АНАЛИЗ НА ЕМПИРИЧНО СОЦИОЛОГИЧЕСКО ИЗСЛЕДВАНЕ (ЕСИ)ЗА ПРОУЧВАНЕ НА ЕКСПЕРТНО МНЕНИЕ В ОБЛАСТТА НА ЗАЩИТАТА НА ИНФОРМАЦИЯТА

Проф. д-р Иво Великов

Варненски свободен университет „Черноризец Храбър“

Резюме: *ЕСИ от 25 въпроса, свързани с политиката по защита на информацията. Има за цел да провери нивото на развитие на тази политика в различни организации, подготовката на персонала, изградените системи за защита на информацията и използвани методи за защита.*

Ключови думи: *Защита на информацията, емпирично социологическо изследване, изследвани фактори, анализ на риск, методи за защита на информацията, обучение, тренинг, нормативна основа в областта на защита на информацията*

ANALYSIS OF EMPIRICAL SOCIOLOGICAL SURVEY (ESS) FOR EXAMINATION OF EXPERT OPINION IN THE FIELD OF INFORMATION PROTECTION

Prof. Dr. Ivo Velikov PhD

Varna Free University “Chernorizets Hrabar”

Summary: *Empirical sociological research (ESI) of 25 questions related to information protection policy. It aims to check the level of development of this policy in various organizations, staff training, information protection systems in place and protection methods used.*

Keywords: *Information protection, empirical sociological research, studied factors, risk analysis, methods of information protection, training, coaching, regulatory framework in the field of information protection*

Настоящето ЕСИ е създадено и проведено като фокус-анкета, с извършен подбор на анкетираните лица, от предварително определена целева група, съобразно тяхната доказана експертиза по темата на анкетата, практикуващи професия или занятие с определени ангажименти в областта на ЗИ, със завършено висше образование, с позиции на експерти, преподаватели и ръководители, които имат отношение към ЗИ. ЕСИ беше проведено в периода 2019 – 2020 г.

Имаме представата, че такива хора са налични в множество организации и институции, поради което подбираме по няколко респондента от различни такива, но с преобладаващи като брой представители на ДКСИ и КЗЛД, двете комисии с безспорно най-важна роля в своите системи за ЗИ. Сред останалите респонденти – служители на МВР, на институти на БАН, преподаватели в университети, и дори в частния сектор. Общо 32 лица.

Обработването на резултатите е напълно стандартно, някои от въпросите обаче са използвани за прилагане на други експертни техники, напр. „Анализ на недопустимата разруха“, „Анализ на неочакваните алтернативи“, и „Анализ: Какво…, ако…?“[i]

Настоящата анкета има за цел да определи степента на защитеност на информацията във водещи или най-малкото организации с налично количество защитена информация и експерти с ангажимент в тази сфера. Изследването е провокирано от необходимостта от повсеместни мерки от страна на физически и юридически лица, държавни органи, органи на местната власт, частни организации и смесени такива, за защита на важната за тях информация. Не се стремим да правим разлика между класифицирана информация, лични данни, обществена информация или друга (напр. търговска тайна по ЗЗТТ от 2019 г.). Необходима е експертната оценка за общото ниво на изграждане на система за защита на информацията, състоянието на нормативната уредба, подготовката на длъжностни лица.

Изследваните фактори в това ЕСИ засягат в последователност:

- **Личността на анкетирания** – предпочели сме лица със значителен професионален и трудов път, с достатъчно житейски опит, но има и млади хора, което поради характера на самата работа (б.а. - ЗИ) е напълно естествено. Описанието на този фактор е чрез 4 въпроса в самото начало на анкетата;

- На второ място, непосредствено след първите 4 въпроса е изследвана **средата за сигурност от гледната точка на ЗИ**. В рамките на 5 въпроса (от № 5 до № 9 вкл.) се разглежда нивото на развитие на информационните технологии у нас, състоянието на нормативната уредба и нейното познаване от респондентите. Имаме предвид, че това все пак са лица със значителен опит и познания в тази сфера и те биха показали реалното състояние на тази дейност, при това разглеждайки я обективно и за състоянието на ЗИ за цялото българско общество и различните му структури;

- Въпросите от № 10 до № 16 са посветени на **състоянието на ЗИ в организациите и структурите, в които нашите респонденти работят**. Отделихме 7 общо въпроса на този фактор, някои от които с възможност за повече от един отговор. Нашата идея е да бъде направена многомерна, многопластова и обхватна картина на състоянието на ЗИ в съвременните български правни субекти;

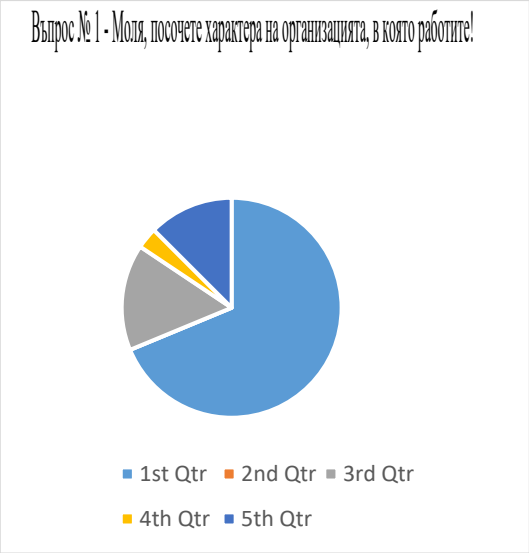
- Въпросите от № 17 до № 20 изследват фактор **„Ниво на конкретна и целенасочена лична и организационна подготовка в областта на ЗИ“** сред анкетираните. Чрез изследване на познаването на терминологията, заплахите в областта на ЗИ, наличието на експертиза въобще в организациите, да се достига до представата за вниманието и ресурсите, които те отделят за да защитават важната за тях информация;

- Въпросите от № 21 до № 24 включително ни помагат да оценим **методите за защита на информацията в организациите**, които са приети и познати на респондентите. Поради естеството на това научно изследване не задаваме въпроси, т.е. не задълбаваме в техническата и технологичната страна на ЗИ. Въпросите касаят социалния и управленски аспект (възглед), който организациите притежават или биха възприели за собствената си информация;

- Последният въпрос № 25 не принадлежи към никой от изброените 5 фактора, които сме поставили за цел на ЕСИ. Чрез него се стремим косвено да разкрием доколко изненадваща или необикновена е била самата анкета за анкетираните лица, но и пряко – колко често са имали възможност да се замислят или да срещнат идеи в тази проблемна област – ЗИ.

Фактор № 1 – Личност на анкетирания

Въпрос № 1 - Моля, посочете характера на организацията, в която работите!



ОТГОВОРИ

- държавна администрация - 22

- местна администрация - 0

- частна организация - 5

- свободна професия - 1

- друга (посочете каква) – 4

Общо: 32 лица

Заб.: Цветът на текстовете на отговорите съответства на полетата на чарта!?

Фиг.1

Вече беше споменато, че сред анкетираните има значителна част респонденти от ДКСИ и КЗЛД, поради което преобладават държавните служители. Тяхното присъствие е оправдано и поради факта, че класифицираната информация, лични данни, защитена обществена информация и голяма част от търговските и други тайни са собственост на държавата (публична собственост) и дотолкова, доколкото и други организации разполагат с тях, те са повече ползватели по повод на тяхната работа, но основната грижа за създаването, правилното използване, съхранение, унищожаване и защитата на информацията е държавна задача. Хората от частни организации и „други“ – напр. университети и свободна професия (общо 10), просто допълват общата картина, но и там също има необходимост от експерти и от защита на важната информация.

Фиг. 2

Според длъжностите на анкетираните, имаме повече хора, които са непосредствено заети с дейността, но и достатъчно такива на ръководни длъжности в съответната система за ЗИ на своята организация. Отсъстват специалисти (имаме предвид според класификатора на длъжностите у нас), което означава, че имаме достатъчно високо образователно ниво на анкетираните, и едновременно с това двете групи на експерти са най-многобройна част, съответно и с достатъчно перспектива за развитие.

Фиг. 3

Смятаме, че разпределението на анкетираните лица според възраст и житейски опит позволява извод за достатъчно зрялост и натрупана квалификация, но и достатъчно добра перспектива и възможности за развитие в кариерата, с оглед и на високото образователно ниво, видно от предходния въпрос. Като имаме предвид нарастващата възраст на трудова активност (вече 65 години за мъже и с тенденция да расте), то и лицата над 50 години не са лишени от перспектива пред себе си. Логично е и отсъствието на анкетирани под 25 години, експертите в областта на ЗИ, една специфична и високо професионална дейност, не е особено вероятно да бъдат толкова млади. Тук не става дума само за умения в областта на информационните технологии, където има достатъчно млади и висококвалифицирани лица, но повече за изградени навици, съзнание за сигурност и отговорност като служители в такава сфера. Тези качества, дори и при висока квалификация, не се придобиват лесно и в първите години на трудовия стаж.

Фиг. 4

Отново виждаме добрият опит и потенциал на анкетираните. С оглед на този факт, смятаме, че съществува високо ниво на компетентност сред респондентите, поради което можем да приемем усреднените резултати от ЕСИ с голяма степен на увереност.

