# ЗАВРШЕН ИЗВЕШТАЈ ЗА НАУЧНОИСТРАЖУВАЧКИ ПРОЕКТ

НАСЛОВ НА ПРОЕКТОТ: ЕМПИРИСКО ИСТРАЖУВАЊЕ НА КИБЕР БЕЗБЕДНОСНАТА ГОТОВНОСТ НА ЕЛЕКТРОНСКИТЕ И ИНФОРМАЦИСКИТЕ СИСТЕМИ

ГЛАВЕН ИСТРАЖУВАЧ: д-р Невен Трајчевски, вон. проф.

ИНСТИТУЦИЈА: Универзитет „Гоце Делчев“ Штип, Воена академија „Генерал Михаило Апостолски“-Скопје, придружна членка

ТРАЕЊЕ НА ПРОЕКТОТ: Од: Октомври 2022 година
До: Мај 2023 година

БРОЈ НА ДОГОВОР: 03-52/32 од 31.10.2022 г.; 03-52/32-1 од 31.10.2022 г.; 03-52/32-2 од 31.10.2022 г.; 03-52/32-3 од 31.10.2022 г.; 03-52/32-4 од 31.10.2022 г.;

ДАТУМ НА ПОДНЕСУВАЊЕ НА ИЗВЕШТАЈОТ: 11.05.2023 година.

РЕЗИМЕ НА ПОСТИГНАТИТЕ РЕЗУЛТАТИ ОД НАУЧНОИСТРАЖУВАЧКИОТ ПРОЕКТ:

Оваа истражување ги презентира резултатите од емпириското истражување на сајбер безбедносната положба на малите организации во Северна Македонија. Резултатите се дадени како квантитативно одредена вредност во рамките на дефинирана таксономија заснована на теоријата на перспектива и сатус кво теоријата. Анализираната големина е однос помеѓу два клучни параметри на сајбер-безбедноста на една организација, сајбер-безбедносната подготвеност и перципираниот ризик за сајбер-напад од страна на носителите на одлуки. Истражувањето исто така содржи компаративна анализа помеѓу овие резултати и добиените резултати за време на други истражувања во ЕУ и САД.

## 1. УЧЕСНИЦИ ВО РЕАЛИЗАЦИЈАТА НА ПРОЕКТОТ:

**а) Главен истражувач:** д-р Невен Трајчевски, вонреден професор

**б) Соработници – истражувачи:**

1. д-р Љупчо Шошоловски, доц. – Воена академија – Скопје
2. м-р Гоце Стеваноски, асс. – Воена академија – Скопје
3. м-р Моника Качурова, асс. – Воена академија – Скопје
4. д-р Надица Тодоровска, насл. доц. – АРСМ

**в) Соработници - млади истражувачи**

1. Марјан Зафировски – магистрант на Воена академија – Скопје

## 2. ЦЕЛИ НА ИСТРАЖУВАЊЕТО:

- Преку емпириско истражување квантитивно и квалитатитвно да се процени кибер безбедносната положба во малите организации во Република Северна Македонија;
- Да се направи компаративна анализа помеѓу состојбата со кибер безбедносната положба во РСМ, ЕУ и САД;
- Да се утврдат и дадат насоки за подобрување на кибер безбедносната положба во малите организации;
- Да се утврдат насоки за следни истражувања со цел да се продлабочат целите на ова истражување.

## 3. ОСВРТ НА ОПРАВДАНОСТА НА ИСТРАЖУВАЊЕТО ВО ПОГЛЕД НА ПОСТИГНУВАЊЕТО НА ДЕФИНИРАНИТЕ ЦЕЛИ:

Сајбер безбедноста станува предизвик, па дури и егзистенцијално важна за малите претпријатија и организации како никогаш досега, бидејќи тие стануваат зависни од информатичката технологија. Информатичката технологија е исто така главниот погон кој го обезбедува нивниот развој. Затоа е предизвик да се биде зависен од информатичката технологија која може да биде ранлива и може да чини многу скапо доколку нема соодветна заштита. Според (UK DCMS, 2020)[1] во Обединетото Кралство, речиси половина од бизнисите (46%), пријавиле дека имале нарушување на сајбер безбедноста или напади сметано во период од 12 месеци. Малите претпријатија се сметаат за столб на економијата во ЕУ и тие исто така претставуваат повеќе од половина од европскиот БДП. Имајќи го ова предвид, многу е важно да се процени нивната сајбер-безбедност и понатаму да се спроведат мерки за подобрување.

