UNIVERZA V LJUBLJANI
EKONOMSKA FAKULTETA

ZAKLJUČNA STROKOVNA NALOGA VISOKE POSLOVNE ŠOLE

POMEN KIBERNETSKE VARNOSTI ZA FINTECH PODJETJA

Ljubljana, julij 2023 VANESA STUDEN

IZJAVA O AVTORSTVU

Podpisana Vanesa Studen, študentka Ekonomske fakultete Univerze v Ljubljani, avtorica predloženega dela z naslovom Pomen kibernetske varnosti za FinTech podjetja, pripravljenega v sodelovanju s svetovalcem red. prof. dr. Alešem Berkom Skokom

I Z J A V L J A M

1. da sem predloženo delo pripravila samostojno;

2. da je tiskana oblika predloženega dela istovetna njegovi elektronski obliki;

3. da je besedilo predloženega dela jezikovno korektno in tehnično pripravljeno v skladu z Navodili za izdelavo zaključnih nalog Ekonomske fakultete Univerze v Ljubljani, kar pomeni, da sem poskrbela, da so dela in mnenja drugih avtorjev oziroma avtoric, ki jih uporabljam oziroma navajam v besedilu, citirana oziroma povzeta v skladu z Navodili za izdelavo zaključnih nalog Ekonomske fakultete Univerze v Ljubljani;

4. da se zavedam, da je plagiatorstvo – predstavljanje tujih del (v pisni ali grafični obliki) kot mojih lastnih – kaznivo po Kazenskem zakoniku Republike Slovenije;

5. da se zavedam posledic, ki bi jih na osnovi predloženega dela dokazano plagiatorstvo lahko predstavljalo za moj status na Ekonomski fakulteti Univerze v Ljubljani v skladu z relevantnim pravilnikom;

6. da sem pridobila vsa potrebna dovoljenja za uporabo podatkov in avtorskih del v predloženem delu in jih v njem jasno označila;

7. da sem pri pripravi predloženega dela ravnala v skladu z etičnimi načeli in, kjer je to potrebno, za raziskavo pridobila soglasje etične komisije;

8. da soglašam, da se elektronska oblika predloženega dela uporabi za preverjanje podobnosti vsebine z drugimi deli s programsko opremo za preverjanje podobnosti vsebine, ki je povezana s študijskim informacijskim sistemom članice;

9. da na Univerzo v Ljubljani neodplačno, neizključno, prostorsko in časovno neomejeno prenašam pravico shranitve predloženega dela v elektronski obliki, pravico reproduciranja ter pravico dajanja predloženega dela na voljo javnosti na svetovnem spletu preko Repozitorija Univerze v Ljubljani;

10. da hkrati z objavo predloženega dela dovoljujem objavo svojih osebnih podatkov, ki so navedeni v njem in v tej izjavi.

11. da sem preverila verodostojnost informacij, ki izhajajo iz zapisov na podlagi uporabe orodij umetne inteligence.

V Ljubljani, dne 3.07.2023 Podpis študentke: _____

KAZALO

KAZALO TABEL

KAZALO SLIK

SEZNAM KRATIC

angl. – angleško
B2B – (angl. business-to-business); poslovanje podjetja s podjetjem
B2C – (angl. business-to-costumer); poslovanje s stranko
E2EE – (angl. end-to-end encryption); šifriranje od konca do konca
EU – Evropska unija
FinTech – (angl. Financial Technology); Finančna tehnologija
MSISDN – (angl. Mobile Station Integrated Services Digital Network); številka mobilnega telefona uporabnika
NFT – (angl. non-fungible token); nezamenljivi žetoni
P2P lending – (angl. peer-to-peer leding): posojanje med posamezniki
PIN – (angl. Personal identifiaction number); unikatna identifikacijska številka uporabnika
RegTech – (angl. Regulatory Technology); Regulatorna tehnologija
ZDA – Združene države Amerike
ZK – Združeno kraljestvo

1 UVOD

Vsako leto postaja vsakdanji svet vse bolj moderniziran in vse bolj prilagodljiv virtualnemu svetu. To spreminjanje lahko opazimo tudi v finančni industriji, saj investicije v FinTech podjetja vsako leto vse bolj rastejo. Finančna tehnologija se vse bolj povečuje, kar pomeni, da je treba analizirati vsakič večjo količino podatkov, vendar primanjkuje regulacije, katera bi skrbela za zaščito teh občutljivih podatkov pred kibernetskimi napadi in vdori hekerjev, katerim je v interesu ukrasti občutljive, osebne in finančne podatke. Podjetja so postala toliko večja tarča kibernetskih napadov med pandemijo covid-19, ko se je velik del poslovanja premestil na splet. Razlog za vso večjo razširjenostjo FinTech bank je prav zaradi njihove preprostosti, dostopnosti in mobilnosti, katere lastnosti klasične fizične banke ne morejo popolnoma zagotoviti. Kljub temu pa se že veliko klasičnih bank poslužuje spletnega bančnega poslovanja in plačevanja. Precejšnja slabost FinTech bank je, da ne morejo zagotoviti enake varnosti podatkov in stabilnosti, kot fizične banke, ker so precej investicijsko omejene za zgoraj omenjen razvoj (Varga, 2017, str. 22).

