Zbornik radova Fakulteta tehničkih nauka, Novi Sad

UDK: 004.9
DOI: https://doi.org/10.24867/20OI01Sekulic

SAJBER OSIGURANJE ZA MALA I SREDNJA PREDUZEĆA

CYBER INSURANCE FOR SMALL AND MEDIUM ENTERPRISES

Jelena Sekulić, *Fakultet tehničkih nauka, Novi Sad*

Oblast – INFORMACIONA BEZBEDNOST

Kratak sadržaj – *U radu su nakon uvoda koji oslikava sajber prostor prikazom nekoliko njegovih karakteristika, izložene osnove upravljanja rizikom, kako bi se ukazalo na značaj sajber osiguranja u tom procesu. Dalje je dat pregled postojećih polisa sajber osiguranja, iz ugla pokrića, ali i izuzetaka. Poslednje poglavlje opisuje metodologiju procene nivoa rizika preduzeća koje aplicira za sajber osiguranje i proračuna cene premije, na koju utiču brojni faktori.*

Ključne reči: *Sajber osiguranje, Procena rizika, Određivanje cene premije*

Abstract – *The paper shortly describes cyberspace, then gives an overview of the risk management process, in order to signify cyber insurance as one of its valuable parts. Existing cyber insurance policies are analyzed, both in the terms of coverage as well as exclusions. The last chapter describes methodology for risk assessment and policy pricing.*

Keywords: *Cyber insurance, Risk assessment, Policy pricing*

1. UVOD

Pojam sajber prostora (engl. *cyberspace*) potiče još iz 1980-ih, a prvi ga je upotrebio pisac naučne fantastike Vilijam Gibson. Danas se sajber prostor formalno definiše kao globalni i dinamički domen, podložan konstantnim promenama, a neretko se izjednačava i sa Internetom [1].

Broj korisnika globalne mreže (engl. *World Wide Web*) od 1991. godine, kada je ovaj informacioni sistem postao dostupan javnosti, do 2022. godine dostigao je 5 milijardi, što čini 63% svetske populacije [2]. Paralelno sa razvojem interneta, pojavljuju se i prvi zlonamerni softveri, koji zatim postaju sve sofisticiraniji, češći i opasniji, te je u 2022. godini zabeležen primer objave rata od strane države ka grupi sajber kriminalaca, kao i primer hibridnog rata između dve države, gde je došlo do formiranja sajber jedinica na poziv državnih zvaničnika [3].

Uz razvoj sajber kriminala, razvija se i pravo. Tako je od 2018. godine u Evropi na snazi Opšta uredba o zaštiti podataka (engl. *General Data Protection Regulation*), koja je značajno uticala na poslovanje svih preduzeća koja rukuju podacima o ličnosti [4].

Tržište sajber osiguranja vodi poreklo iz 1990-ih [5].

NAPOMENA:
Ovaj rad proistekao je iz master rada čiji mentor je bio dr Imre Lendak, vanr. prof.

Popularnost stiče povećanjem obima, ali i cene rizika, kao i sve strožijim zakonima i uredbama o obaveznom obaveštavanju o procurelim podacima, kao i obaveznim koracima koji bi popravili ili ublažili prouzrokovanu štetu. Na početku 2022. godine globalno tržište je imalo vrednost 9.2 milijarde američkih dolara, dok su procene da će ova cifra do 2025. godine porasti na 22.1 milijardu [6].

Iako od polise sajber osiguranja mogu da profitiraju organizacije svih tipova i veličina, kao i fizička lica, u ovom radu je fokus na malim i srednjim preduzećima (MSP). Na osnovu člana 6. Zakona o računovodstvu [7], gornji kriterijumi za MSP su: prosek od 250 zaposlenih, prosečni poslovni prihodi od 40 miliona eura ili vrednost imovine u iznosu od 20 miliona eura. MSP čine 99% domaćeg, ali i evropskog tržišta [8, 9], te uz činjenicu da često nemaju dovoljno sredstava za ulaganje u bezbednosne mere i obuku zaposlenih, predstavljaju laku metu sajber kriminalcima. Ovo potvrđuju i mnogi statistički podaci [10], od kojih je najznačajniji taj da je čak 60% malih i srednjih preduzeća doživelo sajber napad u 2020. godini [11].

