https://doi.org/10.17559/JF-2026010000023

Zaprimljen: 27.12.2025.
Odobren za objavu: 27.1.2026.
Izvorni znanstveni rad

ANALIZA NAPLATE PLASMANA POSLOVNIH SUBJEKATA KOD BANAKA U KONTEKSTU KIBERNETIČKE SIGURNOSTI

Maja Vretenar Cobović[1], Marina Brčelić Kovačević, studentica,[2] Jasna Vujčić[3]
[1] Sveučilište u Slavonskom Brodu, Trg I. B. Mažuranić 2, 35000 Slavonski Brod, Hrvatska, ePošta: mvcobovic@unisb.hr
[2] Sveučilište u Slavonskom Brodu, Trg I. B. Mažuranić 2, 35000 Slavonski Brod, Hrvatska, ePošta: mbrcelic@unisb.hr
[3] Srednja škola Matije Antuna Reljkovića, Ivana Cankara 76, 35000 Slavonski Brod, Hrvatska, ePošta: jasna.vujcic@gmail.com

Sažetak: U suvremenom bankarskom poslovanju, učinkovita naplata plasmana poslovnim subjektima neraskidivo je povezana s osiguranjem kibernetičke sigurnosti. Složen proces naplate obuhvaća kontinuirano praćenje dospjelih obveza za različite vrste plasmana (dugoročni i kratkoročni krediti, revolving krediti, garancije i dr.). Kreditni plasmani i garancije, kao značajan dio bankarskog portfelja, predstavljaju kompleksan i obimom velik segment naplate, zahtijevajući precizno praćenje dinamike plaćanja i promptnu reakciju na eventualna kašnjenja. Komunikacija s poslovnim subjektima tijekom procesa naplate izložena je sve većem riziku kibernetičkih napada, čime kibernetička sigurnost postaje nezaobilazan element. Ovaj rad stoga ima za cilj detaljno opisati proces naplate plasmana poslovnih subjekata te istražiti i analizirati njegovu povezanost s kibernetičkom sigurnošću. Autori u radu koriste niz znanstvenih metoda istraživanja (metode analize, komparacije, indukcije, dedukcije, deskripcije i klasifikacije itd.) kao i pojedine statističko-matematičke metode. Metodologija istraživanja temeljena je na metodi ankete putem instrumenta anketnog upitnika on-line. Dobiveni rezultati istraživanja pokazuju da određena razina kibernetičke sigurnosti značajno doprinosi uspješnosti naplate plasmana unutar bankarskog sustava.
Rad je proizašao iz područja teme obranjenog diplomskog rada pod naslovom "Naplata plasmana poslovnih subjekata kod banaka."

Ključne riječi: banke, kibernetička sigurnost, kreditni plasmani, poslovni subjekti.

1. Uvod

Sveprisutna digitalna transformacija unutar financijskog sektora uvela je određene pogodnosti, mijenjajući način na koji banke posluju i komuniciraju s poslovnim subjektima. No, ova tehnološka prednost istovremeno pojačava rizike kibernetičke sigurnosti. Banke su sve češće ovisne o IT sustavima za većinu ključnih operacija, od upravljanja podacima klijenata i transakcijama do automatizacije složenih procesa dubinske analize (Anand i ostali, 2023.). Financijski sektor koji raspolaže velikim brojem osjetljivih podataka i predstavlja potencijal za financijsku dobit, ostaje primarna meta kibernetičkih napada. Uspješni kibernetički incidenti mogu dovesti do ozbiljnih poremećaja, uključujući velike povrede podataka, značajne financijske gubitke te pravne posljedice za financijske institucije i njihove klijente. Visoko međusobno povezana priroda globalnih financijskih sustava implicira da se povreda u jednoj instituciji može brzo proširiti, stvarajući valovite efekte diljem cijelog sektora i potencijalno dovodeći do sistemskih rizika (Adelusi, 2022.).