[1] UK Department for Digital, Culture, Media and Sport: Cyber Security Breaches Survey 2020: Statistical Release.

Затоа е потребно да се процени сајбер безбедносната полжба и на малите организации во Северна Македонија и да се направи компаративна анализа со резултатите што се добиваат во ЕУ и САД. Дополнително потребата за такво согледување се препорачува во заклучоците од многу сеопфатната студија дадена од (Eilts, 2020)[2]. Соодветно, следи дека е многу значајно да се направи компаративна анализа со резултатите како што се дадени во (ENISA, 2021)[3] и (Eilts, 2020)[2].

## 4. ДЕТАЛЕН ИЗВЕШТАЈ ЗА НАУЧНОИСТРАЖУВАЧКИОТ ПРОЕКТ:

По дефинирање на целите и оправданоста на истражувањето, како што е опишано во точката 2 и 3 од овој извештај, а врз основа на релевантни референци од областа пристапот беше усогласен со современите наоди од оваа област во ЕУ и САД. Така, усвоивме дека ќе користиме веќе развиена таксономија за евалуација на сајбер безбедносната положба и веќе развиениот инструмент во рамките на (Eilts, 2020)[2] за да можеме да направиме соодветна споредба со ЕУ и САД. Понатаму извршена е квантитативна студија, следена со анализа на добиените податоци од 20 мали организации во Северна Македонија. На крајот направена е квантитативна и квалитативна споредба со другите студии во ЕУ и САД и добиени се заклучоци за понатамошни стратешки насоки за управување со сајбер безбедносната положба во Северна Македонија, како и одредени насоки за понатамошно истражување. Следува опис на најважните елементи на имплементираната методологија и добиените резултати.

### МЕТОДОЛОГИЈА

Ова истражување користи променлива т.н. таксономија за проценка на сајбер безбеднонаата подготвеност „Таксономија на сајбер безбедносната подготвеност - ризик“ (CyPRisT–Cybersecurity Preparedness-Risk Taxonomy). Новата променлива е врска (однос) на два клучни параметри на сајбер-безбедноста на една организација, ***сајбер-безбедносната подготвеност*** и ***перципираниот ризик за сајбер-напад од страна на носителите на одлуки***. Основата на CyPRisT е во социјалните теории за управување со ризик. Такви теории се Теоријата на перспектива и Статус кво теоријата. Примената на овие теории ја дефинира CyPRisT и нејзиниот квантитативен домен. Мерењето на сајбер-безбедносната подготвеност, како и перципираниот ризик за сајбер-напад од страна на носителите на одлуки и нивна понатамошна класификација во CyPRisT дава претстава за положбата на сајбер-безбедноста во оргнизацијата. Постојат четири квадранти во CyPRisT како што е прикажано на слика 1. „Индиферентноста“ на првиот квадрант се објаснува со неподготвеноста на одлучувачот да се откаже од статус кво и организациите чија вредност на CyPRisT се позиционира во овој квадрант се смета дека се изложени на ризик од загуба поради сајбер-напад. Вториот квадрант „подложен“, се однесува на однесување кое се карактеризира со склоност кон ризик и се смета дека кај овие организации иако постои свесност на носителот на одлуки за сајбер заканите и можните загуби, нема активности за ублажување на сајбер заканите. Третиот квадрант

[2] Eilts, D.: An Empirical Assessment of Cybersecurity Readiness and Resilience in Small Businesses, Doctoral dissertation, College of Computing and Engineering, Nova Southeastern University, 2020.
[3] ENISA: European Union Agency for Cybersecurity: Cybersecurity for SMEs, Challenges and Recommendations, 2021.

„аверзивен“, се однесува на положба со аверзија од загуба. Аверзијата кон загуба може да го објасни ефектот во релација помеѓу рационално одлучување кога изборот да се стане аверзивен кон ризик се заснова на перципираната референтна точка за сајбер ризик и потенцијална загуба. Во овој случај, носителот на одлуки е помалку фокусиран на управувањето со сајбер ризикот поради нискиот перципиран ризик. Четвртиот стратешки квадрант е положба каде што постои избалансиран однос помеѓу разбирањето на сајбер ризикот и активностите за ублажување на заканите.