2. UPRAVLJANJE RIZIKOM

Osiguranje i upravljanje rizikom su dve čvrsto povezane oblasti. Procena rizika je neophodna radi kreiranja ponude osiguranja koja će biti zadovoljavajuća za obe strane, te su identifikacija i analiza rizika sastavni deo procesa sajber osiguranja. S druge strane, osiguranje je jedna od stavki u procesu upravljanja rizikom.

Može se reći da taj proces ima dve faze - fazu procene i fazu tretiranja rizika [5]. U prvoj fazi se vrše identifikacija i analiza rizika. Pod identifikacijom se podrazumeva evidentiranje pretnji, slabosti i uticaja koje rizik može imati ukoliko se ostvari. Nakon identifikacije, moguće je analizirati rizike, pri čemu se koriste različite tehnike - kvalitativne i kvantitativne. Proračun očekivanih godišnjih gubitaka (engl. *Annualized Loss Expected* - ALE) je primer kvantitativne metode za analizu rizika. Ona se bazira na sledećoj jednačini (1):

$$ALE = ARO \times SLE \quad (1)$$

ARO - od engl. *Annualized Rate of Occurrences* je prosečna stopa incidenata na godišnjem nivou, dok je
SLE - od engl. *Single Loss Expectancy*, prosečna cena jednog incidenta.

Konteksta radi, po izveštaju nastalom kroz saradnju kompanije IBM i Ponemon instituta, prosečna cena sajber napada koji je rezultovao curenjem podataka za 2019. godinu iznosi 3.92 miliona USD, sa verovatnoćom od 29.6% [12]. Ovo bi rezultovalo očekivanim troškom u visini od 1.18 miliona USD godišnje.

Primer kvantitativne metode su tabele ili matrice rizika. Pomoću ove tehnike, vrši se procena nivoa rizika ukrštanjem verovatnoće pojave rizika sa ozbiljnošću uticaja koji bi imao. S obzirom na to da vizuelno klasifikuje rizike, ovaj alat se smatra izuzetno jednostavnim, a efektnim, te se može naći u mnogim uputstvima i standardima za analizu rizika. Jedan takav standard je publikovao Nacionalni institut za standarde i tehnologiju (engl. *National Institute of Standards and Technology* - NIST) kao specijalno izdanje pod brojem 800-30 i naslovom Vodič za sprovođenje procene rizika (engl. *Guide for conducting risk assessment*) [13].

U okviru ovog izdanja propisuje se korišćenje matrice dimenzija 5x5, koju ilustruje tabela 1. Naime, ovaj vodič i nivo verovatnoće (redovi) i nivo uticaja (kolone) deli na pet stupnjeva - veoma nizak, nizak, umeren, visok i veoma visok, a istim kvalifikatorima se opisuje i rizik.

NIST radni okvir je osmišljen kako bi pomogao saveznim informacionim sistemima i organizacijama u Sjedinjenim Američkim Državama da sprovedu procenu rizika.

Verovatnoća	**Uticaj**				
	Veoma nizak	Nizak	Umeren	Visok	Veoma visok
Veoma visoka	Veoma nizak	Nizak	Umeren	Visok	Veoma visok
Visoka	Veoma nizak	Nizak	Umeren	Visok	Veoma visok
Umerena	Veoma nizak	Nizak	Umeren	Umeren	Visok
Niska	Veoma nizak	Nizak	Nizak	Nizak	Umeren
Veoma niska	Veoma nizak	Veoma nizak	Veoma nizak	Nizak	Nizak

Tabela 1. *Tabela/matrica rizika* [13]

Drugi nezaobilazni standard je objavljen od strane Internacionalne organizacije za standarde (engl. *International Organization for Standardization*), pod oznakom ISO27005. Ovaj standard takođe pruža smernice za upravljanje rizikom u domenu informacione bezbednosti. Primenljiv je na sve vrste organizacija, kao što su komercijalna preduzeća, vladine agencije i neprofitne organizacije [14].

Nakon završene analize rizika, treba preduzeti sve moguće mere za smanjenje identifikovanih rizika, po prioritetima.

Osim tehničkih mera, u redovnu praksu treba, između ostalog, da budu uključeni i treninzi iz oblasti sajber bezbednosti, redovna ažuriranja softvera, multifaktorska autentifikacija i redovno pravljenje rezervnih kopija podataka [15].

I uz sve mere za ublažavanje rizika, nikada neće biti moguće smanjiti ih na nulu, te će istinski kvalitetan plan za upravljanje rizikom uvek obuhvatati i prenos rizika putem osiguranja.