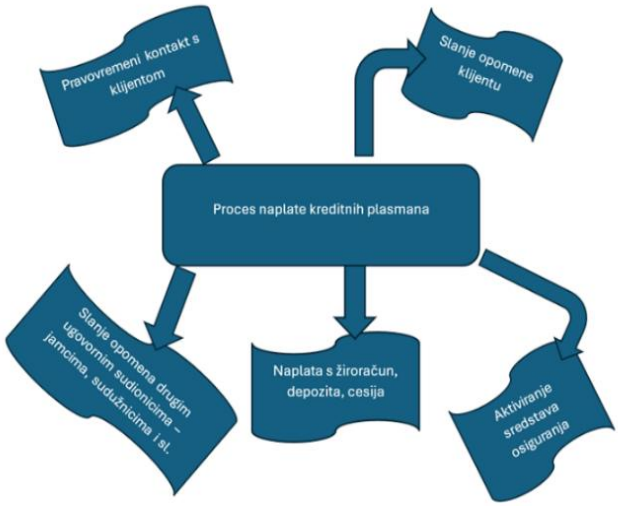
Tradicionalno, upravljanje kreditnim rizikom usredotočilo se na procjenu vjerojatnosti neispunjenja obveza, gubitka u slučaju neispunjenja obveza i izloženosti u trenutku neispunjenja obveza potencijalnih zajmoprimaca. Međutim, u suvremenom digitalnom okruženju, ovaj tradicionalni fokus mora eksplicitno integrirati kibernetički rizik, budući da kibernetički incidenti izravno utječu na financijsko zdravlje poslovnog subjekta, operativnu stabilnost te u konačnici njegovu sposobnost otplate kredita (Sheneman, 2021.).

Stoga je cilj ovog rada pružiti sveobuhvatan pregled postojećih istraživanja o analizi naplate plasmana poslovnih subjekata kod banaka s posebnim naglaskom na to kako kibernetička sigurnost utječe na taj proces.

2. Proces naplate plasmana poslovnih subjekata kod banaka i kibernetička sigurnost - dosadašnja istraživanja

Proces naplate je složen proces koji započinje praćenjem i uočavanjem promjena u financijskim pokazateljima, priljevima na žiro račun, blokadom računa i drugim relevantnim pokazateljima. Svaki plasman ima svoj rok dospijeća koji može biti različit. Dospijeće kreditnog plasmana može biti mjesečno, godišnje, polugodišnje ili sukcesivno. U fokusu djelatnika koji se bave naplatom plasmana kod banaka svakako mora biti svakodnevna kontrola zaduženja pojedinih klijenata, ali i promjene koje se događaju u životnom vijeku jednog poslovnog subjekta. Dani kašnjenja nepodmirenog dospjelog dugovanja iniciraju određenu unaprijed definiranu radnju koja bi trebala dovesti do uspješnog podmirenja duga od strane poslovnog subjekta.

Povezanost i stalna komunikacija između klijenta i zaposlenika banke je vrlo važna jer stvara osjećaj povjerenja između dvije strane. Kratkoročne plasmane je uvijek lakše naplatiti nego dugoročne. U kraćem periodu postoji manja vjerojatnost većih poremećaja u poslovanju poslovnog subjekta, a i banka ima svježe informacije o klijentu prilikom odobravanja plasmana. Banka će svakako provjeravati određene pokazatelje, poput poreznog duga te kratkoročnih blokada. Za klijente koji obavljaju svoj platni promet preko banke kod koje koriste i kreditni plasman, svakako je najbolja opcija ugovoriti i trajni nalog. Trajni nalog će omogućiti naplatu dospjelog dugovanja u svakom trenutku kada klijentu sredstva dospiju na žiro račun (Brčelić Kovačević, 2025.). Kako bi proces naplate bio uspješan on mora pratiti određene postupke prikazane slikom 1.



Slika 1: Proces naplate kreditnih plasmana; (Brčelić Kovačević, 2025.)

Za razliku od naplate dospjelih dugovanja kod kreditnih plasmana, naplata kod garancija je jednim dijelom jednostavnija i manje rizična. Kada klijenta zatraži izdavanje bankovne garancije, a banka odobri istu, potpisuje se ugovor o garanciji i banka izdaje garanciju klijentu. Ovakvi plasmani su manje rizični za banku i rijetko nastaju određeni problemi s naplatom.

Bez obzira o kakvoj se vrsti nepodmirenog dugovanja radi, djelatnici

trebaju imati redovnu komunikaciju s klijentom i to na sljedeći način:
1. obavijestiti klijenta o dugovanju,
2. poslati pisanu opomenu,
3. ponovno kontaktirati klijenta telefonski, e-mailom, SMS porukom i sl.,
4. blokirati klijenta ako nema pomaka u dogovorima ili je prošao veći rok nego što je propisano u ugovoru,
5. ponovno pokušati uspostaviti komunikaciju s klijentom kako bi se pronašlo rješenje za podmirenje dugovanja (Brčelić Kovačević, 2025.).