V bančništvu se kibernetska varnost realizira z raznimi zakonskimi predpisi, kateri zahtevajo varne in verodostojne storitve in opravljanje zahtevnih postopkov kibernetske varnosti in procesov s ciljem optimizacije teh bančnih storitev. Večje institucije stalno testirajo svoje ukrepe, ker ne želijo tvegati visokih kazni in izgube ugleda, saj lahko že manjši incident ogrozi varnost strank in njihovih podatkov. V ta namen uporabljajo najnovejšo tehnologijo in zaposlujejo strokovnjake na področju kibernetske varnosti, ki jih redno izobražujejo in usposabljajo. Na ta način lahko zagotovijo najvišjo raven kibernetske varnosti, ter zaupanja vredne in zanesljive storitve za svoje stranke.

Ker finančne institucije in banke nosijo odgovornost za čuvanje velikih baz osebnih in zelo občutljivih podatkov, se je treba dobro in skrbno zavarovati. Gradnja takega varnostnega sistema, ki bo poskrbel za preprečitev vdorov in kraj občutljivih podatkov je zelo zahtevna, zamudna, draga in potrebuje dovolj usposobljenih kadrov, ki bodo vzpostavili učinkovit sistem.

Za izbrano temo moje diplomske naloge sem se odločila, ker me področje varnosti v kombinaciji s tehnologijo finančnih institucij zelo zanima in, da bi bolje razumela, kako podjetja zavarujejo občutljive osebne podatke in izvedene transakcije. Prav tako bom dobila odgovor na vprašanje, ki sem si ga zastavila, in sicer ali je kibernetska varnost pomembna za FinTech podjetja.

Namen moje diplomske naloge je podrobno raziskati delovanje FinTech podjetij in ugotoviti, kako pomembna je varnost za FinTech podjetja. V zaključni nalogi sem kot paralelo v mnogih segmentih primerjala klasične banke s FinTech bankami. Namen te primerjave je, da se prepoznajo predvsem prednosti FinTech bank, ter hkrati tudi opozorijo pomanjkljivosti.

Cilj diplomske naloge je natančno definirati pomembnost, ter hkrati opredeliti in opisati oblike kibernetske varnosti v FinTech sektorju. Poleg tega bi preučila raven tveganja FinTech podjetij in investicije v varnostne sisteme, katere so potrebne za nemoteno in varno delovanje zgoraj omenjenih podjetij. V drugem delu zaključne naloge sem opravila intervju z Markom Studen, ki deluje na področju varnostnega delovanja in je odgovoren za komercialno izvedbo izdelka imenovanega ArcSight in ArcSight Operations.

Raziskovalne metode, ki sem jih uporabila pri pisanju strokovne zaključne naloge je v večini opisna metoda, s pomočjo katere sem podkrepila teoretični del pisnega izdelka. Za praktični del pa sem uporabila intervju, ki spada pod kvalitativno metodo.

Zaključna strokovna naloga je sestavljena iz teoretičnega dela, kjer sem podrobno opisala FinTech podjetja in njihovo delovanje, ter nato v drugem delu sem s svojim mnenjem in pomočjo intervjuja z Markom prišla do ugotovitve kako pomembna je kibernetska varnost za FinTech podjetja.