3. PREGLED POSTOJEĆIH MODELA SAJBER OSIGURANJA

Ne postoji jedna zvanična definicija sajber osiguranja, kao ni jedan, standardni model. U radu koji je nastao kao posledica analize preko 100 polisa sajber osiguranja na američkom tržištu, daje se sledeća definicija: "Sajber osiguranje je skupni pojam za sve polise osiguranja koje se bave direktnim gubicima, kao i gubicama treće strane, koji su posledica računarski baziranog napada ili disfunkcionalnosti kompanijskog informacionog sistema" [16].

Gubici prve (engl. *first-party*) i treće strane (engl. *third-party*), ili direktni i indirektni gubici, čine dva ključna faktora u sajber osiguranju, ali i osiguranju uopšte, te neki osiguravači upravo preko te podele prezentuju svoje usluge.

Asocijacija britanskih osiguravača (engl. *Association of British Insurers*) navodi da *first-party* osiguranje štiti imovinu preduzeća, te pokriva:

- Gubitak ili oštećenje digitalne imovine, kao što su podaci ili softver
- Prekid poslovanja usled pada mreže
- Sajber iznude
- Obaveštavanje klijenata, ukoliko postoji zakonska obaveza
- Krađu novca ili digitalne imovine kroz krađu opreme ili elektronsku krađu

U paraleli sa ovim, *third-party* osiguranje štiti tuđu, tj. klijentsku imovinu, te uključuje:

- Narušavanja bezbednosti i privatnosti: troškove istrage, odbrane i civilne štete u vezi sa incidentima
- Odgovornost za multimediju: troškove istrage, odbrane i civilne štete nastale usled narušavanja privatnosti ili nemarnog ophođenja u elektronskim i štampanim medijima
- Gubitak podataka treće strane, uključujući troškove kompenzacije klijentima za uskraćen pristup i greške u softveru ili sistemu [17].

Rad pod nazivom "Pregled sajber osiguranja" (engl. *Cyber-insurance survey*), sumira osnovno znanje o sajber osiguranju, iz perspektive i tržišta i nauke [5]. Na slici 1 se može videti tabelarni prikaz pokrića sajber polisa nekoliko vodećih osiguravajućih kompanija. Od direktnih gubitaka, najčešće su pokriveni gubitak ili oštećenje digitalne imovine, prekid poslovanja, sajber iznuda i krađa novca ili digitalne imovine. Pokriće troškova treće strane obuhvata troškove narušavanja bezbednosti i privatnosti, forenzičke istrage incidenta, obaveštavanja oštećenih klijenata, odgovornosti za multimedijalne sadržaje, gubitak podataka treće strane, kao i obeštećenje treće strane, definisano ugovorom.

Što se tiče domaćeg tržišta, kompanija *Respect Serbia* nudi dve različite polise koje adresiraju sajber rizike: sajber osiguranje i IT osiguranje. Dok je osiguranje od IT odgovornosti namenjeno kompanijama koje posluju u IT sektoru, osiguranje od sajber odgovornosti pokriva sve kompanije čije je poslovanje zasnovano na internetu, koje raspolažu podacima o ličnostima i drugim kompanijama i koje su izložene riziku od curenja informacija [18].

	Coverage	***Allianz*** *[55]*	***QBE*** *[56]*	***AEGIS*** *[57]*	***CNA*** *[58]*	***InsureTrust*** *[59]*	***CDRM LLC*** *[60]*	***Travelers*** *[61]*	***Zurich*** *[62]*	***ACE*** *[63]*	***Hiscox*** *[64]*	***Insureon*** *[65]*	***Marsh*** *[66]*	***Chubb*** *[67]*	***AIG*** *[68]*
First-party	Loss or damage to digital assets	×*	×	×	×	×		×	×	×	×	×	×	×	×
	Business Interruption	×*	×	×	×*	×	×	×	×	×	×	×	×	×	×
	Cyber extortion	×	×	×	×*	×	×	×	×			×	×		×
	Theft of money and digital assets	×	×		×*		×	×	×	×	×	×	×	×	
Third-party	Security and privacy breaches	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	Computer Foresincs Investigation	×	×	×*	×	×	×			×		×			×
	Customer notification/PR expenses	×	×		×	×	×	×	×	×		×		×	×
	Multi-media liability	×	×	×		×		×	×*	×					×
	Loss of third-party data	×*		×	×*	×	×	×	×	×	×	×	×	×	
	Third-party contractual indemnification		×			×			×	×				×	

Slika 1. *Tabelarni prikaz pokrića različitih polisa sajber osiguranja* [5]

Uz detaljni opis pokrića, većina polisa eksplicitno navodi i događaje koji su iz tog pokrića izuzeti.

