Ненад М. Јевтић[1]
Јелена Д. Раут[2]
Универзитет „Унион – Никола Тесла“,
Факултет за инжењерски менаџмент
Београд (Србија)

007:004.056.5]:316.772.5
316.32:004
Прегледни научни рад
Примљен 01/11/2023
Измењен 13/02/2024
Прихваћен 19/02/2024
doi: 10.5937/socpreg58-47480

АНАЛИЗА СОЦИОЛОШКИХ АСПЕКАТА ИНФОРМАЦИОНЕ БЕЗБЕДНОСТИ ПРИМЕНОМ HAIS-Q МОДЕЛА

Сажетак: Циљ рада је истраживање социолошких аспеката информационе безбедности кроз HAIS-Q модел, на Факултету за инжењерски менаџмент. Истраживање је спроведено анонимно, у временском оквиру од четири месеца, на узорку од 179 испитаника. HAIS-Q модел је изграђен од седам фокусних области, које прожимају варијабле знање, ставови и понашања, док се предметно истраживање усмерило на фокусну област „употреба интернета“. Анализирајући варијабле са најнижим оценама у једној од седам фокусних области овог модела, истражују се недостаци у свести о информационој безбедности међу запосленима. Рад истиче импликације ових недостатака за организациону безбедност и заштиту информација, са акцентом на важност унапређења варијабли са најнижим оценама. Свеобухватним разматрањем социолошких димензија информационе безбедности, доприноси се бољем разумевању ове важне области данашњег дигиталног доба.

Кључне речи: информациона безбедност, HAIS-Q модел, свест о информационој безбедности (ИСА), перцепција ризика, организациона безбедност

УВОД

У данашњем дигиталном окружењу, где су информације постале највреднији ресурс, предузећа се суочавају са рањивошћу и све већим бројем претњи. Ranas (2020) наглашава да информациона безбедност има кључну улогу у одржавању продуктивности и успеха предузећа. Уколико изостане прилагођена политика информационе безбедности, предузећа су изложена ризику од губитка или компромитовања података, финансијских губитака, оштећења репутације, као и правних проблема. Стога је неопходно успостављање ефикасних мера информационе безбедности, како би

[1] nenad.jevtic@fim.rs
[2] jelena.raut@fim.rs

предузеће било у могућности да осигура континуитет свог пословања и заштити своје податке.

Сајбер безбедност је растућа и значајна област којом се баве различите истраживачке студије. Оно што се у области сајбер безбедности истражује јесте и како унапредити свест о сајбер безбедности, фокусирајући се на оне факторе који су најзначајнији у постизању овог циља (Kovačević et al., 2020). Кругер и сар. (Kruger et al., 2010) у свом истраживању описују студију за тестирање могућности коришћења тестова речника безбедности информација за процену нивоа свести и познавања безбедносних термина где је циљ идентификација погодних подручја и тема за програме подизања свести о информационој безбедности. Ал-Џанаби и Ал-Шоурбаџи (Al-Janabi and Al-Shourbaji, 2016) спровели су истраживање о нивоима свести о информационој сигурности и повезаним ризицима, као и о укупном утицају институције, међу студентима и особљем у оквиру образовног окружења на Блиском истоку. Јеске и Ван Шајк (Jeske and Van Schaik, 2017) спровели су истраживање на узорку испитивања који су чинили ученици са различитим претњама на интернету, где су им представљене дефиниције претњи и затражено да наведу колико су упознати са сваком од њих. Грацијан и сар. (Gratian et al., 2018) спровели су истраживање које се фокусирало на људске карактеристике, где су издвајали склоност ка преузимању ризика, стиловима доношења одлука, демографији и особинама личности, са намерама понашања у области сајбер безбедности међу студентима и особљем на државном универзитету. Моалем (Moallem, 2019) је спровео студију свести о сајбер безбедности међу студентима у Калифорнији (Silicon Valley), као најнапреднијем технолошком окружењу, где је аутор известио да иако студенти верују да су посматрани и да нису безбедни на мрежи, нису били свесни на који начин да заштите своје податке. Парсонс и сар. (Parsons et al., 2017) анкетирали су студенте помоћу свог инструмента HAIS-Q, док су исти студенти такође учествовали у емпиријском phishing експерименту. HAIS-Q је заснован на моделу знања-ставови-понашања, при чему су аутори у својим претходним истраживањима показали снажну и позитивну везу између знања, ставова и понашања (Parsons et al., 2014; McCormac et al., 2017). Анвар и сар. (Anwar et al., 2017) истраживали су колико је значајан фактор пол у погледу уверења и понашања запослених у сајбер безбедности. Кејн и сар. (Cain et al., 2018) анализирали су знање о сајбер хигијени о концептима и понашању крајњих корисника, где су известили да постоје статистички значајне родне разлике у погледу знања. Истраживачки центар Pew је спровео истраживање перцепције, кршења безбедности и понашања Американаца у погледу сајбер безбедности, где наводе да иако је већина Американаца доживела кршење података и нису веровали савременим институцијама које би штитиле њихове личне податке, они сами нису применили најбоље праксе у сајбер простору (Olmstead et al., 2017). Све поменуте студије се баве комплексношћу феномена сајбер безбедност и заједничка им је идентификација различитих фактора који утичу на свест о сајбер безбедности, и настоје да објасне међусобну условљеност фактора, као што је перцепција, кршење безбедности, понашање, знање и демографске карактеристике (Kovačević et al., 2020).

Ковачевић и сар. (Kovačević et al., 2020) настојали су у свом истраживању да тестирају ефекте различитих фактора и покушали да открију на који начин они (као

што су социодемографија, перципирана сајбер безбедност, претходна искуства кршења, употреба информационих технологија и знање) могу појединачно или заједно да утичу на понашање у сајбер безбедности. То је била прва анкета спроведена међу студентима у Србији у области анализе различитих фактора који утичу на свест о сајбер безбедности. Показало се да су ефекти перцепције, знања и искустава о сајбер безбедности јачи од ефеката социодемографских података на понашања у вези са мобилним телефоном, односно да су се употреба и знање из области информационих технологија појавили као значајни предиктори понашања у вези са мобилним телефоном.

Све се више признаје да се многе претње по рачунарске системе организације могу приписати понашању корисника рачунара (Parsons et al., 2014). Парсонс и сар. су настојали да квантификују ове рањивости информационе безбедности, које су засноване на људима, и као резултат настао је Упитник о људским аспектима безбедности информација (HAIS-Q). Циљ њиховог рада је био да се оцрта концептуални развој HAIS-Q модела, укључујући валидност и поузданост, док је са друге стране циљ био да се испита однос између познавања политике и процедура, односа према политици и процедурама и понашања при коришћењу радног рачунара.

HAIS-Q модел је развијен као алат за мерење и анализу људских фактора који утичу на информациону безбедност. Развијен је на основу емпиријских истраживања и валидација, које су му пружиле висок ниво поузданости и ваљаности.