**Сајбер-безбедносната подготвеност** претставува управување со ризик и тој ја вклучува сајбер-безбедносна готовност и отпорност. Проценката на оваа големина се заснова на примената на активностите дефинирани со NIST Cybersecurity Framework[4]. Овие активности се групирани во пет т.н. функции: Идентификација, Заштита, Детекција, Одговор/Реакција и Закрепнување. Активностите се трансформирани во прашања со помош на експертски мислења и добиен е прашалник со 70 (Да=1/Не=0) прашања во рамките на петте NIST функции. Во текот на создавање на прашалникот, исто така, на секое прашање му е доделен и коефициент на значајноста. На тој начин по одговорот на овие прашања и соодветни пресметки се добива големината CPS (Cybersecurity Preparedness Scores – Коефициент на сајбер-безбедносната подготвеност) кој може да има вредност помеѓу 0 и 5.

**Перципираниот ризик** се проценува со мерење на перципираното влијание и перципираната веројатноста за резлизација на некоја закана-напад. Усвоени се 10-те категории на сајбер-напади врз основа на соодветни рефенци од областа: General malware, Напреден malware/zero-day attack, Компромитирани/украдени уреди, Cross-site scripting, Denial of services, Malicious insider, Фишинг/Социјално инженерство, SQL injection, Web-заснован напад, друго. Понатаму, за овие 10 категории (исто така формулирани во форма на прашања), се мери перципираната веројатност, како и перципираното влијание. Потоа, за секоја од 10-те категории, просечната вредност на производите (веројатност x влијание) е претставена во проценти и дадена како големината DMPRCA (Decision makers' perceived risk of cyber-attack score – Коефициент на перцепиран ризик од сајбер-напад од страна на носителите на одлуки).