Asocijacija britanskih osiguravača u svom vodiču za sajber osiguranje namenjenom malim i srednjim preduzećima [19], upozorava na sledeća isključenja: sudska nadležnost - moguće je da se polisa ne odnosi na određene teritorije; tužbe od strane povezanih lica - neke polise pokrivaju samo troškove tužbi od strane klijenata i kupaca, dok su potencijalne tužbe od strane zaposlenih isključene; telesne povrede i oštećenje svojine - iako pokrivaju štetu nanetu digitalnoj imovini, polise sajber osiguranja uglavnom isključuju pokriće troškova usled oštećenja fizičke imovine ili telesnih povreda; sajber kriminal - ukoliko je napad uzrokovao direktne gubitke novca, npr. hakeri su ukrali pare sa bankovnog računa, izgubljeni novac najčešće neće biti nadoknađen u okviru polise sajber osiguranja.

Analiza polisa registrovanih u SAD [16] pokazala je da su najčešća isključenja ona koja nisu u direktnoj vezi sa sajber prostorom, već se odnose na krivična dela, greške i propuste, namerno kršenje zakona, krivične istrage koje su već u toku, otkrivanje poslovnih tajni ili poverljivih informacija, kao i fizičke povrede, neke aspekte odgovornosti i gubitke vezane za sisteme koji su van kontrole osiguranika. Posledice nastale usled terorizma, rata ili vojnih akcija su takođe uglavnom isključene iz pokrića.

Analizom stepena rizika i cene sajber incidenta, može se uvideti prvi benefit sajber osiguranja, a to je pokrivanje dela troškova. Detaljnijim uvidom u konkretne polise, uviđaju se još neke prednosti, kao što je pomoć u odnosima sa javnošću, dostupnost tima tehničkih stručnjaka za analizu i savetovanje, kao i pravnih savetnika. Uopšte govoreći, osiguranje pomaže u fazi oporavka od sajber napada.

Međutim, postoji i treći sloj, a o njemu govore autori Pregleda sajber osiguranja [5]. Navode četiri prednosti sajber osiguranja, među kojima je pre svega mogućnost da se organizacije motivišu da ulažu više u svoju zaštitu, u cilju smanjivanja premije. Dalje, poboljšanjem sveukupnog nivoa sajber bezbednosti, veruje se da se postiže i viši nivo društvene dobrobiti. Treće, sajber osiguranje može služiti kao indikator kvaliteta zaštite neke kompanije. I poslednje, može dovesti do novih i naprednijih standarda u sajber bezbednosti, jer bi posedovanje sertifikata ili ispunjavanje nekog standarda bio najjednostavniji način da osiguravači procene nivo rizika kom je osiguranik izložen.

Primer dobre prakse moće se naći u Ujedinjenom Kraljevstvu, gde je vlada donela standard pod nazivom engl. *Cyber Essentials*, koji definiše bazične bezbednosne mere, kako bi svako preduzeće imalo minimum zaštite. Takođe, omogućena je i sertifikacija, čime osiguravači dobijaju jasniju sliku o sajber bezbednosti kompanije koju procenjuju [20].

4. METODOLOGIJA ZA PRORAČUN CENE SAJBER OSIGURANJA

Advisor Smith je sproveo istraživanje cena sajber osiguranja u SAD, analizirajući ponudu 43 kompanije [21]. U izveštaju navode da je prosečna cena za 2021. godinu 1,589 američkih dolara godišnje ili 132 dolara mesečno, što je 25% više nego godinu pre. Takođe pružaju uvid u uticaj određenih faktora na prosečnu cenu, konkretno: uticaj naknade, franšize, veličine i tipa preduzeća, količine osetljivih podataka i bezbednosnih mera.

Da bi se rizici mogli kvantifikovati, te odrediti visina premije za svako preduzeće, potrebno je te rizike prvo identifikovati i analizirati. Tehnike koje se koriste za identifikaciju i analizu rizika u kontekstu pisanja ugovora o osiguranju su: analiza poslovne dokumentacije, sastanci i intervjui, upitnici i ankete, korišćenje baze znanja, stabla pretnji, grešaka i napada, analiza istorijskih podataka, standardi i sertifikacije, ALE metoda, matrice rizika, profilisanje i teorija igara [5].