Како објашњавају Парсонс и сар. (Parsons et al., 2017), запослени највише доприносе информационој безбедности предузећа кроз знања, ставове и понашања на следећи начин:

- Знање – Неопходно је да запослени поседују одговарајуће знање о информационој безбедности, како би разумели потенцијалне претње, а потом и како би знали како да се од њих заштите.
- Ставови – Ставови запослених према информационој безбедности такође имају важну улогу. Позитиван став према информационој безбедности подразумева свест о важности заштите података и спремност да се предузму потребне мере заштите. Запослени са позитивним ставом ће бити мотивисани да се придржавају безбедносних правила и да буду опрезни у свом раду, како би смањили ризик од безбедносних инцидената.
- Понашање – Понашање запослених у вези са информационом безбедношћу је кључно и односи се на правилно руковање осетљивим информацијама, коришћење сигурносних лозинки, избегавање посећивања сумњивих линкова, као и редовно ажурирање софтвера. Неоходно је да запослени буду одговорни у вези са заштитом података и да се придржавају безбедносних правила и процедура, које успоставља политика информационе безбедности.

Резултати истраживања које су спровели Парсонс и сар. (Parsons et al., 2014), на узорку од 500 аустралијских запослених, показују да је познавање политике и процедура имало јачи утицај на став према политици и процедури него понашање које су сами пријавили. Њихов налаз је сугерисао да ће обука и образовање бити ефикаснији уколико назначе оно што се очекује (знање) и пруже разумевање зашто је то важно (став).

Примена HAIS-Q упитника доноси бројне користи организацијама. HAIS-Q омогућава процену ефикасности програма свести о информационој безбедности и идентификацију области које захтевају побољшање (Parsons et al., 2017). Разумевањем специфичних недостатака у знању и ставовима који треба да буду унапређени, организације могу прилагодити своје иницијативе свести о безбедности информација како би боље одговарале потребама својих запослених. HAIS-Q омогућава организацијама да упореде своју свест о безбедности са индустријским стандардима и најбољим праксама (Parsons et al., 2017). Поређењем резултата са другим организацијама у истом сектору, организације су у могућности да боље разумеју своје релативне перформансе и идентификују области у којима заостају или се истичу (Roberts, 2021). HAIS-Q пружа организацијама квантитативну меру свести о безбедности својих запослених, омогућавајући праћење напретка током времена (Parsons et al., 2017). Блант (Blunt, 2022) је своје истраживање спровео у Сједињеним Америчким Државама, на узорку од 306 испитаника, користећи HAIS-Q модел, где су му резултати показали да запослени Американци имају високу свест о безбедности информација, са значајном везом између ставова о политици и процедурама, као и њиховом коришћењу, које није склоно ризику. Редовним спровођењем процена путем HAIS-Q модела, организације су у могућности да прате ефикасност својих иницијатива свести о безбедности и да доносе одлуке које су засноване на подацима, како би континуирано побољшавале своју информациону безбедност.

Очекује се да ће резултати о информационој свести запослених пружити основу за информисано планирање и имплементацију мера за унапређење информационе безбедности на Факултету за инжењерски менаџмент, Универзитет „Унион – Никола Тесла“, чиме ће се смањити ризици од безбедносних инцидената у вези са информацијама.

СВЕСТ О ИНФОРМАЦИОНОЈ БЕЗБЕДНОСТИ ПОЈЕДИНЦА, КАО ДЕФИНИШУЋИ АСПЕКТ САВРЕМЕНОГ ДРУШТВА

У савременом друштву, информациона безбедност добија све већи значај за неометано функционисање предузећа.

Како су информације често поверљиве и приватне (нпр. лични подаци, пословне тајне, медицинске информације...), очување њихове поверљивости кључно је за заштиту приватности и спречавање злоупотребе (Parsons et al., 2014). Информациона безбедност се односи и на очување интегритета података, што имплицира да се информације не смеју непожељно мењати или уништавати. Информациона безбедност подразумева да информације буду доступне онда када су потребне. Напади, као што су DDoS (Distributed Denial of Service) могу онеспособити мрежне сервисе и ометати ефикасно функционисање организација (Singh et al., 2020). Како се у савременом друштву велики број трансакција и пословних активности одвија онлајн, неуспех у заштити информација може проузроковати велике економске губитке, како за предузећа, тако и за појединце. Како технологија наставља да се развија узлазном

путањом, све већи број уређаја постаје повезан са интернетом (Internet of things – IoT), што повећава површину напада (Laghari et al., 2021). Како би се очувала сигурност овакве врсте уређаја и система, информациона безбедност постаје неопходна. Закони о заштити података, као што је на пример Општа уредба о заштити података (GDPR), постављају строге захтеве за заштиту личних података грађана (Serrado et al., 2020). Безбедност информација има утицај на поверење јавности према организацијама и институцијама. Инциденти у вези са безбедношћу информација могу оштетити репутацију предузећа и довести до губитка поверења и корисника и клијената.

Информациона безбедност је неопходна за очување стабилности, приватности и функционалности савременог друштва. Недостатак адекватне заштите информација може имати последице на индивидуалном нивоу са једне стране, и на друштвеном и економском нивоу, са друге стране.

Информациона безбедност има дубоке социолошке импликације јер утиче на начин комуникације међу појединцима, на начин њихове сарадње, као и на осећај сигурности у дигиталном друштву. Кроз очување поверења и заштиту приватности, информациона безбедност доприноси социјалној динамици и стабилности друштва.

Свест о информационој безбедности код запослених решава низ проблема савременог друштва.

Едукација запослених о информационој безбедности помаже у смањењу ризика од унутрашњих претњи, као што су несавесни или злонамерни запослени који могу покушати да оштете или украду пословне информације (Soomro et al., 2016). Са друге стране, запослени су често „прва линија одбране" против сајбер напада, а свест о информационој безбедности им помаже да препознају потенцијално опасне ситуације и да поступају одговорно, како би били у могућности да спрече нападе. Како запослени имају приступ осетљивим информацијама предузећа, разумевање правилног руковања тим информацијама помаже у заштити пословних тајни, информација клијената и других поверљивих података (Soomro et al., 2016). Грешке које појединци направе могу довести до губитка информација и сличних проблема у вези са информационом безбедношћу. Обука запослених о безбедним праксама утиче позитивно на смањење оваквих ризика. Одређени сектори, попут здравства и финансија, подложни су строжим законима и регулативама о информационој безбедности (Soomro et al., 2016). Свест о информационој безбедности помаже организацијама да се придржавају ових правила и да избегну правне проблеме.

Свест о информационој безбедности код запослених доприноси ефикаснијој заштити организација од унутрашњих и спољашњих претњи и утиче на смањење ризика и штете који су у вези са сајбер безбедношћу, чиме чини друштво сигурнијим у дигиталном добу.

