корпоративната безбедност треба да се следат повеќе модели и врз основа на одреднајсоодветен. Корпоративната безбедност треба да создаде услови за краткорочно, долгорочно и стабилно извршување на дејноста и остварувањето на корпоративните цели. За да се постигне сето ова, задачите кои се поставуваат пред системот на корпоративната безбедност и заштита се проценување на актуелните и предвидување на потенцијалните ризици, воспоставување на соодветна организација за извршување на безбедносните задачи, собирање и обработка на безбедносните информации и обезбедување на континуитет на работењето во насока на остварување на стратешките цели корпоративната безбедност е составен дел на организацијата на работа. Со други зборови

[318] Татјана Г.: Корпоративна безбедност. 2017

организационата единица задолжена за безбедноста на деловната организација мора да биде перманентно вклучена во механизмите на деловното управување така што ќе го штити нормалното извршување на деловните процеси, ќе ги отстранува акутните безбедносни проблеми и ќе создава безбедносни услови за работа. Посебен акцент ќе биде ставен на улогата на физичкото обезбедување во корпоративната безбедност. Потребата од приватно обезбедување во Р.Македонија се јави по стекнување на нејзината сувереност[319]. Приватните безбедносни компании се навистина многу значајни и специфични субјекти, односно тие се значајни деловни субјекти, кои се заинтересирани за создавање на одреден профит на пазарот на безбедносните услги, па не би било добро државата да има големо влијание и на тоа подрачје бидејќи тоа би било контрапродуктивно. Корпоративниот систем на безбедност може да се зборува како и за управувачкиот потсистем, кој има улога, во безбедносен поглед да ги побрзе сите делови помеѓу себе и организацијата со средината што се постигнува со комуницирање со другите делови на системот и средината, врамнотежување на очекувањата и можностите на организацијата и одлучувањето во тој правец. За да може корпоративната безбедност да биде успешно спроведена потребно е таа најпрво добро да биде испланирана, потоа да следува добра организација и на крај треба да се спроведе контрола за да се утврдат евентуалните отстапувања или недостатоци.

Постојат некои начела во корпоративната безбедност на кои теоретичарите но и оние кои се инволвирани во праксата обрнуваат внимание и ги наметнуваат како дел од корпоративното управување. Тие начела се: начело на законитост, начело на систематичност и планирање, начело на координација и соработка, начело на брзина и оперативност, начело на деталност и упорност, начело на објективност, начело на единствено раководење, начело на стручност и специјализација, начело на превентивно постапување, начело за чување на службени и деловни тајни, начело на хуманост и др.

- **Уредба за физичка безбедност на класифицирани информации**

Со оваа уредба се пропишуваат мерките и активностите за физичка безбедност за заштита на класифицирани информации кои се спроведуваат од страна на државните органи, организациите, институциите и другите правни и физички лица[320]. Всушност се врши проценка за можното нарушување на безбедноста на класифицираните информации, а врз основа на проценката на органот се изготвуваат планови за физичка заштита за секој објект посебно. Во планот за физичка заштита се определува безбедносниот појас околу објектот во кој се ракува со класифицирани информации. Безбедносниот појас претставува минималното растојание до објектот кое оневозможува, со примена на активни или пасивни средства, да се открие содржината на класифицираната информација. Во планот за физичка заштита

[319] Прирачник за оспособување и полагање на стручен испит за вршење на работи за физичко обезбедување, стр.4, 2013
[320] Уредба за физичка безбедност на класифицирани информации (16 ноем.2004)

се определуваат безбедносните и административните зони во објектот во кој се ракува со класифицирани информации.

Организацијата на физичката заштита, освен идентификација на локациите и објектите за кои е потребна заштита опфаќа и повеќеслојни безбедносни мерки: безбедносна ограда; безбедносно осветлување; систем за откривање на недозволено физичко присуство на лица; контрола на пристап; чувари односно чуварска служба; интерен безбедносен систем за видео надзор; контрола на посетители и одобрена опрема.

Воспоставениот систем на физичка заштита опфаќа и проверка на влезот и излезот за спречување на неовластено внесување на материјали во просториите или изнесување на класифицирани информации надвор од објектите. Во објектите и просториите во безбедносните и административните зони се влегува со дозвола за пристап. Информации класифицирани со степен "Државна тајна" се чуваат во безбедносни зони од прв и втор степен. Се преземаат некои од следните мерки: сигурносни сефови, постојана заштита со чувари или дежурен персонал; систем за откривање на неовластено физичко присуство. Информации класифицирани со степен "Строго Доверливо" се чуваат во безбедносни зони од прв и втор степен. При чувањето на класифицираните информации се презема една од следните мерки: со одобрени сигурносни сефови или во подрум без дополнителни контроли или на отворен простор за чување во кој се врши една од следните дополнителни контроли: постојана заштита на локацијата на која се наоѓа отворениот простор за чување од чуварска или од дежурна служба; отворениот простор за чување да биде проверуван од чуварска или дежурна служба еднаш на секои четири часа или да е воспоставен систем за откривање на неовластено физичко присуство.

Кога информациите класифицирани со степен "Доверливо" и повисоко се чуваат на отворени полици или се прикажани на карти, мапи или на друг начин во подруми или на отворени простори за складирање изградени во зоните од прв и втор степен, ѕидовите, подовите, таваните и вратит со брави, одобрени од надлежен орган според пропишаните стандарди. Информации класифицирани со степен "Интерно" се чуваат во канцелариски мебел што се заклучува.

Заклучок

Заштитата на информациите е од големо значење за ефикасно и успешно работење во било која институција или коорпорација . Затоа е потребно да се подигне свеста кај корисниците на сите информации, вклучувајќи ги и класифицираните информации за кои е потребна поголема заштита и да се работи со истите со поголемо внимание. Сето тоа ја наметнува потребата од почитување на законските прописи кои го наложуваат тоа, како и преземање на мерки за подигнување на безбедносната свест, како што се: почитување на воспоставените безбедносни политики и процедури, почитување на администравните и безбедносните зони, пријавување на сомневања за

безбедносни нарушувања итн. Тоа значи дека информациите мора да бидат достапни исклучиво на лицата кои поседуваат безбедносен сертификат кој е документ кој овозможува физичките или правните лица да имаат право на пристап и користење на класифицирани информации во извршувањето на работните обврски, потоа, да се почитуваат пропишаните мерки за безбедност на класифицирани информации и одржување на тајноста на информацијата и нејзино ограничување од слободна циркулација во јавност. Во овој процес важна улога има Дирекцијата за безбедност на класифицирани инфорамции како институционална основа за имплементација на системот за заштита на класицифицирани информации.

Користена литература:

1. Закон за класифицирани информации (10 фев. 2004)
2. http://www.dbki.gov.mk/
3. Татјана Г. : Корпоративна безбедност. 2017
4. Прирачник за оспособување и полагање на стручен испит за вршење на работи за физичко обезбедување: стр.4. 2013
5. Уредба за физичка безбедност на класифицирани информации (16 ноем.2004)