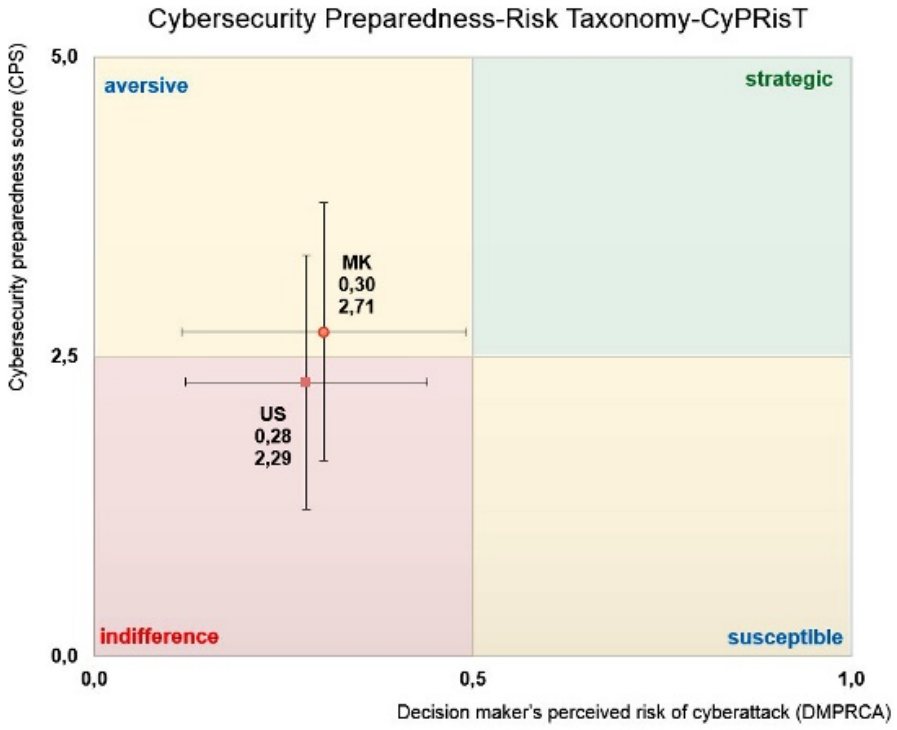
## ИСТРАЖУВАЊЕ И РЕЗУЛТАТИ

Претходно опишаната методологија е употребена со т.н. инструмент во вид на онлајн анкета со цел да се направи квантитативна проценка на сајбер-безбедносната положба на малите организации во Северна Македонија. Избравме одреден број мали организации од различни индустрии. Прибирањето на податоци беше во периодот ноември 2022 година до март 2023 година. До организациите се пристапуваше по телефон, е-пошта и на лице место. Пред истражувањето, носителите на одлуки во овие организации беа информирани дека нивните одговори и податоци ќе останат анонимни и ќе бидат објавени само сумирано и статистички на национално ниво. За да се избегнат неверодостојни резултати, анкетата беше спроведена само кога истражувачкиот тим беше убеден дека носителите на одлуки во избраните организации се мотивирани да учествуваат во анкетата. Во врска со големината на примерокот, постојат многу различни препораки за квантитативно истражување во оваа и слични области и

[4] National Institute of Standards and Technology: Cybersecurity framework, 2018.

одредени референтни извори кои ги користевме препорачуваат примерок со големина од 20 до 30 па и до 40 или повеќе. Во оваа истражување големината на примерокот беше 20, што го сметаме за доволно имајќи ја предвид природата на студијата, комплицираниот процес на спроведување на истражувањето и ограничувањата на ресурсите. Сепак, оваа големина на примерокот ја потврдивме со статистичка пресметка и беше верификувано дека примерокот од 20 организации е оправдан.

Податоците собрани преку претходно опишаниот инструмент беа квантитативно анализирани и беа добиени следните вредности: Просечниот резултат на DMPRCA беше 0,3, што укажува на ниско ниво на воочен ризик од сајбер напад. Просечниот резултат на CPS беше 2,71 што укажува на вредност од среден опсег на подготвеноста за сајбер-безбедност на примерокот. Вредностите беа позиционирани на CyPRisT со DMPRCA на хоризонталната оска и CPS на вертикалната оска, слика 1.




Слика 1. Споредба на CyPRisT и вклучената стандарно отстапување за РСМ и САД

Добиените податоците се споредени со податоците за САД од (Eilts 2020)[2]. Овие резултати беа анализирани со користење на t-тест на нееднакви варијанси (Welch's t-test) за двете големини DMPRCA и CPS, за да се утврди дали постојат статистички значајни разлики, имајќи предвид дека истражуваните популации се различни, но исто така и големините на примерокот и дисперзиите се различни. Резултатите покажаа дека статистички нема значајни разлики помеѓу вредностите $DMPRCA_{MK}$ и $DMPRCA_{US}$, како и помеѓу $CPS_{MK}$ и $CPS_{US}$. Сепак, можеме да забележиме зголемување и на CPS и на DMPRCA во Северна Македонија што ја поместува положбата повеќе кон „аверзивниот“ квадрант на CyPRisT.

Исто така, направена е квалитативна споредба со резултатите презентирани во рамките на (ENISA, 2021)[3], каде се претставени наодите од студијата која опфаќа 249 средни и мали претпријатија од 25 европски земји-членки. Нискиот $DMPRCA_{MK}$ се преклопува со заклучокот во (ENISA, 2021) дека многу мали и средни претпријатија не ги сфаќаат

потенцијалните ризици од сајбер безбедноста што постојат за нивната организација. Исто така, вредноста во средниот опсег на $CPS_{MK}$ се преклопува со заклучокот во (ENISA, 2021) дека организациите се чини дека имплементираат некои од основните мерки за сајбер-безбедност најмногу како дел од нивната севкупна ИТ имплементација или законски обврски.

## 5. ЗНАЧАЈНИ НАУЧНИ СОЗНАНИЈА ЗДОБИЕНИ СО РЕАЛИЗАЦИЈАТА НА ПРОЕКТОТ:

Оваа истражување се однесува на истражувачки прашања кои се релевантни и значајни во областа на безбедноста на информациските системи. Истражувањето дава нови наоди кои вклучуваат квантитативно мерење на моменталната положба на сајбер безбедноста во Северна Македонија, како и квантитативна и квалитативна споредба на овие резултати со слични добиени во студии во ЕУ и САД.