Како бројна истраживања потврђују да су људске грешке најчешћи узрок нарушавања информационе безбедности (Liginlal et al., 2009; Schultz, 2005), Парсонс и сарадници (Parsons et al., 2017) имали су за циљ да развију претежно квантитативни алат за питања безбедности информација. Итеративни процес у њиховом истраживању донео је хипотезу да се ниво знања корисника о рачунарима тиче безбедносне политике и процедура, њиховог односа према унапређењу политика и процедура, што би требало да се преведе у безбедност информација, која је склонија ризику понашања.

HAIS-Q модел пружа квантитативни приступ мерењу знања, ставова и понашања у вези са информационом безбедношћу (Parsons et al., 2017). Овај модел користи упитник са скалама које омогућавају прецизно квантификовање ових варијабли, што омогућава детаљнију анализу и поређење резултата. Са друге стране, HAIS-Q модел узима у обзир и контекстуалне факторе који могу утицати на информациону безбедност. Модел идентификује различите аспекте људских фактора, укључујући свест о безбедности, мотивацију, знање и понашање, и анализира њихову интеракцију са организационим окружењем (Bohren, 1998). Анализа овог контекста омогућава боље разумевање начина на који организациони фактори утичу на понашање људи у вези са информационом безбедношћу. HAIS-Q модел је развијен кроз ригорозан истраживачки процес који је укључивао концептуални развој, тестирање валидности и тестирање поузданости (Parsons et al., 2017). Модел се састоји од 63 ставке које процењују седам фокусних области у вези са политиком информационе безбедности и понашањем запослених (Parsons et al., 2017).

Као што је у уводу назначено, HAIS-Q модел, кроз знање, ставове и понашања, процењује седам фокусних области. На пример, фокусна област пријављивање инцидената је дефинисана кроз три варијабле (подобласти) у области знања, кроз три варијабле (подобласти) у области ставова и кроз три варијабле (подобласти) у области понашања, односно кроз девет варијабли које се огледају у укупној оцени нивоа свести запослених у фокусној области пријављивања инцидената.

Парсонс и сар. (2017) идентификовали су седам фокусних области које прожимају знање, ставове и понашања, где свака фокусна област има три подобласти, што доводи до укупног броја од 63 варијабле, које су аутори дефинисали кроз 63 питања у инструменту истраживања, док ће подобласти фокусних области бити приказане у наставку.

Фокусна област управљање лозинкама подразумева:
- коришћење исте лозинке,
- дељење лозинке и
- коришћење снажне лозинке (Parsons et al., 2017).

Фокусна област коришћење интернета подразумева:
- приступање сумњивим веб локацијама,
- преузимање фајлова и
- стављање информација онлајн (Parsons et al., 2017).

Фокусна област коришћење електронске поште подразумева:
- посећивање линкова у електронској пошти од познатих пошиљалаца,
- посећивање линкова у електронској пошти од непознатих пошиљалаца и
- отварање прилога у електронској пошти од непознатих пошиљалаца (Parsons et al., 2017).

Фокусна област коришћење друштвених мрежа подразумева:
- подешавање приватности,
- прихватање последица и
- постављање информација о послу (Parsons et al., 2017).

Фокусна област управљање лозинкама подразумева:
• коришћење снажних лозинки,
• недељење лозинки и
• коришћење различитих лозинки за различите налоге (Parsons et al., 2017).

Фокусна област инцидент извештавање подразумева:
• пријављивање сумњивих понашања,
• игнорисање неадекватног понашања колега и
• пријављивање инцидената (Parsons et al., 2017).

Фокусна област управљање информацијама подразумева:
• одлагање осетљивог материјала,
• уметање преносивих уређаја и
• остављање осетљивог материјала (Parsons et al., 2017).

HAIS-Q модел се сматра релевантним и корисним алатом за мерење људских фактора у контексту информационе безбедности. Његове предности се огледају у подршци на основу емпиријских података, могућности квантификације, анализи контекста и у високом нивоу поузданости. Овај модел доприноси бољем разумевању и управљању људским факторима у области информационе безбедности, што помаже организацијама да унапреде своје стратегије и промовишу безбедносну културу.

Свест о безбедности информација (ISA – Information Security Awareness) динамички је процес и због тога је потребно да буде континуирано мерен и управљан (Kruger et al., 2006). HAIS-Q модел пружа могућност да се на основу упитника мери зрелост ИСА код запослених и на основу ИСА резултата пружи увид у потенцијалан недостатак свести код запослених у оквиру одређених аспеката, односно фокусних области.

Проблем који решава ИСА резултат јесте утврђивање нивоа свести код запослених о информационој безбедности јер је у могућности да дâ квантитативне резултате о томе колико су запослени свесни важности информационе безбедности. Са друге стране, у могућности је да кроз квантитативни резултат идентификује области за побољшање.

HAIS-Q модел кроз ИСА резултат пружа дубље разумевање свести о информационој безбедности међу запосленима и идентификује кораке за унапређење информационе безбедности кроз обуке и адекватне иницијативе.

АНАЛИЗА ИСА РЕЗУЛТАТА ЗА ИДЕНТИФИКАЦИЈУ КОРАКА ЗА УНАПРЕЂЕЊЕ ИНФОРМАЦИОНЕ БЕЗБЕДНОСТИ

Предуслов за спровођење ИСА теста било је тестирање HAIS-Q модела. У оквиру опширнијег истраживања, на Факултету за инжењерски менаџмент тестиран је HAIS-Q модел, односно, извршено је анкетирање 179 запослених – наставно и ненаставно особље. Најпре је потврђена статистички значајна корелација између знања, ставова

и понашања, након чега је потврђена статистички значајна корелација између седам фокусних области које граде HAIS-Q модел. То је био предуслов за израчунавање ИСА резултата, који ће бити приказани у наставку. У Табели 1 биће приказани резултати упитника, конвертовани у поене, како би били добијени квантитативни резултати на основу Ликертове скале.

Као што се може видети из Табеле 1, укупан резултат за ниво свести запослених износи 84,5278.

Након што је упитник конвертован у поене, да би се квантификовали резултати помоћу Ликертове скале, они су класификовани коришћењем Кругерове скале мерења свести о безбедности информација где се оцене тумаче на следећи начин:

- добра – од 80 до 100 бодова,
- просечна (потребна побољшања) – од 60 до 79,99 бодова,
- лоша (захтева директну акцију) – од 0 до 59,99 (Cindana, 2019).

Из Табеле 1 може се закључити да све фокусне области, осим фокусне области управљање интернетом, имају добре оцене. Фокусна област употреба интернетом има просечну оцену (79,37927), која захтева побољшања. Такође, може се увидети да фокусна област управљање интернетом захтева побољшања у области ставова (67,9702), који су дефинисани следећим варијаблама:

- док сам на радном месту, не би требало да приступам одређеним веб локацијама,
- само зато што не могу да приступам одређеној веб локацији на радном месту, не значи да је она безбедна,
- када приступам интернету на радном месту, посећујем било коју веб локацију.