2 FINTECH PODJETJA

2.1 Definicija in razlaga FinTech

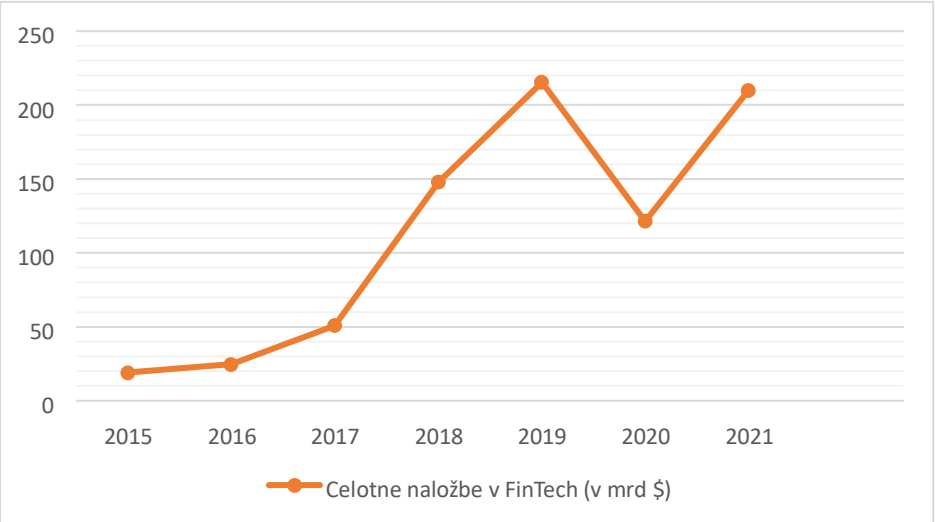
Izraz Finančna tehnologija (angl. Financial Technology, v nadaljevanju FinTech) je v zgodnjih 90ih letih prvič uporabil predsednik družbe Citicorp in ustanovitelj Smart Card Forum konzorcija – John Reed. V osnovi je definicija FinTech-a uporaba tehnologije, s katero dosežemo boljše finančne storitve. Najpomembnejši razvojni mejnik je za FinTech vsekakor dejstvo, da je z informacijsko tehnologijo naredila vse tehnološke proizvode cenejše in bolj funkcionalne. Thomas Philippon je navedel v svoji raziskavi o meritvi in teoriji finančnega posredništva, da so stroški na enoto finančnega posredništva v zadnjih 130 letih v Združenih državah Amerike (v nadaljevanju ZDA) ostali na 2%. FinTech je zavezan k odkrivanju cenejših načinov premagovanja trenj pri finančnih pogodbah in znižanju stroškov finančnih storitev za izboljšanje blaginje potrošnikov (Thakor, 2020, str. 1).

Področja, ki jih krije FinTech so naslednja: digitalna plačila in poravnave, digitalne valute, upravljanje sredstev pod katera spadajo depoziti, posojila, zbiranje kapitala in upravljanje investicij, ter zavarovanja. Študija podjetja KPMG nam razkrije, da so globalne investicije v FinTech podjetja na vrhuncu leta 2015 znašale $19.1 mrd. Med najbolj popularnimi so bile investicije v FinTech podjetja, ki se ukvarjajo s plačili, investicijami, transakcijami in upravljanjem sredstev (Thakor, 2020, str. 2).

Slika 1 prikazuje celotne naložbe v FinTech od leta 2015 naprej. Podatki so prikazani v milijardah dolarjev. Kot je razvidno iz linijskega grafikona je panoga v konstantnem porastu. Največji porast se je zgodil leta 2019, ko je industrija zrasla na $215,4 mrd. Zaradi ekstremne pandemijske situacije v letu 2020 je zabeležen skoraj polovični upad, kar pa ne preseneča,

saj so na globalni ravni to gospodarsko krizo občutila skoraj vsa podjetja v enakem ali še večjem deležu. Situacija se je v letu 2021 občutno izboljšala in je skočila nazaj na $210 mrd. V prihodnosti lahko za to panogo pričakujemo še večjo rast.

Slika 1: Celotne naložbe v FinTech od 2015 – 2021



Vir: lastno delo.

Vendar za pospešitev širitve sektor finančne tehnologije potrebuje veliko naložb. V letu 2018 so skupne naložbe v FinTech znašala $111,8 mrd., kar je 492% več kot leta 2014, ko so naložbe znašale $18,9 mrd. (Ageyev in drugi, 2020, str. 15).

Za lažje dojemanje FinTech tehnologije je potrebno dobro poznavanje tehnološke plati delovanja. Samo na kratko, čeprav to ni tema moje naloge bi povzela bistvene indikatorje tehnologije verige blokov (angl. blockchain). Tehnološkemu stebru FinTecha pravimo Blockchain tehnologija (Treleaven in drugi, 2017, str. 14).

Blockchain tehnologija je konstantno rastoča, porazdeljena knjiga blokov – to so svojevrstno identificirani, povezani transakcijski zapisi v verigi, ustvarjeni s funkcijo zgoščevanja, le – ti so kriptografsko zaklenjeni in zaščiteni z digitalnim prstnim odtisom. Vsak blok je posebej pripet na prejšnji blok s sklicevanjem na njegovo zgoščeno vrednost. Računalniki, ki so povezani s to verigo blokov, nato preverijo, če je transakcija veljavna v skladu z veljavnimi pravili, znane kot pametne pogodbe (Treleaven in drugi, 2017, str. 14).