Ако генерализираме произлегува дека помалку од една четвртина од малите организации во Северна Македонија се потенцијално индиферентни кон сајбер безбедноста, што во споредба со САД е подобро, каде што повеќе од половина од малите и средните претпријатија се позиционирани во оваа група. Исто така, резултатите покажаа дека само неколку од организациите се проценети дека позиционираат како „risk seeking“ – склони кон ризик, што се преклопува со наодите од студиите во САД и ЕУ. Повеќето од организациите во Северна Македонија беа позиционирани како аверзивни кон загуба – „loss aversive“. Аверзивноста кон загубата се чини дека е главниот двигател во одлучувањето. Ова укажува дека постојните регулативи, особено во банкарскиот и ИТ секторот даваат резултати, но носителите на одлуки не се доволно фокусирани на управувањето со сајбер заканите. Наодите, исто така, едвај го забележаа постоењето на положба каде што постои стратешка рамнотежа помеѓу разбирањето на сајбер ризикот и спроведувањето на безбедносните активности за справување со сајбер заканите, што е ист наод како и во студиите во ЕУ и САД.

## 6. КОРИСНИЦИ НА ИСТРАЖУВАЧКИТЕ РЕЗУЛТАТИ, НАЧИНИ НА ПРЕНЕСУВАЊЕ И ПРИМЕНА НА ИСТИТЕ:

Една многу практична импликација што произлегува од оваа студија е дека постои потреба од понатамошен развој на програми кои можат да им помогнат на малите организации да ја подобрат својата сајбер-безбедност. Најважно би било развивањето на свеста на носителите на одлуки за ублажување на ризиците од сајбер безбедноста паралелно со нивниот постоечки фокус на нивните примарни активности. Ова ќе придонесе малите организации да станат поаверзивни на ризик.

## 7. ОБЈАВЕНИ РЕЗУЛТАТИ КОИ ПРОИЗЛЕГУВААТ ОД ИСТРАЖУВАЊЕТО

### а) Оригинални научни трудови објавени во списанија во земјата:

Trajchevski, Neven and Stevanoski, Goce (2023), Cybersecurity posture research in small organizations. Современа Македонска Одбрана (44). ISSN 1409-8199 (In Press)

## 8. РЕКАПИТУЛАЦИЈА НА ПОТРОШЕНИ СРЕДСТВА ЗА РЕАЛИЗАЦИЈА НА ПРОЕКТОТ:

Во тек на истражувањето не беа предвидени материјално-финансиски трошоци. Сите трошоци беа лично покриени од истражувачите. Превземената обврска согласно член 5 од потпишаните договори со организациите е извршена и сите се запознаени со резултатите од истражувањето.

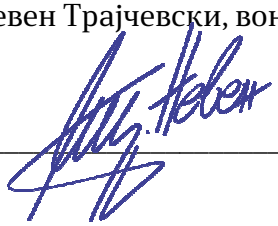
## 9. ПОВАЖНИ ЗАКЛУЧУВАЊА И НАСОКИ ЗА ПОНАТАМОШНИ ИСТРАЖУВАЊА КОИ ПРОИЗЛЕГУВААТ ОД НАУЧНО-ИСТРАЖУВАЧКИТЕ РЕЗУЛТАТИ:

При спроведувањето на оваа истражување во рамките на нејзините ограничувања, доживеавме чувство дека само ја изгребавме површината на темата, така што овде можеме да дадеме некои од многуте прашања кои ги сметаме за важни за идните истражувања:

- Зголемување на бројот на примерокот – број на истражувани организации;
- Понатамошна статистичка анализа во однос на демографските податоци на организациите за индустријата, бројот на вработени (големина), годините во работењето, годишниот приход, буџетот за ИТ;
- Анализа на CPS и DMPRCA со споредба по индустрија, број на вработени и буџет за ИТ;
- Анализа на DMPRCA во однос на перципираната веројатност за сајбер-напад по одредени вектори на напад;
- Анализа на CPS во однос на перципираното влијание на сајбер-нападот по одредени вектори на напад.

ГЛАВЕН ИСТРАЖУВАЧ

д-р Невен Трајчевски, вон. проф.



_____