Sve radnje koje se poduzimaju za naplatu najviše su vezane uz starost duga. Tako se u određenim danima kašnjenja definira određena radnja. Djelatnik u naplati mora biti fleksibilan i prilagodljiv klijentu te donositi brze odluke kako bi naplata dugovanja bila što uspješnija. Stres u ovom poslu je na vrlo visokoj razini. Djelatnici se nose s velikim stresom za koji moraju pronaći način kako ga eliminirati. Dodatan stres svakako je i kibernetička sigurnost prilikom komunikacije s klijentima (Brčelić Kovačević, 2025.).

Financijski sektor posluje unutar stalno razvijajućih i sve sofisticiranijih kibernetičkih prijetnji potaknutih tehnološkim napretkom i domišljatošću zlonamjernih aktera (Bowcut, 2025.). Postoji nekoliko načina za kibernetičke napade unutar financijskog sektora:
1. Zlouporaba umjetne inteligencije i strojnog učenja - dok financijske institucije koriste AI za poboljšanu sigurnost, kibernetički hakeri usvajaju te tehnologije za stvaranje uvjerljivijih phishing napada, automatizaciju iskorištavanja ranjivosti i razvoj prilagodljivog zlonamjernog softvera (Anand i ostali 2022.).
2. Ransomware - ovi napadi razvili su se izvan pukog šifriranja podataka i uključuju eksfiltraciju podataka (poznatu kao dvostruka iznuda), povećavajući njihov utjecaj (Khemka, 2024.).
3. Phishing napadi - ovo su raširene taktike socijalnog inženjeringa, često isporučene putem poruka ili e-pošte, osmišljene da iznude od korisnika osjetljive podatke poput vjerodajnica za prijavu ili brojeva kreditnih kartica.
4. Distribuirani napadi uskraćivanja usluge - ovi napadi imaju za cilj poremetiti normalan promet poslužitelja, usluge ili mreže preopterećenjem online sustava banke prekomjernim volumenom prometa, čime se blokira pristup legitimnim korisnicima bankarskim uslugama.
5. Rizik trećih strana i ranjivosti udaljene radne snage - sve veća ovisnost financijskih institucija o dobavljačima trećih strana za razne usluge (npr. usluge u oblaku, alati za upravljanje rizikom) znači da svaki dobavljač predstavlja potencijalnu metu za kibernetičke napade. Uspješan napad na dobavljača može poremetiti kritične bankarske usluge i izravno utjecati na klijente. (Jasinska; Dobosz, 2025.).
6. Mobilne ranjivosti - s povećanim korištenjem mobilnog bankarstva, mobilni uređaji postali su značajne mete za kibernetičke prijetnje. Napadači mogu iskoristiti nedostatke u mobilnim bankarskim aplikacijama za zarazu uređaja zlonamjernim softverom ili dobivanje neovlaštenog pristupa korisničkim računima (Alsakini i ostali, 2024.).

U konačnici moguće je zaključiti da je iskustvo djelatnika banke u komunikaciji s klijentom izuzetno važno kako bi se izbjegli neželjeni kibernetički napadi.

3. Metodologija i rezultati istraživanja

Metodologija istraživanja temeljena je na metodi ankete putem instrumenta anketnog upitnika on-line. Istraživanje je provedeno u svibnju i lipnju 2025. godine, na reprezentativnom uzorku od 204 ispitanika. Istraživanje je provedeno na području istočne, sjeverne i središnje Hrvatske.

Ciljna skupina uzorka obuhvaćala je djelatnike unutar financijskih institucija (posebice banka) koji sudjeluju u

procesu naplate kreditnih plasmana njihovih klijenata te su svakodnevno izloženi i kibernetičkim napadima. Anketni upitnik bio je strukturiran u dva dijela. Prvi dio upitnika odnosio se na osnovne podatke o uzorku (spol, životna dob, prebivalište i sl.). Drugi dio upitnika odnosio na pitanja vezana uz informiranost djelatnika o kibernetičkoj sigurnosti unutar njihove institucije. Cilj istraživanja je bio dobivanje informacija o adekvatnoj informiranosti djelatnika o kibernetičkoj sigurnosti unutar njihove institucije te značaju iste za uspješnost naplate kreditnih plasmana.

Sukladno predmetu istraživanja i postavljenim ciljevima, rad polazi od sljedećih istraživačkih hipoteza:
H1: Postoji statistički značajna pozitivna povezanost između razine implementiranih mjera kibernetičke sigurnosti i uspješnosti naplate plasmana poslovnim subjektima u bankarskom sektoru.