В нашия случай, профилът на „средния“ респондент изглежда по следния начин приблизително:

- Държавен служител;
- Със завършено висше образование;
- На експертна или длъжност по-висока от експертна;
- Около 20 години трудов стаж, вкл. в областта на ЗИ, но и с достатъчно дълъг трудов път пред себе си;
- На възраст между 45 и 48 години (колкото и условно да изглежда присвояването на възраст).

След горния „портрет“ на нашия респондент имаме основание да се доверим на получените резултати от анкетирането им.

Фактор № 2 – Средата за сигурност при политиките по ЗИ

5 въпроса (от № 5 до № 9 включително)

Фиг. 5

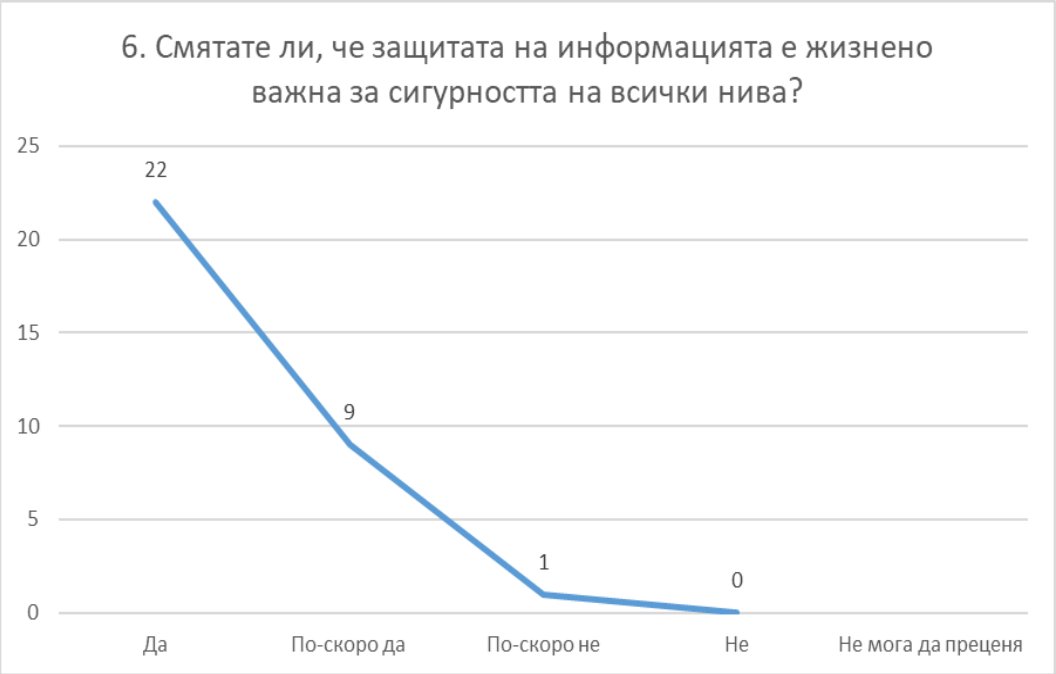
От 32 отговора 24, или 75% са позитивни, че сме на прага на информационното общество. Вероятно повечето отговори „по-скоро да“ се дължат на колебанието на респондентите по отношение на критериите за „информационното общество“, т.е. какви и кои трябва да бъдат показателите за такова качество. По спомени от други подобни анкети, критериите се градят върху мястото и ролята на информационните технологии в живота на обществото. Очевидно при все повече услуги, повече възможности и дори ежедневна трудова дейност онлайн (пандемията от Ковид 19 катализира подобни процеси навсякъде), имаме позитивни отговори на този въпрос. Дори без да се познават критерии за причисляване към такова общество, интуитивно нашите респонденти дават очакван и правдоподобен отговор.

По отношение на световните тенденции, държавите и народите с напреднало информационно общество не са толкова много, т.е. все още обществата са предимно аналогови, но дигитализацията във всички сфери неотклонно и все по-бързо ни води към такова развитие. Разбира се, че това явление е прогресивно и отваря нови възможности, особено в държавното управление, но също така крие в себе си достатъчно опасности за атаки и посегателства срещу държавни структури и дори срещу цели държави (припомняме само за атаките срещу Естония, една силно цифровизирана страна, и Италия през периода 2006 – 2008 г., когато кибератаките бяха преодолени и отблъснати с непосредствената намеса на НАТО).

Ето и малко допълнителна фактология по този въпрос: През април и май 2007 г. става ясно, че дигитални активисти от руската диаспора са готови да поставят Естония на колене и в рамките на два месеца не просто да осакатят страната, но и да нанесат нечувани последствия върху нейното управление и начин на живот.

Руските хакери удрят с такава сила, че и до днес в историята на Естония точно тези два месеца ще бъдат представяни за един абсолютен интернет тероризъм. Благодарение на успешните атаки, повечето транспортни услуги, търговски и правителствени операции са спрени. Естонските пристанища се затварят, а тогавашния военен министър Жак Авиксо ще наблюдава неоспоримия успех на хакерите. По това време в Естония има твърде малко защити, защото това е все още нова технология, която тепърва трябва да се опознава. Това ще мотивира правителството бързо да потърси съдействието на специалисти от Финландия, Германия, Израел и Словения, които да върнат

работата на компютърните мрежи. Именно тази атака поставя и нуждата от европейска и международна охранителна агенция на интернет. На първо място се забелязват тежки удари и така наречените DDoS атаки – претоварване на сървъри, които не могат да предоставят обслужването на клиенти, ping атаки и още много други. Според изследването на изпратените специалисти, това е била планираната първа вълна, а след това се очаква и втора, която да бъде още по-жестока. Едва през 2008 г. Естония ще осъди Русия за тези действия. По време на разследването ще стане ясно, че това е дело на Сергей Марков, депутат от руската Дума, който също има участие във въпросната хакерска атака.[ii]



Фиг. 6

Категоричността на дадените отговори (над 70% твърдо „да“ и 26% „по-скоро да“) дава ясна представа, че ЗИ в организациите, където нашите респонденти работят, се приема като първостепенна и „жизнено важна“ задача. Вероятно и без А.Тофлър (б.а. – имаме предвид „Третата вълна“[iii]), е очевидно, че в информационната епоха основната стока и основна ценност ще

бъде информацията. И не е достатъчно само да я притежаваме или използваме, абсолютно необходимо е да умеем да я защитаваме от посегателства. Както се вижда от този труд, посегателства се случват непрекъснато, източниците на заплахи са много и дори стават повече, а ефективна ЗИ става все повече скъпа и отговорна задача за всякакви субекти, вкл. и за отделния човек.

Фиг. 7

В този въпрос и получените отговори има малка изненада. Нашите респонденти са хора с експертиза в областта на ЗИ и въпреки, че повечето отговори (18 бр. от общо 32) са позитивни, т.е. познаваме нормативната основа, има обаче и близо 30% (по-точно е 28%), които твърдят, че нормативната база не се познава. Нещо повече, има 5 отговора, съответно 16 % от анкетираните, които не са сигурни на практика, че нормативната база се познава. С други думи, делът на колебаещите се и негативно настроени експерти относно познаването на нормативната основа на ЗИ надхвърля 40% стабилно и е близо до половината от анкетираните (44%).

Изброените няколко закона и стандарт използвахме с идеята да подскажем, че в областта на ЗИ имаме някакъв краен брой нормативни актове и те могат да бъдат опознати, вкл. и такива на по-ниско ниво. Точно обаче хора, които имат ангажимент към ЗИ смятат, че масово обществото има проблем с тази материя. Това положение не може да не буди тревога. След близо 5 години в ДКСИ отчитаме, че има множество случаи на отнемане на достъпа на Служители по сигурността на информацията, т.е. на хора, които по принцип имат като функционален ангажимент/длъжностна характеристика да познават нормативната основа на ЗИ, да изграждат ведомствена система за ЗКИ и да ръководят тази система. Като изключим един случай, всички останали отнемания се случваха поради ниска компетентност и неизпълнение в пълен обем на изискванията на ЗЗКИ (в БДЖ, в ОДМВР, в общини и т.н.). Имаме и достатъчно случаи на отнемания на РДКИ на Ръководители на организационни единици по смисъла на ЗЗКИ, напр. в НОИ – Силистра, В и К Монтана, на директори на служби за сигурност и т.н. с други думи, точно хора, които трябва да познават най-добре ЗЗКИ и да защитават държавните тайни, са пренебрегвали тази задача.