Ниске оцене варијабли у области ставова, фокусне групе управљање интернетом, сугеришу да запослени нису у довољној мери свесни ризика и важности информационе безбедности на свом радном месту. Недостатак свести доводи до повећаног ризика од сајбер претњи. Ниске оцене варијабли указују и на недостатак разумевања о томе да ограничен приступ одређеним веб локацијама не значи нужно да су те локације безбедне. Запослени би требало да разумеју да одређене веб локације које су популаризоване, могу представљати ризик по информациону безбедност предузећа. Ниска оцена у овој области сугерише да запослени не практикују одговорно понашање на интернету док су на радном месту, што свакако укључује посету несигурним веб локацијама или ризик од преузимања малвера.

Унапређење оцена набројаних варијабли потенцијално осигурава повећану свест и одговорно понашање, које смањује ризик од сајбер напада, „цурења" података и других безбедносних инцидената. Недостатак информационе безбедности може угрозити репутацију организације, што може резултирати губицима на тржишту и губитком поверења клијената. Такође, недостатак информационе безбедности може довести до проблема са законским регулативама о заштити података, што може резултирати и у високим новчаним казнама.

Кроз организоване обуке о информационој безбедности, како би се запослени оснажили да боље разумеју ризике и праксе, може се потенцијално утицати на варијабле које су оцењене као просечне да достигну ниво оцене добар. Имплементација јасних и политика и процедура за коришћење интернета на радном месту, која ограничава

приступ одређеним веб локацијама такође позитивно утиче на достизање оцене добар. На самом крају, неопходна је редовна комуникација о важности информационе безбедности, као и промовисање одговорног понашања међу запосленима. Унапређење свести кроз ставове запослених о информационој безбедности кључно је за стварање безбедног радног окружења и заштиту организације од потенцијалних претњи.

Уколико се организација не придржава предложених корака, може доћи до последица не само у фокусној области употребе интернета него и у другим фокусним областима, са којима је фокусна област употреба интернета у статистички значајној корелацији.

На основу предложених корака, закључујемо да је неопходно да организација утврди процедуре за спровођење истих. Уколико не утврди, то ће довести до негативних утицаја на фокусну област управљање информацијама и фокусну област пријављивање инцидената јер су ове две фокусне области у статистички значајној позитивној корелацији са фокусном облашћу употреба интернета. Анализирајући статистички значајну корелацију која постоји између фокусне области употреба интернета и фокусне области управљање информацијама, недостатак напретка у области употребе интернета може негативно утицати на ефикасност и сигурност управљања информацијама, што потенцијално може довести до проблема са праћењем, складиштењем и заштитом података, односно може доћи до повећања ризика од губитка информација. Са друге стране, статистички значајна позитивна корелација између фокусне области употреба интернета и фокусне области пријављивање инцидената, недостатак свести о безбедности на интернету може довести до пропуштања важних информација о инцидентима, што може продужити време реаговања на такве ситуације.

Недостатак напретка у области фокусне области употреба интернета може потенцијално довести до општег смањења информационе безбедности у испитиваној организацији и створити рањивости које би нападачи могли да искористе за нападе на систем.

Како би се спречиле потенцијалне негативне последице, важно је предузети мере за унапређење фокусне области употреба интернета и подизање свести о безбедности на интернету међу запосленима, што се може постићи кроз континуирану обуку и едукацију, како би се осигурало да запослени разумеју и примењују најбоље праксе информационе безбедности и безбедности на интернету.

ЗАКЉУЧАК

У раду су показани резултати истраживања социолошких аспеката информационе безбедности, које је спроведено на Факултету за инжењерски менаџмент. Кроз анализу HAIS-Q модела и дубинску анализу резултата, разматрана је важност мерења свести, ставова и понашања запослених у вези са информационом безбедношћу на академској институцији.

HAIS-Q модел се показао као користан инструмент за идентификацију фокусних области које захтевају пажњу у контексту информационе безбедности. Иако су резултати указали на добар ниво знања, ставова и понашања, а самим тим и свести запослених, у већини фокусних области, посебан је акценат стављен на фокусну област

употребе интернета, која је оцењена као просечна, са потребом за побољшањем. Оцена те фокусне области је додатно истакла недостатак свести о безбедности на интернету међу запосленима. Недостатак свести може довести до последица, као што су потенцијалне сајбер претње, цурење осетљивих података и кршење законских регулатива.

У контексту академске институције, унапређење оцена у вези са употребом интернета и свести о безбедности на интернету је од суштинског значаја. Предложено је институцији на којој је спроведено истраживање да се спроведу обуке о информационој безбедности, како би се оснажили запослени да адекватније разумеју ризике и правилне праксе. Имплементација јасних политика и процедура за употребу интернета на радном месту може значајно допринети побољшању информационе безбедности. Такође, значајно је континуирано комуницирати о важности информационе безбедности и промовисати одговорно понашање међу запосленима. Недостатак напретка у области употребе интернета може негативно утицати на ефикасност и сигурност управљања информацијама на факултету, што може довести до проблема у праћењу, складиштењу и заштити података.

Кроз предузимање предложених мера, Факултет за инжењерски менаџмент може унапредити своју безбедносну културу и адекватно се заштити од потенцијалних сајбер претњи, чиме ће обезбедити сигурно и безбедно окружење за рад и учење у дигиталном свету.

Факултет за инжењерски менаџмент, као академска институција која је омогућила спровођење овакве врсте истраживања у оквиру својих граница, преузима иницијативу лидера у области информационе безбедности. Факултет је препознао важност информационе безбедности и кроз овакав приступ показао посвећеност институције друштвеној одговорности и бризи о заштити информација унутар свог окружења. Овакав приступ ће имати директан утицај на образовање и подизање свести о информационој безбедности како код студената, тако и код запослених на факултету. Студенти ће стећи прилику да уче о важности информационе безбедности и развијају вештине и свест о заштити информација, док ће запослени унапређивати своје разумевање информационе безбедности и одговорност према њој. Информациона безбедност је кључна за заштиту репутације сваке академске институције. Ова институција показује спремност да препозна и адресира потенцијалне ризике унутар свог окружења, чиме се обезбеђује интегритет институције и поверење студената, запослених и јавности. Кроз унапређење свести и знања о информационој безбедности унутар својих оквира, факултет доприноси бољој припреми својих студената за рад у савременом дигиталном окружењу, што ће се одражавати на њихову конкурентност на тржишту рада и њихову способност да допринесу заштити информација у свом будућем професионалном окружењу. За запослене на факултету, свест о информационој безбедности значи да имају сигурно радно окружење, где се њихове информације чувају и штите на адекватан начин, чиме се осигурава њихова продуктивност и безбедност унутар институције.

Овај социолошки аспект информационе безбедности одражава дубљу друштвену одговорност и лидерство у домену заштите информација и наглашава колико је значајно едуковати и оснажити све чланове друштва, укључујући студенте и запослене, како би разумели и примењивали најбоље праксе унутар ове области.