Kot rezultat vse večjega razvoja in digitalizacije v zadnjih petih desetletjih so bile klasične finance priča velike digitalne preobrazbe. Digitalizacija ima zelo močan vpliv na finančno storitveno industrijo, saj finančni produkti skoraj v celoti temeljijo na informacijah, kot so plačilne transakcije in kreditne pogodbe, katere ne potrebujejo fizične prisotnosti. Drugi razlog je, da se skoraj vsi finančni procesi izvajajo brez fizične interakcije, kot na primer plačilo storitev in proizvodov prek spleta, trgovanje z delnicami ali kripto valutami. Izjema

so še vedno neke storitve, kot svetovanje strankam, katere se še vedno izvajajo v fizični obliki. Proces hitro rastočega razvoja informacijske tehnologije ne vodi le v večjo avtomatizacijo procesov, ampak tudi v ključno reorganizacijo vrednostne verige finančnih storitev z novimi poslovnimi modeli in z vstopanjem novih subjektov na finančni trg (Puschmann, 2017, str. 59).

Delovanje osnovnih skupin FinTech po navadi povezujemo z vlogo inovatorjev in motilcev v finančnem sektorju, ki se poslužujejo vseh razpoložljivih komunikacij, še posebej preko interneta in avtomatske obdelave informacij. Take organizacije imajo nove poslovne modele, kateri ponujajo več varnosti, učinkovitosti, priložnosti, prožnosti, kot tradicionalne finančne storitve. Pod inovatorje lahko štejemo start up podjetja (iZettle), uveljavljena tehnološka podjetja (Google) ali uveljavljene ponudnike storitev (Commerzbank) (Gomber, in drugi, 2017, str. 4).

Inovatorje lahko delimo v dve skupini, in sicer vzdrževalni FinTech ponudniki storitev, ki z uporabo tehnoloških informacij želijo zaščititi svoj tržni položaj in moteče Fintech, pod katere štejemo nova podjetja in novoustanovljena podjetja, ki izzivajo že ustaljena podjetja s ponudbo novih bolj konkurenčnih izdelkov in storitev (Gomber in drugi, 2017, str. 2).

S pomočjo FinTecha, podjetja lahko odpravijo kot spodaj navedeni najbolj pogosti poslovni težavi v finančnem sektorju (Varga, 2017, str. 26 – 27):

1. Povečanje konkurenčnosti na bančnem trgu; modernizirane informacijske tehnologije in njihov trg so prave odskočne deske za veliko število start up podjetij, saj je za uspešno poslovanje potrebno zasesti mesto v specifični tržni niši in konkurirati večjim tradicionalnim udeležencem, tako imenovanih bank.
2. Minimiziranje stroškov bančnih storitev; za FinTech podjetja je značilno, da imajo nižje provizije v primerjavi s klasičnimi bankami. Velika prednost je tudi ta, da FinTech banke ne zaračunavajo stroška upravljanja računa.

Kot sem na začetku poglavja navedla definicijo delovanja FinTecha nam olajša uporabniško izkušnjo s koriščenjem naslednjih bančnih storitev (Varga, 2017, str. 26 – 27; Gomber in drugi, 2017, str. 540; Das, 2019, str. 998):

1. Posojanje med posamezniki (angl. peer-to-peer - P2P), kjer sodelujeta samo dva udeleženca. Oseba – posojilodajalec posoja drugi osebi – posojilojemalec brez potrditve posojila s strani posrednika, kot so banke in kreditne institucije. Omenjena vrsta posojila zna biti zelo tvegana, saj ni možno preveriti kreditno zgodovino posojilojemalca in oceniti tveganost njegovega posojila. Za tako vrsto posojil so obrestne mere zelo visoke. Pri teh vrstah posojil se upniki zato odločajo za veliko manjših posojil številnejšim posojilojemalcem in se na ta način ognejo tveganju neplačila.
2. Trenutno spada finančna tehnologija med najbolj globalno rastoče in aktivne trge. Finančni, monetarni in kreditni mehanizmi so zelo hitro spreminjajoči zaradi konstantnega tehnološkega razvoja in inovacij. Kot primer lahko povzamemo prehod iz

klasičnih denarnic z gotovino in karticami, kateri se je transformiral in moderniziral v obliko elektronske denarnice. Ali pa prehod iz klasičnih bančnih posojil v spletno posojanje, ki se vrši prek spletnih transakcij. Aplikacije za spletno posojanje, katero se lahko vrši ne samo med pravnimi ampak tudi med fizičnimi subjekti, so s strani kibernetske varnosti že močno zaščitene. Na tak način uporabnikom omogočajo tudi transakcije v višjih zneskih. Skratka FinTech ni samo odlična odskočna deska za start up podjetja, ampak tudi predstavlja veliko grožnjo za klasične finančne institucije, kot so banke in kreditne agencije.