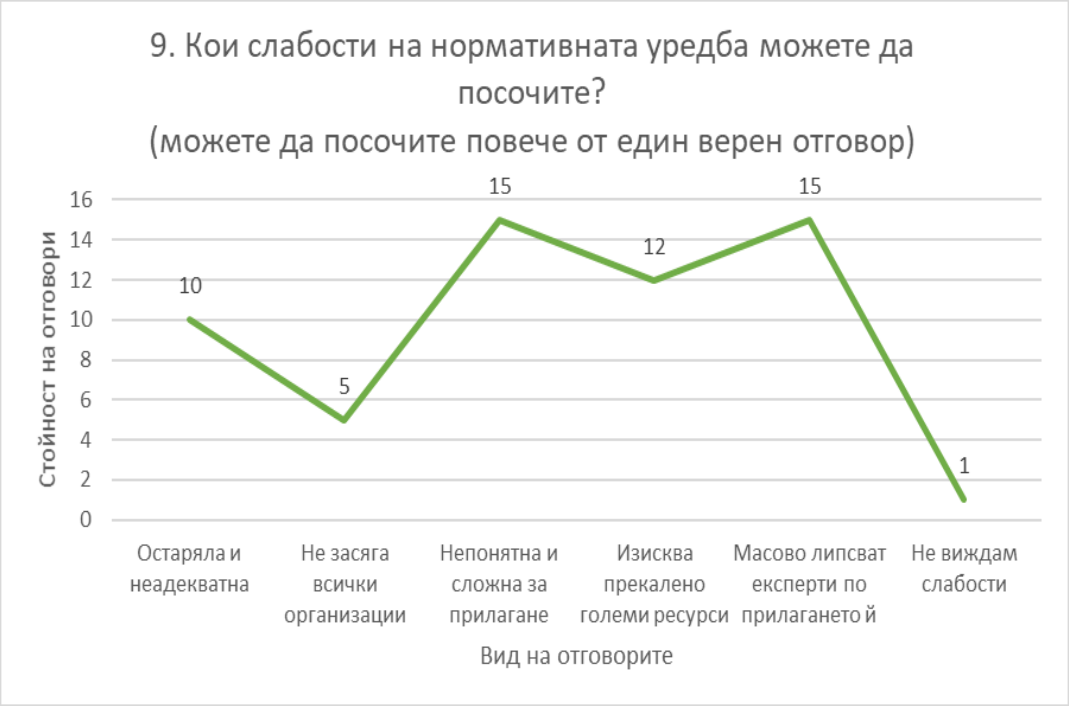
В различни разговори и при различни случаи, е ставало въпрос за средното ниво на подготовка на българина в областта на националната и корпоративна сигурност. ЗИ е точно такъв показател. Вероятно като участник в Студената война, България десетилетия наред е подготвяла своите граждани да пазят информацията. Но вече 30 години и в условията на взривното развитие на информационните технологии и социални мрежи, изглежда не сме в състояние да се справим с това предизвикателство. Съвсем доскоро повечето колеги в системата за национална сигурност смятаха, че у нас има готовност за защита на класифицираната информация, т.е. налична е подобна нагласа или по-скоро обществена култура, но това положение (особено при отсъствието на наборна военна служба за младежите) се променя очевидно бързо. Нещо повече, смятахме, че няма култура по защита на лични данни (пак по причини на Студената война), но промените в тази система от 2016 г., влезли в сила през 2018 г. за всички страни-членки на ЕС, показаха доста високо ниво на държавен, обществен и частен интерес към подобни политики.

Този въпрос ни създаде доста многопосочни и различни теми за размисъл, както и възможни различни коментари. Раздробените отговори, без някакъв особено отличаващ се сред тях, показват и колебания сред респондентите. Въпреки различните отговори, приемаме създадената картина за достоверна, т.е. нашето общество има какво да развива и подобрява в тази област.

Фиг. 8

Отново има почти пълен паритет между позитивните от една страна, и колебливите или направо негативни отговори, от друга. Нашите респонденти по равно ни представят една не дотам оптимистична картина, по подобие на предходния въпрос. Т.е., като имаме предвид общо последните два въпроса, у нас имаме както накъде да развиваме нормативната си уредба в посока на нейното по-адекватно състояние, така и самите ние да сме по-добре запознати с нея. Това ни казват анкетирани, които имат познанията и качествата да правят подобна оценка, най-вече поради факта на самия техен целенасочен подбор от наша страна.

Следващият въпрос № 9 завършва този критерий, свързан с оценката на националната среда. Имахме колебание за него, т.като той само доразвива и доуточнява въпрос № 8. Би могло да се каже, че той стои малко конюнктурно и просто засилва ефекта на предходния въпрос. От друга страна обаче, изброяването на слабости в него ни насочва към обективния поглед на множество експерти, т.е. не може да подминем величината и стойността на някои отговори в него (още повече, че даваме възможност респондентите да посочат повече от един верен отговор).



Фиг. 9

Общият брой на отговорите тук е 58, т.е. почти всеки от анкетираните лица е намерил и втори подходящ отговор по отношение на проблемите в нормативната уредба. Веднага прави впечатление ниското ниво на два от отговорите (5 отговора за „Не засяга всички организации“, и само един, който не вижда слабости). По този начин става ясно, че нашите респонденти смятат нормативната основа на дейността като масово приложима и полезна (още повече, че във въпрос № 7 посочихме някои от прилаганите и налични актове в областта на ЗИ, т.е. те бяха ясни). Също така, самият характер на въпроса по принцип не е насочен към последния отговор (б.а. – Не виждам слабости). Вероятно отговорилият по такъв начин е дал само този отговор и от 32 лица е само един, т.е. всички други са отправили достатъчно критичен поглед и оценка към състоянието на нормите в тази сфера.

Самият характер на въпроса обаче не предполага този отговор, при големия избор на други и по начина на задаването си. Поради този коментар не смятаме, че трябва да се прави трагедия от единствения позитивен отговор на въпроса.

Много по-важно обаче е да насочим вниманието си към трите отговора с най-висока и почти равна стойност. Отсъствието на експертиза и сложността за прилагане на материята са два отговора, които си кореспондират. За нашите анкетирани лица двата отговора имат еднаква стойност (най-висока). Заявяваме неведнъж в това изследване, че ЗИ изисква комплексна експертиза в областта на информационните технологии, на сигурността, на управлението в социалната сфера, на психологията и т.н. високото ниво на тези два отговора доказва нашата теза – специалисти и експерти в областта на ЗИ се изграждат трудно и не се намират лесно.

Що се касае до високите изисквания на ЗИ към ресурсите (в оригиналния въпрос на анкетата при този отговор дори сме изброили – „човешки, финансови, материални“ ресурси, този проблем е също с висок приоритет (12 отговора), но той по ред причини не е неизвестен, не е невероятен и с този отговор не откриваме нищо ново. ИТ са скъпи, прилагането им често е свързано с обществена поръчка или аутсорсинг на дейности[iv], обслужването е скъпо, остаряването на техниката е на практика мигновено и след 2-3 години вече има нужда от съществено обновяване. Самото изграждане на една ведомствена или корпоративна система за ЗИ също не е лека задача, изисква време и експертиза, които не всеки субект може да си позволи.

Нещо повече, работейки 20 години в АМВР, имахме идея да потърсим от близкия до нея Бизнеспарк – София излезлите от употреба компютри. По наша информация водещите компании в ИТ сектора (там се намират офиси на IBM, Hewlett Pacard и др.) сменят компютърната техника и софтуер веднъж на всеки три години (а офис мебелите веднъж на 5 години). На нас, в държавната структура, тригодишните компютри ни се струваха супер нови и модерни. А всъщност тази идея е показател за съществен проблем – в държавните структури няма възможности за модернизация на софтуера и хардуера по начин, който да гарантира ЗИ, търсят се разни варианти „на парче“, което си е компромис със сигурността. Т.е. изтеклите данни от НАП и Агенция по вписвания вероятно няма да са единствени случаи.

При всички случаи обаче, отговорите … „В) непонятна и сложна за прилагане; Г) изисква прекалено големи ресурси – човешки, финансови, материални; и Д) масово липсват експерти за прилагането ѝ“…, са изключително важни за нашата оценка на средата в областта на ЗИ. От анализа на отговорите в този втори фактор следва:

- Българското общество вероятно е на входа на информационно общество (иска или не иска), каквото и да означава това към настоящия момент;

- Нашето общество притежава съзнанието, че ЗИ е важен (най-съществен) елемент на сигурността въобще;

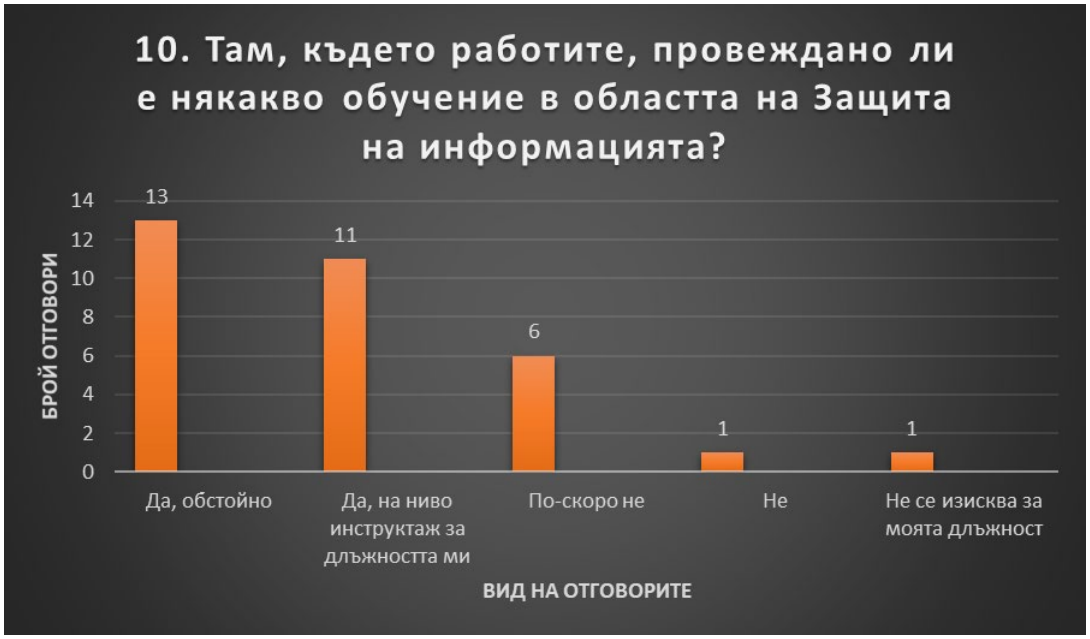
- В нашата страна има определено средно ниво на познаване на нормативната основа на тази дейност, т.е. не сме лишени от експерти, но те не са достатъчно за всички системи, които имат нужда от такива;

- Нормативната основа поддържа също определено среден стандарт на адекватност със средата за сигурност. Има много насоки, в които да се работи за нейното развитие;

- Най-малко три насоки основно виждат нашите респонденти за промяна на нормативната основа на дейността – обучение на експерти и улесняване на прилагането, както и облекчаване на отделените ресурси в тази сфера.