Nenad M. Jevtić[1]
Jelena D. Raut[2]
University "Union – Nikola Tesla",
Faculty of Engineering Management
Belgrade (Serbia)

ANALYSIS OF SOCIOLOGICAL ASPECTS OF INFORMATION SECURITY USING THE HAIS-Q MODEL

(Translation *In Extenso*)

Abstract: The aim of the paper is to research the sociological aspects of information security through the HAIS-Q model, at the Faculty of Engineering Management. The research was conducted anonymously, within a time frame of four months, on a sample of 179 respondents. The HAIS-Q model is built from seven focus groups, which pervade the variables of knowledge, attitudes and behaviours, while the subject research is focused on the focus area "use of the Internet". By analyzing the variables with the lowest scores in one of the seven focus areas of this model, gaps in information security awareness among employees are explored. The paper highlights the implications of these deficiencies for organizational security and information protection, with an emphasis on the importance of improving the variables with the lowest scores. Through a comprehensive consideration of the sociological dimensions of information security, this paper contributes to a better understanding and management of this important field, emphasizing its importance in today's digital age.

Keywords: information security, HAIS-Q model, information security awareness (ISA), risk perception, organizational security

INTRODUCTION

In today's digital environment, where information has become the most valuable resource, enterprises encounter vulnerability and an increasing number of threats. Ranas (2020) emphasizes that information security plays the key role in maintaining productivity and success of enterprises. Without an adjusted information security policy, enterprises are exposed to the risk of data loss or data compromise, financial losses, reputation damage, as well as legal problems. Therefore, it is necessary to establish efficient information security

[1] nenad.jevtic@fim.rs
[2] jelena.raut@fim.rs

measures in order to make the enterprise able to ensure the continuity of its operations and to protect its data.

Cyber security is a growing and significant area dealt with by different research studies. What is researched in the field of cyber security is also how to raise cyber security awareness, focussing on the most important factors in achieving this goal (Kovačević et al., 2020). In their research, Kruger et al. (2010) describe a study for testing the possibilities of using tests of the information security glossary for the assessment of awareness level and knowledge of security terms, where the goal is to identify adequate areas and topics for the programs of raising information security awareness. Al-Janabi and Al-Shourbaji (2016) conducted the research about the awareness levels regarding information security and related risks, as well as about the overall impact of the institution among the students and staff within the educational environment in the Middle East. Jeske and Van Schaik (2017) conducted their research on a sample of the respondents who were students with different threats on the Internet, where they were presented the definitions of threats and asked to state if they were familiar with each of them. Gratian et al. (2018) conducted the research focused on human characteristics, where they distinguished the inclination towards risk-taking, the styles of decision-making, demography and features of a person, with the intentions of behaviour in the area of cyber security among students and staff at a state university. Moallem (2019) conducted a study about cyber security awareness among the students in California (Silicon Valley) as the most advanced technological environment, where the author reports that, although the students believe that they are being watched and are not secure on the network, they were not aware of the manner of protecting their data. Parsons et al. (2017) interviewed the students with their HAIS-Q instrument, while the same students also participated in the empirical phishing experiment. HAIS-Q is based on knowledge-attitudes-behaviours model, whereas in their previous research the authors showed a strong and positive correlation between knowledge, attitudes and behaviours (Parsons et al., 2014; McCormac et al., 2017). Anwar et al. (2017) examined the importance of the gender factor in the employees' beliefs and behaviours in cyber security. Cain et al. (2018) analyzed the knowledge of cyber hygiene, of the concepts and behaviours of end users, and reported that there were statistically significant gender differences regarding knowledge. The Pew Research Center conducted research into the perception, security breach and behaviour of Americans regarding cyber security, where it is stated that almost the majority of Americans experienced data breach and did not trust modern institutions supposed to protect their personal data, they themselves did not apply the best practices in cyber space (Olmstead et al., 2017). All the above-listed studies deal with the complexity of the phenomenon of cyber security and what they have in common is the identification of different factors affecting cyber security awareness, and they try to explain mutual conditionality of the factors, such as perception, security breach, behaviour, knowledge and demographic characteristics (Kovačević et al., 2020).

In their research, Kovačević et al. (2020) tried to test the effects of different factors and to discover ion what manner they (such as socio-demography, perceived cyber security, previous experiences of breach, use of information technologies and knowledge) may individually or collectively affect cyber security behaviour. It was the first survey conducted among the students in Serbia in the area of the analysis of different factors affecting cyber

security awareness. The effects of cyber security perception, knowledge and experiences proved to be stronger than the effects of sociodemographic data on behaviours regarding the mobile phone, i.e., that the use and knowledge from the field of information technologies have emerged as significant behaviour predictors regarding the mobile phone.

It is increasingly admitted that organizations can ascribe numerous threats to computing systems to computer users' behaviour (Parsons et al., 2014). Parsons et al. tried to quantify these vulnerabilities of information security based on people and, as a result, the Human Aspects of Information Security Questionnaire (HAIS-Q) was developed. The aim of their paper was to outline the conceptual development of the HAIS-Q model, including validity and reliability, while, on the other hand, the goal was to examine the relationship between the knowledge of the policy and procedures, the attitude towards the policy and procedures, and the behaviour in the use of the work computer.

The HAIS-Q model was developed as a tool for measuring and analyzing human factors that affect information security. It was developed on the basis of empirical research and validations that provided it with a high level of reliability and validity.

According to Parsons et al. (2017), the employees contribute most to the organization's information security through knowledge, attitudes and behaviours in the following manner:

- Knowledge – The employees need to have adequate knowledge about information security in order to understand potential threats and also to known how to protect themselves from those threats.
- Attitudes – The employees' attitudes towards information security also play an important role. A positive attitude towards information security implies awareness of the importance of data protection and willingness to undertake necessary protection measures. The employees with a positive attitude will be motivated to observe security rules and be cautious in their work in order to reduce the risk of security incidents.
- Behaviour – The employees' behaviour regarding information security is crucial and it refers to the proper handling of sensitive information, the use of security passwords, the avoidance of visiting suspicious links, as well as regular software updating. The employees need to be responsible regarding data protection and to observe security rules and procedures established by the information security policy.

The results of the research conducted by Parsons et al. (2014) on a sample of 500 Australian employees show that being familiar with the policy and procedures had a stronger effect on the attitude towards the policy and procedure than behaviour reported by the employees themselves. Their finding suggest that the training and education will be more efficient if they state what is expected (knowledge) and offer understating about why it is important (attitude).