Kako upitnici predstavljaju tehniku prisutnu i u fazi identifikacije i u fazi analize rizika, a i u praksi predstavljaju najčešće korišćenu tehniku, u nastavku će biti data analiza prikupljenih upitnika iz polisa registrovanih u SAD [16]. Analizirana su 24 upitnika, u kojima je identifikovano 97 različitih tema. One su podeljene u 4 oblasti: pitanja o organizaciji, tehnička pitanja, pitanja koja se tiču interne politike i procedura, pitanja o usaglašenosti sa zakonima, uredbama i propisima.

Pitanjima o organizaciji se uzimaju podaci poput naziva kompanije, kontakt osobe, tipa industrije, kao i uže delatnosti; veličine firme u kontekstu broja zaposlenih, zatim podaci o finansijama, među kojima su najvažniji godišnji prihod i vrednost imovine; podaci o broju klijenata, vrednosti i trajanju njihovih ugovora; istorija osiguranja kao i trenutna pokrivenost. Posebna pažnja se pridaje tematici prikupljanja i upravljanja osetljivim

podacima, kao što su podaci o ličnosti, medicinski podaci, podaci o karticama i finansijama, poslovne tajne i intelektualna svojina.

Tehnička pitanja su podeljena u tri grupe, koje se bave, redom: informaciono-tehnološkom infrastrukturom, implementiranim tehničkim merama bezbednosti i kontrolom pristupa.

Treća oblast služi za skupljanje informacija o bezbednosnoj politici i procedurama firme. Npr. ispituje se postojanje politike privatnosti, kao i njena usaglašenost sa vladinim zahtevima, zatim postojanje planova za reagovanje na incident, oporavak od nesreće i nastavak poslovanja, kao i pravljenje rezervne kopije podataka i održavanja bezbednosnih treninga za zaposlene.

I konačno, skoro svaki upitnik sadrži pitanja o usaglašenosti sa standardima za rukovanje medicinskim podacima, podacima o kreditnim karticama, kao i drugim podacima o ličnosti.

Da bi se od upitnika došlo do konkretne cene premije, potrebno je kvantifikovati odgovore, tj. dobijene informacije. Literatura [16] sve dostupne metode grupiše u dve osnovne grupe: paušal (engl. *Flat Rate Pricing*) i modifikacije bazne stope (engl. *Base Rate with Modifications*). Prva određuje prosečnu cenu spram učestalosti i ozbiljnosti nekog događaja (na godišnjem nivou) i ta cena ostaje fiksna za sve kompanije.

S druge strane je malo sofisticiranija metoda, koja će prvo odrediti baznu stopu spram godišnjeg obrta ili imovinske vrednosti kompanije, a zatim će tu stopu modifikovati različitim faktorima: standardnim faktorima u osiguranju (visina naknade, franšize, istorija osiguranih događaja i sl), faktorima specifičnim za industriju kompanije i/ili faktorima koji se direktno tiču položaja firme po pitanju sajber bezbednosti.

4. ZAKLJUČAK

Pred tržištem sajber osiguranja su mnogi izazovi. Informaciono-tehnološki sistemi konstantno evoluiraju, a sa njima i pretnje. Uz to su i međuzavisni, pa je sve teže proceniti realnu štetu. Takođe, sve do sada izloženo se pretežno odnosilo na računarske sisteme, bez posebnog adresiranja mobilnih uređaja, ugrađenih sistema, interneta stvari, itd [5, 16].

Uz dalji razvoj polisa, nazire se i razvoj u pogledu načina pružanja usluge osiguranja. Na ovo ukazuje partnerstvo koje su sklopile kompanije *Allianz*, *Apple* i *Cisco*, u svrhu pružanja boljih paketa sajber osiguranja od strane kompanije *Allianz*, ukoliko osiguranici koriste *Apple* i *Cisco* proizvode. Procene su da će se u budućnosti sajber osiguranje prodavati kao proizvod za sajber bezbednost, direktno nadležnima za tu oblast u kompanijama [22]. Međutim, uz odgovarajuće tehničke mere bezbednosti i svest zaposlenih, već sada sajber osiguranje ima značajnu ulogu u borbi protiv sve opasnijih sajber rizika. Polako se taj značaj uviđa i na domaćem tržištu, te se o sajber osiguranju sve više priča i piše. Iako kod dela zainteresovanih kompanija postoji stav da ne žele da otkrivaju detalje o svom poslovanju ili sigurnosnim procedurama koje imaju, ili stav da mere zaštite čine osiguranje nepotrebnim, potražnja za ovim vidom zaštite poslovanja svakako raste, a rast potražnje će nesumnjivo dovesti i do rasta ponude i promena na tržištu [23].