Следващият критерий, който изследва състоянието на ЗИ в организациите на нашите анкетирани лица, се изследва чрез 7 въпроса:

Фактор № 3 - Състоянието на ЗИ в организациите и структурите.



Фиг. 10

При този въпрос има приятната новина, че в 75% от структурите и организациите е имало обучение, при това можем да твърдим – достатъчно съобразено с необходимостта на конкретната длъжност.

Нещо повече, формалният отговор „по-скоро не“ при този въпрос е по-близък до „по-скоро да“, отколкото до напълно негативния. Т.е. смятаме, че дори и хората с такива отговори имат някакво обучение, може би недостатъчно, или без необходимото ниво на компетентност от страна на обучаващия орган/работодателя, но и вече видяхме при предходния изследван фактор, че експертите не са налични навсякъде, нито са всички на достатъчно високо ниво. Единствено последните два отговора отхвърлят каквото и да е обучение, инструктаж или просто запознаване с изискванията на ЗИ. Те представляват обаче едва 6 % от анкетираните, напълно е възможно да заемат в момента такава длъжност, или просто да не осъзнават изискванията на информационната епоха относно ЗИ.

Като цялост обаче, отговорите създават представа за отговорност и осъзнаване на реалностите на съвремието от страна на организации и ръководителите в тях.

Фиг. 11

До този въпрос имахме непрекъснато колебания, доколко правилно е определена фокус-групата на анкетата. Очевидно е вече, че изборът е бил правилен – подбраните респонденти са осведомени лица с достъп до множество факти и данни, които са обект на защита от широк достъп, поради своята несъмнена стойност. Защитената информация съобразно трите закона у нас – ЗЗКИ, ЗЗЛД и ЗДОИ е достъпна на практика на повечето от анкетираните. Като че ли достъпа до професионални тайни, оценен на 7% е малко изненадващо нисък. Вероятно се дължи на големия брой държавни служители, които имат представа от горните три закона, но съвсем по-малка от други актове и други професионални тайни – по ЗЗТТ, Закона за адвокатурата, по Хипократовата клетва за медици, тайната на осиновяването (издаването е наказуемо по НК) и др.

Широкият достъп до защитена информация се потвърждава от факта на 68 отговора при 32 анкетирани. Т.е. като изключим единствения отговор „Нямам достъп“, то останалите лица са дали по 2 или 3 отговора. Също очевидна е и комбинацията между трите най-често споделяни отговора, един от тях при всички случаи е комбиниран с друг от трите, просто нивото на процентите дава основание за такъв коментар на резултата. Това положение дава основание да твърдим, че нашите респонденти са експерти в областта на информацията и притежават компетентността, необходима за това изследване.

Фиг. 12

Двата позитивни отговора дори надхвърлят очакванията по отношение на полаганите усилия за изграждане на система за ЗИ в организациите. Общо 80% от анкетираните са дали отговорите „Да“ и „По-скоро да“.

За автора на анкетата е радващ и нулевия резултат при „Не мога да преценя“. Този отговор по принцип е най-нежелан при подобни анкети. Както се вижда от други въпроси, подобен отговор заменяме някъде с „колкото да, толкова и не“, но замяната не винаги е възможна и търсим по-правдоподобен за респондентите отговор. Отговорът „по-скоро не“ като стойност не трябва да се пренебрегва, но в случая може да се приеме, че някои усилия на организациите по изграждане на ЗИ просто не са известни или не са в кръга на известната информация на анкетираното лице.

Каквито и коментари обаче да правим, винаги ще имаме позитивното впечатление от организациите и структурите в нашата страна по отношение на изследвания в този труд проблем. Очевидно е също, че изследваните организации създават или поне правят опити своя специфична микросреда/микроклимат на внимание към проблема, на опити за развитие на политики, на насочване на енергия и ресурси за защита на ценната за тях информация. Разбира се, различните организации имат различни материални, човешки, експертни и битови условия, изискващи различен и нестандартен поглед, но полаганите усилия рано или късно ще имат своя положителен ефект върху резултатите. Линията на тренда, т.е. тенденцията има изключително благоприятно разположение и насока, с оглед на получените отговори.

13. **Какво знаете за системата за защита на информацията във Вашата организация? (отговорете на всеки от зададените въпроси с един от отговори да/не след въпроса)**

Въпрос		
Познава се нормативната уредба в тази област	**Да** **27**	**Не** **5**
Издадени са вътрешни актове на ръководството, определени са планове, процедури и механизми за защита	**Да** **27**	**Не** **5**
Имаме назначени отговорни лица, експерти и консултанти	**Да** **29**	**Не** **3**

Имаме контролни органи за защита на информацията	**Да** **25**	**Не** **7**
Персоналът е обучен/инструктиран	**Да** **25**	**Не** **7**
Имаме някаква подобна система	**Да** **17**	**Не** **3**

Фиг. 13

Поради простотата на отговорите си, въпрос № 13 не изисква чарт или диаграма за представяне на резултатите. С този въпрос допълнително се изяснява характера на полаганите грижи за ЗИ (поставен в предходния въпрос № 12). Прави впечатление, че последното твърдение (б.а. – почти изключващо предходните 5, поставено с идеята, ако някой не е съвсем наясно или няма информация за тези твърдения, да покаже, че все пак има полагани някакви минимални грижи по проблема в неговата организация) е възприето като несъвместимо с останалите и не всички анкетирани лица са отговорили. Т.е. при отговори в порядъка на 75 до 90 % позитивни, част от респондентите се въздържат от последното твърдение, което разпознават като неприемливо на фона на останалите.

В цялост обаче, картината от въпрос 12 се изгражда доста логично. След позитивните отговори там от 80%, тук имаме повторение на голямата част от 5-те твърдения с много близък и дори по-висок резултат. В този смисъл приемаме за доказано, че на прага на информационното общество, организациите и структурите на наша територия обръщат значително, многопосочно внимание към ЗИ.

Съвсем леко противоречие, вероятно и поради близостта на въпрос № 12, намираме при сравнение на първото твърдение от въпрос № 13 и въпрос № 7, където познаването на нормативната уредба е оценено малко над 55%. Приемаме, че такова е мнението на нашите респонденти по отношение на външни и други организации, докато тук става дума за техните собствени, и така се проявява тази значима разлика. А че се познава нормативната уредба става ясно от следващите твърдения – създадената е необходимата вътрешна уредба на дейността по ЗИ, има разпределени отговорности сред длъжностните лица, ясни са контрольорите на системата, провеждат се необходимите обучения и инструктажи на персонала.

В този фактор следват три въпроса, които могат сами по себе си да бъдат обособени в отделна подгрупа – „Изследване на състоянието на

организациите в условия на заплаха за сигурността на информацията“. Поставихме ги тук, т.като все пак става дума за собствените организации на анкетираните лица.

Фиг. 14

С този въпрос изследваме собствен негативен опит и практики сред анкетираните. С оглед експертизата им, очаквахме минимум 50% от тях да познават или да имат представа за случаи на неоторизиран достъп до важна информация. На практика под 20 % са сигурни, че имат знание за подобен случай, и под 40 % общо потвърждават, че имат представа, без да са наясно с подробностите. 2/3 от нашите респонденти нямат опит с нанесени поражения от достъп до информация за тях или тяхната организация от външни лица.

Тези отговори са в известна степен изненадващи, още повече, че медиите непрекъснато тръбят за фалшиви новини, хибридни атаки срещу държавни и общински учреждения, изтекоха множество данни за българските граждани в следствие на пробиви в НАП, в Български пощи, пред банки и Съдебна палата бяха изхвърляни различни документи, имаме скандала с шпионите на Русия и т.н. Твърде вероятно е подобни вреди да са косвени, нямат пряко отражение върху анкетираните лица, но тяхната експертиза

вероятно трябваше да подскаже сериозната опасност от незащитена важна информация.

Т.е. очаквахме по-развито чувство за самосъхранение и професионален инстинкт.