H2: Sigurnost digitalnih kanala komunikacije s klijentima (poslovnim subjektima) pozitivno utječe na brzinu i dinamiku naplate dospjelih obveza.
Za utvrđivanje povezanosti između varijabli na intervalnoj ljestvici, koje su u linearnom odnosu, korišten je Pearsonov koeficijent korelacije (r). Postojanje linearnog odnosa procijenjeno je vizualno pomoću točkastog dijagrama, promatranjem grupiranja točaka oko zamišljenog pravca.

Koeficijent r kreće se u rasponu od -1 do +1. Pozitivne vrijednosti (od 0 do 1) ukazuju na proporcionalan rast obje varijable, dok negativne vrijednosti (od 0 do -1) označavaju obrnutu proporcionalnost - rast jedne varijable praćen je padom druge.

Vrijednost 0 označava odsutnost linearne povezanosti, što znači da varijable ne dijele zajedničku varijancu. Statistička obrada podataka provedena je u programskom paketu Statistica.

Tablica 1. Korelacijske istraživačke varijable - važnost pojedinih elemenata kibernetičke sigurnosti i naplate kreditnih plasmana

Varijabla	Visina budžeta namijenjenog kibernetičkoj sigurnosti	Postojanje naprednih softverskih rješenja za detekciju napada	Učestalost edukacije zaposlenika o phishing napadima i socijalnom inženjeringu	Postotak uspješno naplaćenih dospjelih potraživanja	Smanjenje udjela loših kredita u portfelju poslovnih subjekata	Skraćenje vremena od dospijeća do stvarnog priljeva sredstava
Visina budžeta namijenjenog kibernetičkoj sigurnosti	1	0.62*	0,71*	0,67*	0,77*	0,64*
Postojanje naprednih softverskih rješenja za detekciju napada	0,62*	1	0,60*	0,60*	0,66*	0,64*
Učestalost edukacije zaposlenika o phishing napadima i socijalnom inženjeringu	0,71*	0,60*	1	0,59*	0,61*	0,51*
Postotak uspješno naplaćenih	0,67*	0,60*	0,59*	1	0,56*	0,56*

dospjelih potraživanja						
Smanjenje udjela loših kredita u portfelju poslovnih subjekata	0,77*	0,66*	0,61*	0,56*	1	0,41*
Skraćenje vremena od dospijeća do stvarnog priljeva sredstava	0,64*	0,64*	0,51*	0,56*	0,41*	1

Izvor: autor
*Korelacija je značajna na razini od 0,01
0 < | r | < 0,25 - slaba jačina korelacije između varijabli
0,25 < | r | < 0,64 - srednja jačina korelacije između varijabli
0,64 < | r | < 1 - čvrsta jačina korelacije između varijabli

Korelacija odnosno mjera stupnja linearne povezanosti između pojedinih bitnih varijabli za provedeno istraživanje prikazana je u tablici 1. U radu je prikazan izračun korelacijskih vrijednosti između pojedinih elemenata kibernetičke sigurnosti i naplate kreditnih plasmana.

S obzirom na izračun korelacijskih vrijednosti između pojedinih elemenata kibernetičke sigurnosti i naplate kreditnih plasmana moguće je zaključiti da dobiveni rezultati ukazuju na postojanje pozitivne povezanost između svih istraživanih varijabli iz anketnog upitnika. Za većinu varijabli postoji srednja jačina povezanosti, dok čvrsta jačina povezanosti postoji između čak šest varijabli. Na temelju dobivenih rezultata istraživanja moguće je zaključiti da postoji statistički značajna pozitivna povezanost između razine implementiranih mjera kibernetičke sigurnosti i uspješnosti naplate plasmana poslovnim subjektima u bankarskom sektoru. Pored toga potvrđeno je da sigurnost digitalnih kanala komunikacije s klijentima (poslovnim subjektima) pozitivno utječe na brzinu i dinamiku naplate dospjelih obveza.

Sukladno potvrđenim hipotezama moguće je zaključiti da djelatnici banaka prolaze adekvatne i pravovremene edukacije te su na vrijeme informirani o promjenama vezanim uz kibernetičku sigurnost njihove institucije.

4. Rasprava i zaključak

Digitalna transformacija bankarskog sektora donijela je mnoge prednosti, ali je istovremeno stvorila i složene kibernetičke prijetnje koje izravno utječu na naplatu plasmana poslovnih subjekata. Tradicionalni modeli procjene kreditnog rizika, iako temeljni, suočavaju se s izazovima zbog nedostatka povijesnih podataka o kibernetičkim incidentima što zahtijeva njihovu hitnu prilagodbu. Kibernetički napadi više nisu samo operativni rizici, već se izravno pretvaraju u financijske gubitke, povećane troškove zaduživanja i narušavanje kreditne sposobnosti poslovnih subjekata.