The application of the HAIS-Q questionnaire brings numerous benefits to organizations. HAIS-Q ensures the assessment of efficiency of the information security awareness programs and the identification of the areas that need improvement (Parsons et al., 2017). By understanding specific deficiencies in knowledge and attitudes to be improved, organizations may adjust their initiatives regarding information security awareness in order to suit them better to the needs of their employees. HAIS-Q enables organizations to compare their security awareness with the industrial standards and best practices (Parsons et al., 2017). By

comparing the results with other organizations in the same sector, organizations are able to understand better their relative performances and to identify areas in which they fall behind or excel (Roberts, 2021). HAIS-Q provides organizations with a quantitative measure of their employees' security awareness, enabling them to monitor progress over time (Parsons et al., 2017). Blunt (2022) conducted his research in the USA on a sample of 306 respondents, by using the HAIS-Q model, where the results showed that employed Americans had a high degree of information security awareness, with a significant correlation between the attitudes about the policy and the procedures, as well as their use, which is not risk-prone. Thanks to the regular assessment conducted through the HAIS-Q model, organizations are able to follow the efficiency of their initiatives regarding security awareness and to make data-based decisions in order to continuously improve their information security.

The results about the employees' information awareness are expected to give the basis for informed planning and implementation of the measures for improving information security at the Faculty of Engineering Management "Union – Nikola Tesla", which will reduce risks from security incidents related to information.

INFORMATION SECURITY AWARENESS OF AN INDIVIDUAL AS A DEFINING ASPECT OF MODERN SOCIETY

In modern society, information security is becoming increasingly important for the unobstructed operations of enterprises.

Since information is often confidential and private (e.g., personal data, trade secrets, medical information...), keeping their confidentiality is key to privacy protection and misuse prevention (Parsons et al., 2014). Information security also refers to the preservation of data integrity, which implies that information must not be changed or destroyed arbitrarily. Information security implies that information is available when necessary. Attacks, such as Distributed Denial of Service (DDoS) may disable network services and disturb efficient functioning of organizations (Singh et al., 2020). As a large number of transactions and business activities in modern society take place online, failure to protect information can cause huge economic losses both to enterprises and to individuals. Since technology continues its upward development, an increasing number of devices is connected to the Internet (Internet of things – IoT), which increases the surface of attacks (Laghari et al., 2021). In order to preserve security of this type of devices and systems, information security is becoming indispensable. Data protection laws, for example the General Data Protection Regulation (GDPR), stipulate strict requirements for citizens' personal data protection (Serrado et al., 2020). Information security affects the trust of the public towards organizations and institutions. Incidents related to information security may damage the reputation of an enterprise and lead to the loss of trust, as well as of users and clients.

Information security is necessary for maintaining stability, privacy and functionality of modern society. The lack of adequate information protection may have consequences at the individual level, on the one hand, and at the social and economic levels, on the other hand.

Information security has deep sociological implications because it affects the manner of communication among individuals, the manner of their cooperation, as well as the feeling

of security in digital society. By maintaining trust and protecting privacy, information security contributes to social dynamics and stability of society.

Information security awareness among employees resolves a series of problems of modern society.

The employees' education about information security helps to reduce the risk of internal threats, such as negligent or malicious employees who may try to damage or steal business information (Soomro et al., 2016). On the other hand, employees are often the "first line of defence" against cyberattacks, and information security awareness helps them to recognize potentially dangerous situations and to act responsibly in order to be able to prevent attacks. Since employees have access to the enterprise's sensitive information, understanding how to handle this information properly helps to protect trade secrets, clients' information and other confidential data (Soomro et al., 2016). Mistakes made by individuals can lead to information loss and similar problems related to information security. Training employees about secure practices has a positive effect on the reduction of such risks. Certain sectors, such as healthcare and finance, are subject to stricter laws and regulations regarding information security (Soomro et al., 2016). Information security awareness helps organizations to observe these rules and avoid legal problems.

Information security awareness among employees contributes to more efficient protection of organizations from internal and external threats and leads to the reduction of risks and thus makes society more secure in the digital era.

As numerous studies confirm that human mistakes are the most frequent cause of disturbing information security (Liginlal et al., 2009; Schultz, 2005), Parsons et al. (2017) set the goal of developing primarily quantitative tools for information security matters. The iterative process in their research has led to a hypothesis that the users' level of knowledge about computers refers to the security policy and procedures, their attitude towards the improvement of such policies and procedures, which should be translated into information security as more prone to the behaviour risk.

The HAIS-Q model provides a quantitative approach to the measurement of knowledge, attitudes and behaviours regarding information security (Parsons et al., 2017). This model uses the questionnaire with scales that enable precise quantification of these variables, thus ensuring a more detailed analysis and comparison of the results. On the other hand, the HAIS-Q model also takes into account the contextual factors that may affect information security. The model identifies different aspects of human factors, including security awareness, motivation, knowledge and behaviour, and analyzes their interaction with the organizational environment (Bohren, 1998). The analysis of this context enables a better understanding of the manner in which organizational factors affect people's behaviour regarding information security. The HAIS-Q model was developed through a rigorous research process which included the conceptual development, validity testing and reliability testing (Parsons et al., 2017). The model consists of 63 items which assess seven focus areas in relation to the information security policy and the behaviour of employees (Parsons et al., 2017).

As stated in the introduction, the HAIS-Q model assesses seven focus areas through knowledge, attitudes and behaviours. For example, the focus area of incident reporting is defined through three variables (sub-areas) in the area of knowledge, through three variables (sub-areas) in the area of attitudes, and through three variables (sub-areas) in the

areas of behaviours, i.e., through nine variables reflected in the total score of the employees' awareness level in the focus area of incident reporting.

Parsons et al. (2017) identified seven focus areas that pervade knowledge, attitudes and behaviours, where each focus area has three sub-areas, which leads to the total of 63 variables defined by the authors through 63 questions in the survey instrument, while sub-areas of the focus areas will be shown below.

The focus area of password management involves:
- using the same password,
- password sharing, and
- using a strong password (Parsons et al., 2017).

The focus area of the Internet use involves:
- access to suspicious web locations,
- downloading files, and
- placing information online (Parsons et al., 2017).

The focus area of electronic mail use involves:
- visiting links in e-mails from known senders,
- visiting links in e-mails from unknown senders, and
- opening attachments in e-mails from unknown senders (Parsons et al., 2017).

The focus area of social media use involves:
- privacy settings,
- accepting consequences, and
- placing information about someone's work (Parsons et al., 2017).

The focus area of password management:
- using strong passwords,
- not sharing passwords, and
- using different passwords for different accounts (Parsons et al., 2017).

The focus area of reporting incidents involves:
- reporting suspicious behaviours,
- ignoring coworkers' inadequate behaviour, and
- reporting incidents (Parsons et al., 2017).

The focus area of information management involves:
- sensitive material disposal,
- insertion of portable devices, and
- keeping sensitive material (Parsons et al., 2017).

The HAIS-Q model is considered a relevant and useful tool for measuring human factors in the context of information security. Its advantages are reflected in support based on empirical data, the possibility of quantification, the context analysis and in the high level of reliability. This model contributes to a better understanding and management of human factors in the area of information security, which helps organizations to improve their strategies and promote security culture.

Information Security Awareness (ISA) is a dynamic process and that is why it should be continuously measured and managed (Kruger et al., 2006). The HAIS-Q model offers the possibility of measuring the degree of ISA among the employees based on the questionnaire and, using the ISA results, to give insight into potential lack of awareness among the employees within certain aspect, i.e., focus areas.