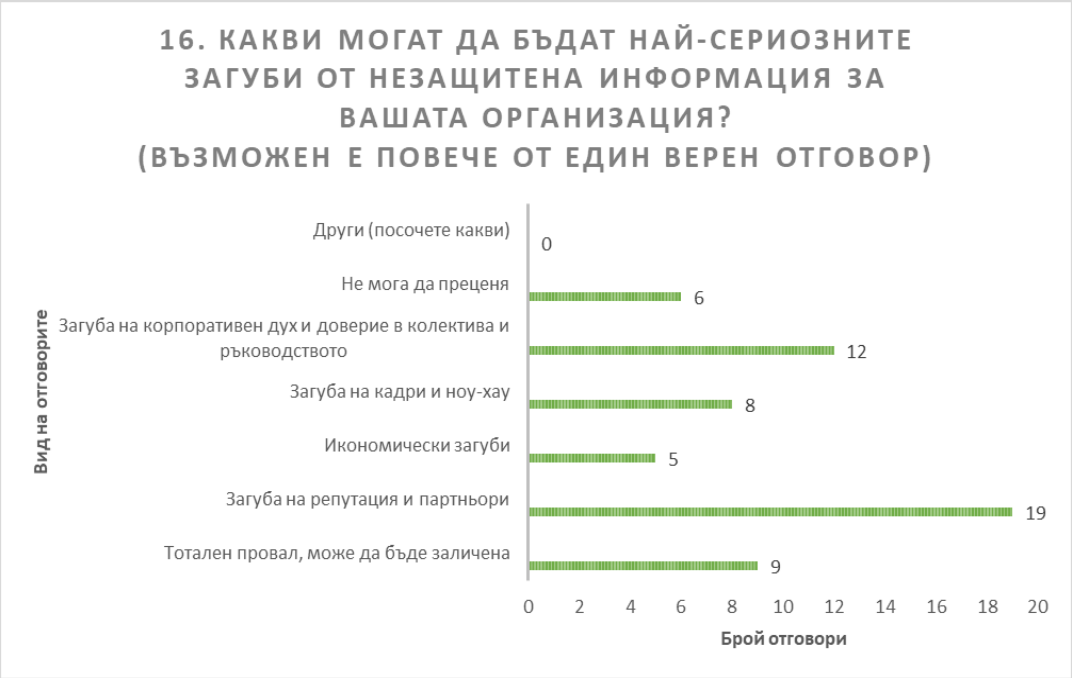
Фиг. 15

В унисон с отговорите на въпроси №№ 12 и 13 от този изследван фактор, около 70 % анкетирани смятат, че организациите имат потенциал за справяне със заплахите за сигурността на информацията. Отново във връзка и по логиката на предходните въпроси, след като твърдим, че се познава нормативната уредба, създадена е подходяща вътрешно-организационна система, приемаме и отсъствието на отговори за никакъв ресурс като нормално и закономерно.

Трябва да обърнем конкретно внимание обаче на отговорите „по-скоро не“. Те са 30 % от всички отговори, и като количество не трябва да се подценяват. Вероятно част от респондентите свързват този отговор и с предходния въпрос № 14, и отсъствието на опит от нанесена вреда при изтичане на информация. Но въпреки това, този отговор на несигурно отрицание е двойно по-висок от отговорите „да“, т.е. категорично да се

твърди, че организациите имат ресурс, и съизмерим (точно 60%) от „По-скоро да“ – несигурният позитивен отговор.

Като извод от анализа на въпроса – само 5 отговора са убедителни (в случая „Да“) останалите 27 (над 80%) изразяват несигурността на анкетираните по този въпрос.



Фиг.16

Този въпрос съзнателно предложихме с най-много отговори и възможност за повече от един верен отговор. По този начин има възможност да се избегнат колебания сред анкетираните относно най-важните загуби, или да бъде изпусната от нас сред отговорите някоя възможна или често срещана. Общо отговорите са 59, повечето от анкетираните са посочили и втори отговор има вероятно 2 случая и на три отговора, т.е. на практика над 90 % от тях имат идеята за многообразно влияние и различни загуби от изтичане на информацията. Можем да приемем също, че шестте отговора „не мога да преценя“ са единствените, които 6 лица са подали (не е логично да мислим, че при този отговор е бил посочен и друг). Като стойност обаче са пренебрежими с оглед на повечето отговори.

Никой не се опитал да посочи някой изпуснат от нас отговор, т.е. да допълни отговорите, за което беше дадена такава възможност. Поради което приемаме, че сме изброили възможните загуби сравнително изчерпателно.

Също пренебрежими с оглед на общото количество отговори са „икономическите загуби“. Т.като въпросът е зададен относно „най-сериозните загуби“, то вероятно нашите респонденти намират икономическите загуби за най-малкото, с което организацията ще пострада. Т.е. останалите 4 отговора са много по-вероятни, много по-сериозни и с повече последствия.

Отговорите „тотален провал…“, „загуба на кадри и ноу-хау“, „загуба на корпоративен дух и доверие…, съответно със стойности 9, 8 и 12 отговора, на практика са съизмерими и образуват група на наистина сериозни следствия от загубата на незащитена информация. Нещо повече, организацията би могло да изчезне или да фалира и вероятността е около 1/6, от порядъка на 15 процента. Нашите наблюдения върху системата за национална сигурност показват, че провали в служби за сигурност и обществен ред (особено проникване на чужди специални служби и влияние на организирани престъпни групи), са предизвиквали най-сериозните организационни, функционални и структурни промени, т.е. вътрешен катаклизъм, който дори да доведе до унищожаване на организацията най-малкото в досегашния си вид и управление. Нещо повече, изтеклите публикации за действията на структурите за сигурност и обществен ред в САЩ по линия на актовете от 9/11 доведоха до толкова сериозно преструктуриране на тази дейност, че се създаде ново Министерство на териториалната сигурност с 200 хил. служители (б.а. – най-голямата реформа в държавната администрация на тази страна след Втората световна война).

„Загуба на кадри и ноу-хау“, „загуба на корпоративен дух и доверие…,“ не са на пръв поглед толкова фатални, но тези загуби са продължителни във времето, преодоляването им е свързано с много усилия и също може да завършат по подобен начин. Изтичането на информация за проблеми с ваксината на „Астра Зенека“ автоматично нанесе огромни щети на компанията, и то не само с Ковид ваксината.

Най-масовият отговор е с 19 отговора, на практика 1/3 от всички и се отнася до загуба на репутация и партньори на организацията. В интерес на истината, нашата предварителна нагласа беше, че това ще е най-масовият отговор. Независимо какво ще се случи, какво ще е нивото на другите загуби,

загубата на репутация и партньори като че ли винаги е гарантирана. И няма значение дали става дума за органи на държавната власт, местното самоуправление, бизнес организации или НПО – такава загуба от изтичане на информация е гарантирана.

При този въпрос мога да бъдат използвани за прилагане и споменатите в началото други експертни техники, напр. „Анализ на недопустимата разруха“, „Анализ на неочакваните алтернативи“, и „Анализ: Какво…, ако…?“

Какво ще се получи, ако изтече информация за ноу-хау на организацията? Задължително ще загуби печалба, репутация и партньори. Вероятно най-прогресивните й кадри, с най-висока експертиза и умения ще бъдат подложени на изкусителни предложения от конкуренти и вероятно една част от тях ще преминат при конкуренцията. Задължителна е във времето загубата на доверие към управляващия екип, т.е. че не е в състояние да осигурят плавно и хармонично развитие на организацията. Дали може да доведе това състояние до масово напускане и фалит, на практика няма сигурен отговор, но също е вероятно или може периодът на страдание на организацията да продължи достатъчно дълго, да бъдат разходвани много средства за защита и пропуснати много ползи… И да се премине към кризисен мениджмънт, ситуация, която няма нищо общо с нормалната работа.

Коя би била недопустимата разруха? Вероятно за държавните структури – загуба на бюджета или орязване на бюджета, което е следствие от или причина за последващи кадрови и структурни промени, както и промени във функциите на организацията и мястото й в системата на държавната администрация.

Недопустимата разруха за бизнес организацията би могло да бъде изтичането на информация, с която организацията да загуби конкурентно предимство на пазара. Дали свързана с кадри, ноу-хау, производствени мощности, търговски връзки и доставки, всяка една организация трябва да пази важната за нея информация.

Недопустима разруха за една община спокойно би могло да се приеме отсъствието на подходяща заетост, обезлюдяването, постоянното намаляване на персонала на държавни служители и на местна власт (хора с гарантирана кариера, колкото и да е малка и гарантиран месечен доход). Закриването на РУП в една община автоматично я обрича на несигурност по отношение на

обществения ред. Закриването на училище и поща също. Така в страната има населени места без нито един държавен служител, дори без кмет… Как хората узнават за такива загуби в общината – чрез изтичането на информация!

От направените анализи на отговорите в този фактор, сме в състояние да направим следните изводи:

- ЗИ е приоритет на организациите в нашата страна и се провежда целенасочено обучение на персонала в тях;
- Нашите анкетирани са експерти със широк достъп до различни видове защитавана информация, което ни дава основание да претендираме за представителност на това ЕСИ;
- Организациите полагат грижи за познаване на нормативната уредба в областта на ЗИ, имат изградени вътрешни системи за защитата й, има длъжностни лица, вътрешни нормативни актове, както и контролни органи. В общия случай притежават и ресурси за реагиране при заплахи от изтичане на информация;
- Анкетираните имат неголям опит или познания относно нанесени вреди на организации и лица, в следствие на изтичане на информация;
- Анкетираните лица си дават сметка, че загубата на ценна информация може да доведе до множество загуби и дори до ликвидиране на организацията.