5. LITERATURA

[1] https://en.wikipedia.org/wiki/Cyberspace (pristupljeno u avgustu 2022.)

[2]https://www.statista.com/statistics/617136/digital-population-worldwide/ (pristupljeno u avgustu 2022.)

[3] Cyber Attack Trends, Check Point's 2022 Mid-Year Report, Check Point Research

[4] https://gdpr.eu/what-is-gdpr/ (pristupljeno u avgustu 2022.)

[5] A. Marotta et al, "Cyber-insurance survey", Computer Science Review, Maj 2017.

[6]https://www.munichre.com/topics-online/en/digitalisation/cyber/cyber-insurance-risks-and-trends-2022.html (pristupljeno u avgustu 2022.)

[7] Закон о рачуноводству: 73/2019-11, 44/2021-4, "Службени гласник РС", April 2021.

[8]https://single-market-economy.ec.europa.eu/smes/sme-definition_en#modal (pristuplje u avgustu 2022.)

[9]https://www.privreda.gov.rs/lat/ministarstvo/organizaciona-struktura/sektor-za-razvoj-malih-i-srednjih-preduzeca-i-preduzetnistva (pristupljeno u avgustu 2022.)

[10]https://www.forbes.com/sites/chuckbrooks/2022/01/21/cybersecurity-in-2022--a-fresh-look-at-some-very-alarming-stats/?sh=3c1a8e716b61 (pristupljeno u avgustu 2022.)

[11] "Cybersecurity in the Remote Work Era: A Global Risk Report", Ponemon Institute, Oktobar 2022

[12]https://www.ibm.com/downloads/cas/RDEQK07R#:~:text=The%20average%20total%20cost%20of%20a%20data%20breach%20in%20the,average%20number%20of%20breached%20records. (pristupljeno u avgustu 2022.)

[13] NIST SP 800-30, "Guide for Conducting Risk Assessments", NIST, Septembar 2012.

[14] https://www.iso.org/standard/75281.html (pristupljeno u avgustu 2022.)

[15]https://hyperproof.io/resource/cybersecurity-risk-management-process/#:~:text=and%20manage%20risk.-,What%20is%20Cybersecurity%20Risk%20Management%3F,has%20a%20role%20to%20play. (pristupljeno u avgustu 2022.)

[16] S. Romanosky et al, "Content Analysis of Cyber Insurance Policies: How do carriers write policies and price cyber risk?", SSRN Electronic Journal, Mart 2017.

[17]https://www.abi.org.uk/products-and-issues/choosing-the-right-insurance/business-insurance/cyber-risk-insurance/ (pristupljeno u avgustu 2022.)

[18] https://respect-serbia.rs/cyber-i-it-osiguranje/ (pristupljeno u avgustu 2022.)

[19]https://www.abi.org.uk/globalassets/sitecore/files/documents/publications/public/2016/cyber-insurance/making-sense-of-cyber-insurance-a-guide-for-smes.pdf (pristupljeno u avgustu 2022.)

[20] https://www.ncsc.gov.uk/cyberessentials/overview (pristupljeno u avgustu 2022.)

[21]https://advisorsmith.com/business-insurance/cyber-liability-insurance/cost/ (pristupljeno u avgustu 2022.)

[22]https://www.techtarget.com/searchsecurity/news/252434612/Cybersecurity-insurance-breaks-coming-for-Apple-Cisco-customers (pristupljeno u avgustu 2022.)

[23]https://bonitet.com/buducnost-sajber-osiguranja-ima-li-koga-na-golu/ (pristupljeno u avgustu 2022.)

Kratka biografija:

Jelena Sekulić rođena je u Zrenjaninu 1997. god. Master rad na Fakultetu tehničkih nauka iz oblasti Informacione tehnologije – Informaciona bezbednost, odbranila je 2022. god.

kontakt: jelena.sekulic@uns.ac.rs