The problem resolved by the ISA result is establishing the degree of the employees' information security awareness because it is able to give quantitative results about the extent to which the employees are aware of the importance of information security. On the other hand, through the quantitative result it is able to identify the areas for improvement.

Through the ISA result, the HAIS-Q model ensures a deeper understanding of c information security awareness among the employees and identifies steps for improving information security through trainings and adequate initiatives.

ISA RESULT ANALYSIS FOR THE IDENTIFICATION OF STEPS FOR INFORMATION SECURITY IMPROVEMENT

The prerequisite for conducting the ISA test was testing the HAIS-Q model. Within an extensive research study at the Faculty of Engineering Management, the HAIS-Q model was tested, i.e., 179 employees – teaching and non-teaching staff – were surveyed. First the statistically significant correlation was confirmed among knowledge, attitudes and behaviours, and then the statistically significant correlation was confirmed among seven focus areas that constitute the HAIS-Q model. It was the prerequisite for calculating the ISA results which will be shown below. Table 1 will show the questionnaire results converted into points in order to get quantitative results according to the Likert scale.

As it can be seen from Table 1, the total score for the employees' awareness level is 84.5278.

After converting the questionnaire into points in order to quantify the scores with the aid of the Likert scale, they were classified by using Kruger's scale of measuring information security awareness, where the scores are interpreted in the following manner:

- good – 80 to 100 points,
- average (improvements necessary) – 60 to 79.99 points,
- bad (direct action required) – 0 to 59.99 (Cindana, 2019).

From Table 1 it can be concluded that all the focus areas, except for the focus area of the Internet management, have good scores. The focus area of the Internet use has the average score (79.37927), which requires improvements. Furthermore, it can be seen that the focus area of the Internet management requires improvements in the area of attitudes (67.9702), which are defined by the following variables:

- While I am at work, I should not access certain web locations,
- Just because I cannot access a certain web location at my work place, it does not mean that it is secure,
- When accessing the Internet at my work place, I visit any web location.

The low scores of the variables in the area of attitudes, the focus group of the Internet management, suggest that the employees are not sufficiently aware of the risks and importance

of information security at their work places. The lack of awareness leads to an increased risk of cyber threats. The low of the variables also point to the lack of understanding of the fact that limited access to certain web locations does not necessarily mean that those locations are secure. The employees should understand that some web locations which have been popularized may pose a risk for information security. A low score in this area suggests that the employees do not practise responsible behaviour on the Internet while they are at work, which definitely involves visiting insecure web locations or a risk of downloading malware.

The improved scores of the listed variables potentially ensure increased awareness and responsible behaviour, which reduces the risk of cyberattacks, data "leakage" and other security incidents. The lack of information security may jeopardize the reputation of an organization, which may result in its losses in the market and in losing its clients' trust. In addition, the lack of information security may lead to problems related to legal regulations on data protection, which may also result in high fines.

Through organized trainings about information security, intended to empower the employees for a better understanding of risks and practices, it is possible to affect the variables assessed as average and make them reach a good score level. The implementation of clear policies and procedures for the Internet use at the work place, which limits access to certain web locations, also has a positive effect on reaching a good score. At the very end, regular communication is necessary about the importance of information security, as well as the promotion of responsible behaviour among the employees. The improvement of awareness through the employees' attitudes regarding information security is crucial for creating a secure working environment and the protection of the organization from potential threats.

If an organization does not observe the proposed steps, consequences may occur not only in the focus area of the Internet use, but also in other focus areas with which the subject focus area of the Internet use is in a statistically significant correlation.

Based on the proposed steps, we conclude that an organization needs to establish the procedures for the implementation of these steps. In case it fails to do so, it will lead to negative effects of the focus area of information management and the focus area of incident reporting because these two focus areas are in a statistically positive correlation with the focus area of the Internet use. By analyzing the statistically significant correlation that exists between the focus area of the Internet use and the focus area of information management, the lack of progress in the former focus area can negatively affect the efficiency and safety of information management, which can potentially lead to an increased risk of information loss. On the other hand, in the statistically significant positive correlation between the focus area of the Internet use and the focus area of incident reporting, the lack of information awareness on the Internet may lead to omitting important information about incidents, thus prolonging the response time in such situations.

The lack of progress in the focus area of the Internet use may potentially lead to a general reduction of information security in the analyzed organization and create vulnerabilities that may be used by hackers to attack the system.

In order to prevent potential negative consequences, it is important to undertake measures for improving the focus area of the Internet use and for raising Internet security awareness among the employees, which can be achieved through continued training and education so as to enable the employees to understand and apply the best practices of information security and the Internet security.

CONCLUSION

The paper shows the results of the research of the sociological aspects of information security which was conducted at the Faculty of Engineering Management. Through the analysis of the HAIS-Q model and the in-depth result analysis, the importance was considered of the importance of measuring the employees' awareness, attitudes and behaviours regarding information security at an academic institution.

The HAIS-Q model has proved to be a useful instrument for identifying focus areas that need attention in the context of information security. Although the results indicate a good level of knowledge, attitudes and behaviours, and thus of the employees' awareness, in most focus areas the emphasis is laid on the focus area of the Internet use, which has been assessed as average, with the need for improvement. The assessment of this focus area has further pointed to the lack of the employees' security awareness on the Internet. This lack of awareness may lead to consequences, such as potential cyber threats, sensitive information leakage and the breach of legal regulations.

In the context of the academic institution, it is of crucial importance to improve the assessments regarding the Internet use and security awareness on the Internet. The institution at which the research was conducted was advised to organize trainings about information security in order to empower the employees in adequate understanding of risks and proper practices. The implementation of clear policies and procedures for the Internet use at work may significantly contribute to the improvement of information security. Moreover, it is also important to communicate continuously about the importance of information security to promote responsible behaviour among the employees. The lack of progress in the area of the Internet use may negatively affect the efficiency and security of information management at the faculty, which may lead to problems in data monitoring, storage and protection.

By undertaking the proposed measures, the Faculty of Engineering Management can improve its security culture and adequately protect itself from potential cyber threats, thus providing a safe and secure environment for working and learning in the digital world.

The Faculty of Engineering Management, as an academic institution allowing the realization of this type of research within its competences, assumes the leading initiative in the area of information security. This Faculty has recognized the importance of information security and, through this approach, it has shown the commitment of this institution to social responsibility and care for information protection within its environment. This approach will directly affect the education and raising of information security awareness both among the students and the staff at the faculty. The students will have the opportunity to learn about the importance of information security and to develop skills and awareness in relation to information protection, while the staff will improve their understanding of information security and responsibility for it. Information security is key to protecting the reputation of every academic institution. This institution shows willingness to recognize and address potential risks within its environment, thus ensuring the integrity of the institution and the students' trust, employees and the public. By improving the awareness and knowledge of information security within its frameworks, the faculty contributes to the better preparation of its students for working in the modern digital environment, which will be reflected in their competitiveness in the labour market and their ability to contribute to information

protection in their future professional environment. For the faculty staff, information security awareness means having a secure working environment, where their information is kept and protected adequately, thus ensuring their productivity and security within the institution.