Фактор № 4 „Ниво на конкретна и целенасочена подготовка в областта на ЗИ“.

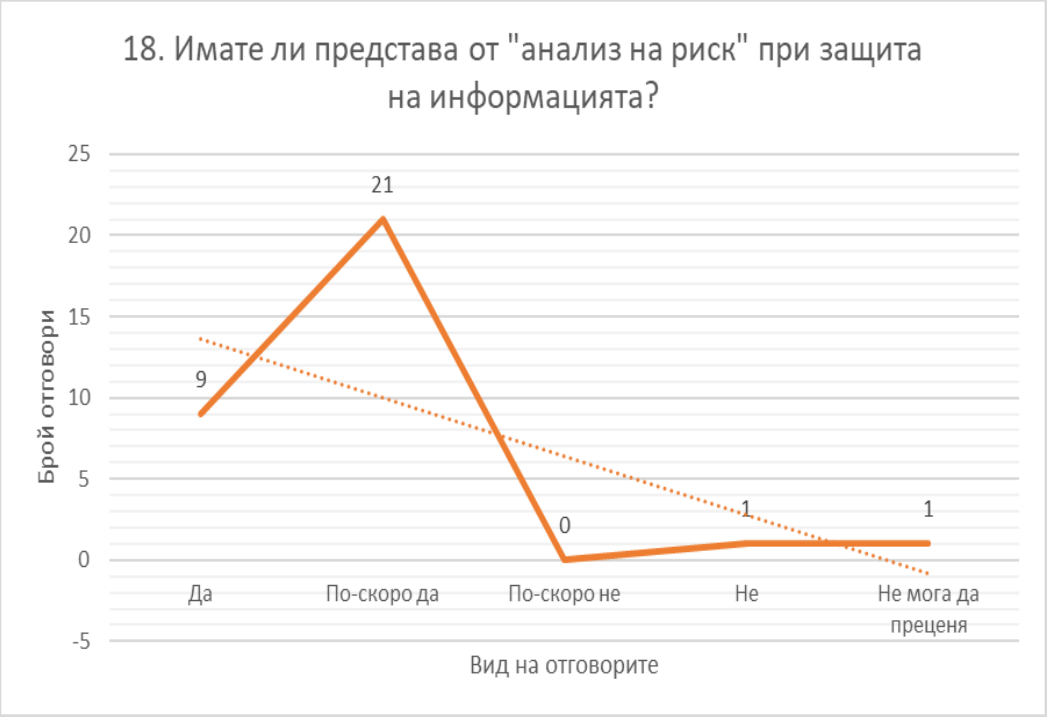
Въпросите от 17 до 20 реализират този фактор:

За следващият въпрос № 17 избрахме този вариант на чарт (б.а. – виж по-долу), защото демонстрира един достатъчно ясен уклон при отговорите – отговорът „по-скоро да“ сам е над 60% верен, а с твърдия отговор „да“ общо над 80%. В интерес на истината, през последните години навсякъде срещаме експерти, които говорят за заплахи, анализ на риска и др. модерни термини, поради което приемаме като напълно достоверно това ниво на представена подготовка при нашите респонденти.

Фиг. 17

По-несигурният, но силно подкрепен отговор дори приемаме като позитив (истинските експерти и специалисти се съмняват твърде често както в знанието си, така и в способностите си, още повече, че динамиката на средата винаги може да ни изненада, обратно самоуверени са слабо подготвени и ниско интелигентни хора). Този феномен, познат като „ефект на Дънинг-Крюгер“ вече сме разглеждали по-подробно. За целта просто прилагаме една популярна диаграма, свързана с него:

Става дума за онази вътрешна, присъща на индивидите склонност, при която неквалифицираните индивиди страдат от илюзорно превъзходство, поради което погрешно оценяват способностите си много по-високо от средното. Обратно, квалифицираните имат способността да подценяват експертизата си – просто са наясно колко много не знаят. Добър пример за подобен ефект е сравнението на лаиците срещу експертите – ако приемем, че лаикът притежава знания колкото една малка локвичка, то границата (крайбрежната ивица) с неизвестното също е малка. Т.е. той има доста тесен допир с неизвестното. Обратно експертът с добри познания има на разположение цяло езеро от такива, но така и крайбрежната ивица (границата с неизвестното) за него става много по-голяма. Така експертът има допир с огромно количество неизвестни за него познания, които го карат най-често да се съмнява много повече в себе си, отколкото лаикът. Състоянието е известно в науката и множество учени са подчертавали това очевидно противоречие, особено при вземането на важни решения.[v]



Фиг. 18

В синхрон с предишният отговор и с нашата представа за съвременните експерти, имаме убедително доказателство, че анализ на риска е както често срещано професионално понятие, така и напълно ясна теоретико-приложна концепция в съвременните организации. Разбира се, ситуацията с анализа на риска е по-вероятно да е ясна като теоретична концепция, особено в държавните структури, където по натиска на МФ и Системата за финансово управление и контрол в публичния сектор всички субекти създават Стратегии за управление на рисковете. В частните организации, особено в сферата на ИТ, корпоративната и вътрешна сигурност, тази концепция е повече практическа и по-често дори осъществявана. И приемаме и този отговор по линия на ефекта на Дънинг-Крюгер, т.е. хората масово отчитат, че средата е на практика непознаваема и винаги може да ги изненада.

Въпреки това отговорите са достатъчно убедителни и приемливи.

Фиг. 19

Анализът на риска анализираме с този въпрос от съвсем друг ъгъл. Ако в организацията, където работи нашият респондент има ССИ; началник на охраната; лице по защита на личните данни; системен администратор;, аналитик по развитие“; или аналитик по инвестиране или кредитиране, то той

задължително ще познава такова лице. Невероятно е в днешно време организациите и структурите да не притежават подобни фигури сред състава си. Тук процентите от 75, които са позитивни изобщо не са толкова важни за нашите изводи. 25 % негативни отговори (по-скоро не, не, не мога да преценя) са направо изумителна цифра, т.е. съществуват съвременни организации в нашата страна (б.а. – подчертавам), където някой няма понятие от анализ на риска, и не става дума за строителна бригада или селскостопански колектив (с цялото ми уважение към такива важни за страната ни организации).

ЗИ е толкова изискваща, толкова чувствителна и на практика мултилатерална система, че само едно слабо звено (както се оказва – такива има) може да я доведе до пробив, колапс или компрометиране. Тази особеност е в основата на нашите изводи по отношение на негативните отговори. В XXI век не би трябвало да съществува правен субект, който не е наясно с необходимостта от ЗИ. В държавните структури и структурите на местната власт задължително има екип/работна група/комисия, които съставят Стратегия за управление на риска за институцията (съгласно СФУКПС). Най-малко такива хора трябва да са известни на нашите респонденти. Финансовите органи винаги имат отношение към анализа на риска при разходване на финанси.

С горните 3 пасажа просто фиксираме съвременното състояние на анализа на риска. Той е на практика неотменима част от всяка съществуваща организация, от всеки правен субект. Поради което идва и нашето неразбиране на тези 25 % отговори.

Фиг. 20

Въпрос № 20 допълва и разширява № 19. Неговият смисъл бе да се види не просто длъжностното лице, което във въпрос 19 трябваше да съществува на хартия (поне), т.е. някой назначен и отговорен по длъжностна характеристика (независимо дали е компетентен), а дали наистина има експерт в тази насока, дори да не заема такава длъжност, но е показал достатъчно качества като такъв експерт.

Стойността на отговорите почти препокрива на 100% предходните от въпрос № 19. В този смисъл смятаме, че има някакво инстинктивно проникване на двата отговора, и вероятно идеята на въпрос № 20 не е правилно възприета. Експерт по анализ на риск може да има в множество направления, както отбелязахме по-горе, но тук се търси лице с профил в областта на сигурността и ЗИ, каквато е идеята на цялата анкета.

Ако обаче приемем за обективни дадените отговори, то отново при 75% от организациите имаме ясно подредена система, т.е. има длъжностно лице по анализ на риска (въпрос № 19) и има наистина лице с доказани качества и професионална подготовка по анализ на риска (въпрос № 20). Въпреки, че картината съвпада, то общият извод е по-скоро позитивен, т.е. нашите анкетирани лица познават експерт по анализ на риска и в множеството случаи той е и лице, което по длъжностна характеристика трябва да прави анализ на риска. Всъщност тази корелация не е задължителна, но е твърде вероятна, с оглед на невисокия брой експерти в тази област.

Отново отчитаме 25 % отсъствие на експерти по анализ на риска (отговорите „не“ и „по-скоро не“), но в този случай това не е изненада вече.

Отново нашите респонденти не дават нежеланият отговор „не мога да преценя“, което показва най-малкото отговорното им отношение.