Uz ove izazove, ključno je da banke usvoje dinamičan, integriran i proaktivan pristup upravljanju rizikom. To uključuje holističku integraciju kibernetičkog rizika u sve aspekte kreditnog poslovanja, od početne procjene zajmoprimca do strategija oporavka kredita. Kontinuirano ulaganje u napredne tehnologije kibernetičke sigurnosti, svakodnevna obuka zaposlenika i usklađenost s rastućim regulatornim okvirom postaju imperativ. U konačnici, konstantna briga o kibernetičkoj sigurnosti, kako unutar

banke tako i u interakciji s klijentima, bit će temelj za osiguravanje financijske stabilnosti i povjerenja u sve digitaliziranijem svijetu.

Sukladno donesenim zaključcima veoma je važno napomenuti da će biti nužno u okviru budućih istraživanja analizirati informiranost djelatnika te ulaganje banka u kibernetičku sigurnost i u ostalim dijelovima Republike Hrvatske kao bi se jasnije dobio uvid u cjelokupni bankarski sektor.

5. Literatura

Adelusi, J. B. (2022.): Cybersecurity Regulations in the Financial Industry, ResearchGate, preuzeto 14.11.2025. https://www.researchgate.net/publication/387787224_Cybersecurity_Regulations_in_the_Financial_Industry

Alsakini, S. A. (2024.): The Impact of Cybersecurity on the Quality of Financial Statements, An International Journal, Applied Mathematics & Information Sciences, 18, No. 1, preuzeto 14.11.2025. https://digitalcommons.aaru.edu.jo/cgi/viewcontent.cgi?article=3459&context=amis

Anand i ostali (2023.): Cybersecurity and Financial Stability, ECB Banking Supervision, preuzeto 14.11.2025. https://www.bankingsupervision.europa.eu/press/conferences/shared/pdf/2024_research_conf/12_anand.pdf

Anand i ostali (2022.): Cybersecurity and financial stability, SUERF, The European Money and Finance Forum, preuzeto 14.11.2025. https://www.suerf.org/wp-content/uploads/2023/11/f_5146e571830505f01c08e5f53548d5e7_46763_suerf.pdf

Bowcut, S. (2025.): Securing financial services: A focus on cybersecurity, preuzeto 14.11.2025. https://cybersecurityguide.org/industries/financial/

Brčelić Kovačević, M. (2025). Naplata plasmana poslovnih subjekta kod bankaka, diplomski rad, Sveučilište u Slavonskom Brodu, preuzeto 14.11.2025. https://zir.nsk.hr/object/unisb:2483

Jasinska; Dobosz (2025.): Cybersecurity in Banking: Understanding the Impact - Neontri, preuzeto 14.11.2025. https://neontri.com/blog/cybersecurity-in-banking/

Khemka, A. (2024.): The impact of cyber attacks on financial institutions and the need for improved security measures, IJNRD Journal, 9, No. 10, preuzeto 14.11.2025. https://www.ijnrd.org/papers/IJNRD2410093.pdf

Sheneman, A. (2021.): Cybersecurity Risk and the Cost of Debt, SEC.gov, preuzeto 14.11.2025. https://www.sec.gov/comments/s7-09-22/s70922-20137932-308239.pdf

ANALYSIS OF COLLECTION OF PLACEMENT OF BUSINESS ENTITIES WITH BANKS IN THE CONTEXT OF CYBER SECURITY

Abstract: In modern banking business, effective payment of placements to business entities is inextricably linked to ensuring cyber security. The complex collection process includes continuous monitoring of overdue obligations for various types of placements (long-term and short-term loans, revolving loans, guarantees, etc.). Credit placements and guarantees, as a significant part of the banking portfolio, represent a complex and large-scale collection segment, requiring precise monitoring of payment dynamics and prompt reaction to possible delays. Communication with business entities during the billing process is exposed to an increasing risk of cyberattacks, which makes cyber security an indispensable element. This paper therefore aims to describe in detail the process of collection of placement of business entities and to investigate and analyze its connection with cyber security. In the paper, the authors use a number of scientific research methods (methods of analysis, comparison, induction, deduction, description and classification, etc.) as well as certain statistical and mathematical methods. The research methodology is based on the survey method using an online questionnaire instrument. The research results obtained show that a certain level of cyber security significantly contributes to the success of loan collection within the banking system.

Keywords: banks, business entities, credit placements, cyber security.