This sociological aspect of information security reflects deeper social responsibility and leadership in the domain of information protection and emphasizes how important it is to educate and empower all members of society, including students and employees, to understand and apply the best practices within this area.

REFERENCES / ЛИТЕРАТУРА

Al-Janabi, S., Al-Shourbaji, I. (2016). A Study of Cyber Security Awareness in Educational Environment in the Middle East. *Journal of Information & Knowledge Management*, 15 (1). Available at: https://www.worldscientific.com/doi/abs/10.1142/S0219649216500076

Anwar, M., He, W., Ach, I., Yuan, X., Li, L., Xu, L. (2017). Gender difference and employes cybersecurity behaviors. *Computers in Human Behavior*, 69, 437–443. Available at: https://www.sciencedirect.com/science/article/abs/pii/S0747563216308688?via%3Dihub

Blunt, S. (2022). *Understanding Information Security Awareness in the American Workforce*. St. Thomas University, Florida.

Bohren, O. (1998). The agent's ethics in the principal-agent model. *Journal of Business Ethics*, 17 (7).

Cain, A., Edwards, E., Still, J. (2018). An exploratory study of cyber hygiene behaviors and knowledge. *Journal of Information Security and Applications*, 42, 36–45. Available at: https://www.sciencedirect.com/science/article/abs/pii/S2214212618301455?via%3Dihub

Cindana, J., Ruldeviyani, Y. (2019). Measuring information security awareness on employee using HAIS-Q: Case study at XYZ firms. *In 2018 Internation Conference on Advanced Computer Science and Information Systems*. ICACSIS 2018. Available at: https://ieeexplore.ieee.org/abstract/document/8618219/

Gratian, M., Bandi, S., Cukier, M., Dykstra, J., Ginther, A. (2018). Correlating human traits and cyber security behavior intentions. *Computers & Security*, 73, 345–358. Available at: https://www.sciencedirect.com/science/article/abs/pii/S0167404817302523?via%3Dihub

Laghari, A. A., Wu, K., Laghari, R. A., Ali, M., Khan, A. A. (2021). A review and state of art of Internet of Things (IoT). *Archives of Computational Methods in Engineering*, 1–19. Available at: https://link.springer.com/article/10.1007/s11831-021-09622-6

Jeske, D., Van Schaik, P. (2017). Familiarity with Internet threats: Beyond awareness. *Computers & Security*, 66, 129–141. Available at: https://www.sciencedirect.com/science/article/abs/pii/S0167404817300214?via%3Dihub

Kovačević, A., Putnik, N., Tošković, O. (2020). Factors Related to Cyber Security Behavior. In: *IEEE Access*, vol. 8, pp. 125140–125148. Available at: https://ieeexplore.ieee.org/abstract/document/9136668

Kruger, H., Drevin, L., Steyn, T. (2010). A vocabulary test to assess information security awareness. *Information Management & Computer Security*, 18 (5), 316–327. Available at: https://www.emerald.com/insight/content/doi/10.1108/09685221011095236/full/html

Kruger, H., Kearney, W. (2006). A prototype for assessing information security awareness. *Computers & Security*, 25 (4), 289–296. Available at: https://www.sciencedirect.com/science/article/abs/pii/S0167404806000563

Liginlal, D., Sim, I., Khansa, L. (2009). How significant is human error as a cause of privacy breaches? An empirical study and a framework for error management. *Computers & Security*, 28, 215–228. Available at: https://www.sciencedirect.com/science/article/abs/pii/S0167404808001181

McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., Pattinson, M. (2017). Individual differences and Information Security Awareness. *Computer in Human Behavior*, 69, 151–156. Available at: https://www.sciencedirect.com/science/article/abs/pii/S0747563216308147?via%3Dihub

Moallem, A. (2019). Cybersecurity Awareness Among Students and Faculty. CRC Press. https://doi.org/10.1201/9780429031908

Olmstead, K., Smith, A. (2017). Americans and cybersecurity. Available at: https://www.pewresearch.org/internet/2017/01/26/americans-and-cybersecurity/ (accessed 27-12-2023)

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., Jerram, C. (2014). Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q). *Computers & Security*, 42, 165–176. Available at: https://www.sciencedirect.com/science/article/abs/pii/S016740481300179X

Parsons, K., Calic, D., Pattinson, M., Butacivius, M., McCormac, A., Zwaans, T. (2017). The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies. *Computers & Security*, 66, 40–51. Available at: https://www.sciencedirect.com/science/article/abs/pii/S0167404817300081

Roberts, S. (2021). *Exploring the Relationships Between User Cybersecurity Knowledge, Cybersecurity and Cybercrime Attitudes, and Online Risky Behaviors*. Diss. Northcentral University.

Schultz, E. (2005). The human factor in security. *Computers and security*, 24 (6), 425–426.

Serrado, J., Peneira, R. F., Mira da Silva, M., Scalabrin Bianchi, I. (2020). Information security frameworks for assisting GDPR compliance in banking industry. *Digital Policy, Regulation and Governance*, 22 (3), 227–244. Available at: https://www.emerald.com/insight/content/doi/10.1108/DPRG-02-2020-0019/full/html

Singh, R., Tanwar, S., Sharma, T. P. (2020). Utilization of blockchain for mitigating the distributed denial of service attacks. *Security and Privacy*, 3 (3), e96. Available at: https://onlinelibrary.wiley.com/doi/abs/10.1002/spy2.96

Soomro, Z. A., Shah, M. H., Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. *International Journal of Information Management*, 36, 215–225. Available at: https://www.sciencedirect.com/science/article/abs/pii/S0268401215001103

APPENDIX / ПРИЛОГ

Таβела 1. *ИСА резулшаш (резулшаш аушора)*
/ Table 1. *ISA result (the authors' result)*

Фокусна област / Focus area	Варијабле свести / Awareness variables			Укупан резултат / Total result
	Знање / Knowledge	Ставови / Attitudes	Понашања / Behaviours	
Управљање лозинком / Password management	84,69274	83,9851	84,80447	84,4941
Употреба електронске поште / Use of electronic mail	85,92179	85,95903	85,69832	85,85971
Употреба интернета / Use of the Internet	84,80447	67,9702	85,36313	79,37927
Употреба друштвених мрежа / Use of social media	86,7784	85,77281	85,2514	85,9342
Мобилни уређаји / Mobile devices	84,39479	84,76723	85,47486	84,87896
Управљање информацијама / Information management	85,5121	85,73557	84,54376	84,90379
Пријављивање инцидената / Reporting incidents	84,43203	85,73557	84,54376	84,90379
Укупан резултат за ниво свести / Total result for the awareness level	85,21947	83,0008	85,36313	84,5278

НАЗАД

ВАСК