Изследването на този Фактор № 4 „Ниво на конкретна и целенасочена подготовка в областта на ЗИ“ ни води в крайна сметка към следните изводи:

- В съвременните организации (можем да го твърдим със сигурност в процентно изражение между 75 и 80 %) си дават сметка за необходимостта от анализа на риск, в конкретния случай – свързано със ЗИ;
- Отново в същия процент и вероятност експертният състав има представа от анализа на риска;

- По принцип има назначени длъжностни лица, които имат в длъжностната си характеристика задачата да провеждат анализ на риска, и най-често тези хора имат и необходимата експертиза за това.

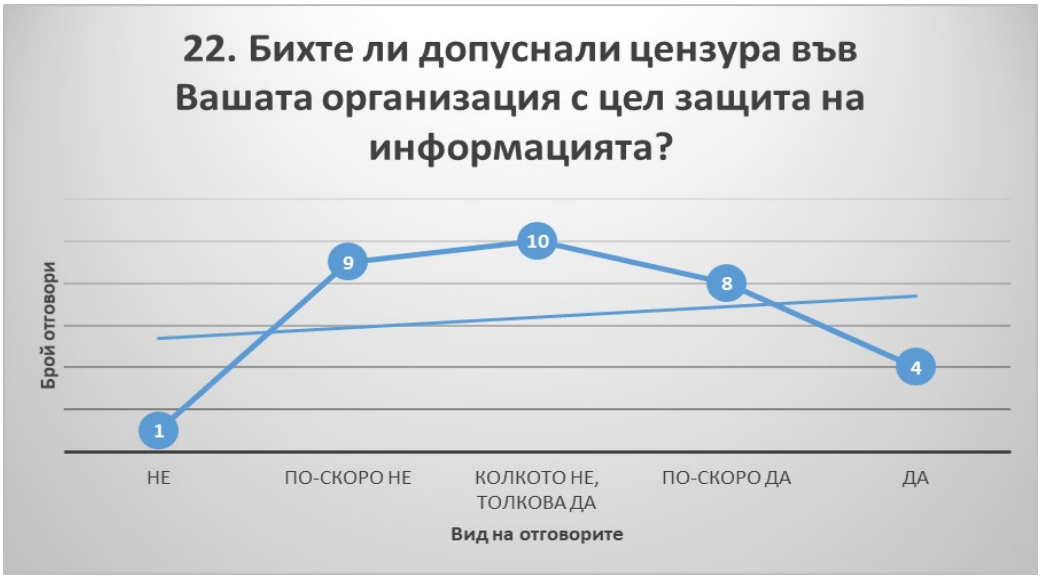
Фактор № 5 (въпросите от № 21 до № 24 включително) ни помага да оценим методите за защита на информацията в организациите. Не твърдим, че с 4 въпроса изчерпателно ще направим подобна оценка, напротив, смятаме, че методите могат да бъдат най-разнообразни (от самоконтрол при сериозни професионалисти, т.е. без активна намеса на управляващия екип в ЗИ, когато имаме високо подготвени колеги; до налаган със заповеди и стриктен контрол (буквално с „твърда ръка“) ред в организации, където квалификацията и опита на персонала в областта на ИТ и ЗИ са недостатъчни).

Нещо повече, задавахме въпросите съвсем конюнктурно, с единствената цел да потвърдим или отхвърлим някои предварително набелязани от нас цели и идеи. По този начин ще се опитаме да предложим или отхвърлим някои възможни методи в областта на ЗИ, дори непопулярни или престъпващи определени морални норми.

Фиг. 21

Тук позитивните отговори са почти 90%, т.е. имаме в нашите организации наложени ограничения от управляващия екип за изнасяне на информация. Увереността на 22 лица с твърд отговор „да“ ни позволява да направим извод, че навсякъде, в различни системи и сфери на дейност се осъзнава необходимостта от писмени правила и ограничения върху разпространението на информацията. Дотолкова, доколкото самите ЗЗКИ, ЗЗЛД, ЗДОИ и ЗЗТТ съдържат ограничителни режими, то неминуемо техните изисквания са вплетени и въведени в ограниченията върху разпространението на информацията. Но конкретната среда вероятно навсякъде създава предпоставки и за други, индивидуални за организацията ограничения. Тяхното изследване обаче би разширило неограничено това изследване.

Този чарт в случая ни позволява да възприемем състоянието на ЗИ като писмено развита политика на организациите. Като позитивен знак при отговорите отново приемаме, че двусмисленият отговор, изразяващ и несигурност - „колкото не, толкова да“ изобщо не е посочен, т.е. остава малък/приемлив процент анкетирани да смятат, че при тях няма създадени писмени документи, ограничаващи достъп до информация – под 12 %. Което по принцип може да се дължи и на обикновено незнание, но това предположение не е много вероятно, все пак твърдим, че нашите респонденти са експерти в областта на ЗИ. Вероятно просто това е истинското положение, или не се възприемат определени документи непременно като ограничаващи.



Фиг. 22

В този въпрос има малка уловка за анкетираните. По принцип понятието „цензура“ е натоварено с негативен подтекст по ред причини, най-малкото защото се свързва с комунистическия период в нашата държава и ограниченията в гласността и правото на информираност в обществото и медиите. Нашето изследване има по-различен уклон, и доколкото цензурата е исторически появило се и утвърдило се понятие, механизъм за ЗИ, то приемаме нейното съществуване за логично и нормално, още повече, че цитираните тук ограничения в Русия при медийното отразяване на инвазията в Украйна автоматично ни припомня ефективността на цензурата, особено при кризисни ситуации, военно положение и положение на война. Нещо повече, пристрастната към този конфликт западна преса и медии разпространяват официалната украинска позиция и ограничават (цензурират) руските съобщения, т.е. друг вариант на цензура.

Този въпрос е единствен с преобладаващи несигурни отговори, вкл. по принцип неприемливия за подобни ЕСИ несигурен отговор „колкото не, толкова да“. Очевидно е колебанието на нашите респонденти, които отговарят с 27 отговора (повече от 80%) недостатъчно убедително (в трите средни отговора), т.е. преобладаващият отговор тук не смятаме за порок, като вероятно колебанието е породено от привичният негативен по отношение на демокрацията и правата на човека контекст на цензурата.

Като изследовател на ЗИ обаче изобщо не отхвърляме този метод, достатъчно доказан в нашата и световната история. Нещо повече, чрез цензурата не само се защитава информация от публичен достъп, но и също се възпитава, убеждава, градят се ценности, каквито едно общество смята за правилни. В контекста на политиката за ЗИ в една държава, група, организация или общество, цензурата не трябва да бъде изначално отхвърляна и отказвана, поради доказаните си ефекти и качества при нейното използване, а и понякога ще се наложи определен вид информация да бъде запазена на всяка цена. Тогава малки и бързи промени в законовата основа, напр. в ЗОВС, ЗМВР, Закона за народната просвета и др. могат да предизвикат огромен ефект върху общественото мнение и нагласи. Не трябва да се забравя, особено от изследването на проф. Н.Проданов, че можем да имаме военна, цивилна цензура, цензура върху учебни материали, върху електронни и хартиени медии, върху издания и т.н.[vi]

Фиг. 23

В този въпрос няма „уловка“, като при предходния № 22, но има провокация към мисленето и нагласите на нашите респонденти. Демагогията е модерно, дори може да се нарече политологичното понятие за „лъжа“. И трите използвани понятия имат по-скоро негативен контекст семантично. Като изследовател обаче не трябва да изключвам тези методи, просто защото искаме или не искаме, демократи или не, те съществуват и се използват. Провокацията в този случай е да се признае от анкетираните, че ЗИ може да се реализира и чрез „непочтени“ или „недемократични“ подходи. ЗИ често е единствената правилна политика на една организация, свързана е със просъществуването ѝ, в такъв случай трябва ли да се отказваме от всякакви методи и дори на всякаква цена? Този вариант на отговорите на въпроса изобщо не дава категорично становище дали трябва, кога трябва и защо да се използват подобни непопулярни подходи и методи за ЗИ.

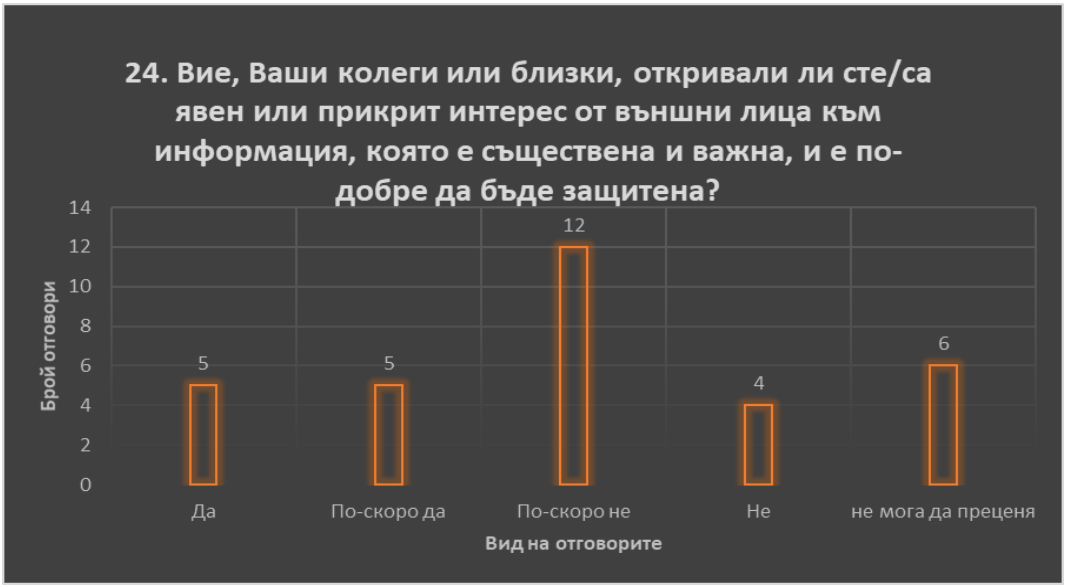
Отново виждаме превес на несигурните отговори (по-скоро да и по-скоро не), но и също двата негативни отговора (не и по-скоро не) имат превес над двата позитивни (17 срещу 13 отговора). В този случай нашите анкетирани лица просто не осмислят, че ЗИ би могло да бъде и в противоречие с общоприети норми и морал, да бъде на ръба на законите и дори да премине отвъд тях. Не

препоръчваме да се престъпват закони, но има вероятност това да стане, колкото и недемократично, антиобществено или непочтено да изглежда.

Не сме привърженици на сентенции от типа „Целта оправдава средствата“ или „Прави каквото трябва, да става каквото ще“, дори напротив по-скоро се считаме за противник на подобен род сентенции, но в крайна сметка те са се появили, защото имат своята логика и защото наистина са се случвали, т.е. в реалния живот и ситуации, както един човек, така и група, партия, държава, коалиция от държави могат да използват (б.а. – да се налага да използват) демагогия или манипулация. Нещо повече, пиар агенциите като че ли се специализират непрекъснато в използването на подобни методи, които имат благоприятен ефект върху техните клиенти. Ако в политиката е прието да се демагогства, то дали това не трябва да се използва и в професионалния живот, когато е необходимо, в случая – при ЗИ.

Резултатите от този въпрос, най-вече 17-те отговора „не“ и „по-скоро не“ са малко изненадващи. Експерти от типа на нашите анкетирани би трябвало да си дават сметка за разнообразните заплахи и рискове, за уникалните атаки срещу сигурността на информацията, за гигантските средства и усилия за разузнаване и информационно превъзходство, за да предвидят, че методите за ЗИ могат да бъдат и не дотам популярни или да са полузаконни.

Всъщност нашата „малка“ провокация в този случай се оказа сериозна провокация.



Фиг. 24

Въпросът кореспондира в известен смисъл с въпрос № 14 относно данни за нанесени вреди на физически или юридически лица, в следствие на изтичане на информация. Там също преобладаваха отговорите „по-скоро не“, т.е. анкетираните не познават такива случаи. В случая става дума за любопитство или откровен интерес по отношение на чувствителна информация, притежавана от нашите респонденти. За да бъде прихванат подобен интерес или опит за контакт, то са необходими усет и рефлекс, които се придобиват при дългогодишна оперативна практика. Очевидно не всички от анкетираните притежават подобен опит и качества, вероятно и това е причина трите последни и смятани от нас за негативни отговори да представляват 70% от отговорите.

Невероятно е, т.е. смятаме за невъзможно, нашите анкетирани лица да не са попадали в ситуация, където са били проучвани от събеседниците си, въпреки, че не е било непременно необходимо. И не става дума само за класифицирана информация, тук може да намесим личните данни, търговските тайни, другите видове професионални тайни и т.н. При този широк набор от данни, които трябва да бъдат недостъпни за широката публика, най-вероятно всички многократно сме изпадали в ситуация да задоволяваме (или пък не) чужд интерес.

Тук също бихме използвали техниката „Какво…, ако…?“ какво трябва да се направи при проявен нездрав интерес към класифицирана информация (б.а. – за реакцията при разузнавателна заплаха в обучението на ДКСИ има нарочна лекция). За подобен контакт просто трябва да се докладва, както се оказва, по-добре де имаме грешна преценка, отколкото да допуснем контактът да се състои. Какво да се прави, ако има интерес към личните данни на определени лица? Отговорът никак не е лесен поради разнообразието и вида на личните данни, както и личното мнение на всеки индивид, ръководител или администратор на лични данни. Задаваме обаче този въпрос с идеята, че при личните данни най-добре да се извести собственикът на тези данни (физическото лице) и администратора на лични данни, който ги притежава и обработва. Или това е най-малкото, което по принцип трябва да се предприеме…

От изследваното в този фактор, следват някои изводи:

- В съвременните организации има създадени правила за ограничаване на изтичането на информация, т.е. имаме писани политики в това отношение;

- Анкетираните се колебаят относно използването на методи, които имат полезен ефект върху ЗИ, но изглеждат непопулярни и недемократични;

- Анкетираните лица не признават за разкриване на проявен интерес към притежавана от тях информация.

Въпрос № 25 е самостоятелен, не принадлежи към изследваните фактори. С него проверихме полезността на анкетата за самите анкетирани, т.е. дали проявиха интерес и дали има зададени въпроси за самите тях и тяхната работа. Не предлагаме чарт, т.като отговорите са дълги и трудно биха били поставени в диаграма, просто самият въпрос и получените отговори.

25. За тази анкета смятате:

А) полезна, дадох си сметка за необходимостта от защита на важната информация - 15 отговора;

Б) сравнително полезна, не ми казва много нови идеи - 12 отговора;

В) нищо ново, тази политика е известна и разпространена - 1 отговор;

Г) безполезна за мен и моята работа - 1 отговор;

В) не мога да преценя - 3 отговора.

Стойността на отговорите дава основание да твърдим, че анкетата определено има своята роля в разбирането на политиката по ЗИ в нашите организации. Сравнителната равностойност на първите два (позитивните) отговори, вероятно се дължи и на експертното ниво на нашите респонденти. Определено ги изненадахме в съвсем малко въпроси, като тези от № 22 и 23. В останалата част масово намираха за нормални и прогнозируеми въпросите от ЕСИ, както и логика в тяхното подреждане.

Общи изводи от настоящото ЕСИ:

За провеждане на ЕСИ бяха избрани предимно експерти с висше образование, достатъчно добър опит в областта на ЗИ, достъп до защитена информация и перспективи пред себе си. Поради което смятаме получените резултати за достоверни;

- Нашето общество притежава съзнанието, че се намира на прага на информационно общество, където ЗИ е важен (най-съществен) елемент на сигурността въобще;

- В нашата страна има определено ниво на познаване на нормативната основа на тази дейност, но експертите не са достатъчно за всички системи, които имат нужда от такива;

- Има най-малко три насоки за промяна на нормативната основа на дейността – обучение на експерти и улесняване на прилагането, както и облекчаване на отделените ресурси в тази сфера.

- Организациите имат изградени вътрешни системи за ЗИ, има длъжностни лица, вътрешни нормативни актове, както и контролни органи. В общия случай притежават и ресурси за реагиране при заплахи от изтичане на информация;

- Анкетираните лица си дават сметка, че загубата на ценна информация може да доведе до множество загуби и дори до ликвидиране на организацията.

- В съвременните организации си дават сметка и имат налични експерти (макар и недостатъчно) за анализ на риск, в конкретния случай – свързано със ЗИ;

- Анкетираните се колебаят относно използването на методи, които имат полезен ефект върху ЗИ, но изглеждат непопулярни и недемократични;

- Анкетираните лица нямат усет и опит за разкриване на проявен интерес към притежавана от тях информация.

Авторът е член на ДКСИ, бивш служител на служба за сигурност, дългогодишен преподавател в Академията на МВР, експерт и изследовател в областта на сигурността. За контакти – сл. 02/9333 603, e-mail – manoflight@abv.bg

[i] За повече информация – Гюров, Р., Матричен анализ на риска и сигурността, учебник, София, 2020 г., стр. 155 и следващи

[ii] https://chr.bg/istorii/tehno/kak-estoniya-beshe-pobedena-prez-2007-g-v-kiber-vojna/, chronicle.bg, Как Естония беше победена през 2007 г. в кибер война, 4 май, 2022, 16:30 от Даниел Петров

[iii] Тофлър, А., Третата вълна, С., изд. Пейо Яворов, 1991 г.

[iv] Кантарджиев, И., Станев, С., Христов, Хр. Относно финансовото осигуряване на дейността на фирмено контраразузнавателно звено, Сборник научни трудове - Научна конференция с международно участие "MATTEX 2018" - 25-27 октомври 2018, ISSN: 1314-3921, т.2, ч.1, 2018, с.96-108, както и Христов, Л. и Железов, С., Аутсорсинг на корпоративната икономическа сигурност. Сборник доклади от годишна университетска научна конференция, 27-28 юни 2019. Електронно издание, Издателски комплекс на НВУ „Васил Левски". В. Търново, 2019. ISSN 2367-7481. Стр. 902-910.

[v] Великов, И., „Закон за непрекъснатото минимизиране на голямото и максимизиране на малкото" , Авангард Прима, София, 2017 г.

[vi] Проданов, Н., Проблеми на историографската текстология, В.Търново, Св.св. Кирил и Методий", 2006 г., стр. 150 и следв.