3. Najnovejši razvoj v računalniški tehnologiji se pozna tudi z veliko cenejšo in dostopnejšo strojno opremo, katera omogoča državam tretjega sveta, da se vključujejo v svet finančne tehnologije in zagotavlja posameznikom z nižjimi dohodki, da se naučijo programiranja in računalniških spretnosti, ter z izobraževalnimi materiali, kateri so na voljo na spletu. Kot primer navajam Indijo, le-ta je zgradila sodobno gospodarstvo s poceni in zanesljivo računalniško tehnologijo. Telekomunikacijska infrastruktura je instalirana v vseh večjih in bolj razvitih mestih, katera omogoča brezplačen internet ljudem na socialnem dnu.
4. FinTech podjetja ponujajo nove izdelke in rešitve, kateri izpolnjujejo potrošnikove želje in potrebe, ter jih niso mogli uresničiti v preteklosti s strani klasičnih ponudnikov finančnih storitev. Vzorčno predstavljam vzpostavitev enot za branje kartic na pametnih telefonih in tablicah, kateri to omogočajo. To prakso vse pogosteje uporabljajo ulični trgovci in potujoči prodajalci, da na tak način sprejemajo gotovinske ali kreditne kartice.
5. FinTech zagotavlja tudi novejše vrste tveganega financiranja preko množičnega financiranja (angl. crowdfunding) – ko veliko število uporabnikov prispeva manjši znesek za financiranje start upov in novih poslovnih podvigov, inovacij. Primer spletnih strani, katere ponujajo množično financiranje so GoFundMe, Kick-Starter, indiegogo in Kiva. S pomočjo množičnega financiranja se na letni ravni zbere več kot 35 mrd dolarjev, vendar pa zgoraj naštete platforme po navadi vzamejo 5 – 10 % delež zbranega denarja kot pristojbino.

2.2 Razvoj FinTech

V povezavi z zgornjo trditvijo o globalno hitrorastočem trgu FinTech tehnologije, nadaljujem s predstavitvijo razvoja le tega. Razlog za tako hitro rast je v tem, da se finančni, monetarni in kreditni mehanizmi zelo hitro spreminjajo zaradi konstantnega tehnološkega razvoja in inovacij.

Povzemam izjavo raziskovalne novinarke Amy King iz spletnega finančnega portala Unquote, katera je razvila prepričljiv argument o ustanoviteljih FinTech podjetij. Avtorica članka je skozi svoje raziskovalno delo ugotovila, da so lastniki FinTech podjetij večinoma bivši bančni delavci, kateri so posledično po veliki finančni krizi leta 2008 izgubili delovna mesta. Zaradi svojega preteklega dela imajo znanje in izkušnje za upravljanje in povezovanje finančnega sektorja s tehnologijo (Gomber in drugi, 2017, str. 541).

Kot prej navedeno je FinTech novejša dejavnost, začetki katerega segajo v 19. stoletje. Razvoj bančništva in finančnih institucij skozi čas je veliko prispeval k razvoju finančne tehnologije. Časovni presek razvoja se prepleta s tremi razvojnimi mejniki (Bates, 2015, str. 5):

1. FinTech 1.0 (1866 – 1967): se šteje kot začetek FinTech-a in sicer od vgraditve prvega čezatlantskega kabla do inovacije bankomata. Tehnološki razvoj v tem obdobju je temeljil na telegrafski povezavi, kateri je omogočal hiter prenos finančnih informacij in transakcij. Prav tako je krepil medsebojne mednarodne finančne povezave.
2. FinTech 2.0 (1967 – 2008): je obdobje, ko se je FinTech zasidral interno v sektorju, ter je bil precej prisoten pri tradicionalnih finančnih storitvah. Le-te so uporabljale finančno tehnologijo za nudenje finančnih produktov in storitev svojim strankam. Značilno za to obdobje je, da je finančna industrija pridobila nove storitve, kot so elektronski plačilni in klirinški sistemi, bankomati in spletno bančništvo. Sredi 90-ih let je finančna industrija postala največji kupec informacijske tehnologije, kjer prevladuje še sedaj.
3. FinTech 3.0 (2008 – sedanjost): od globalne finančne krize leta 2008, preko začetniških težav, ki so jih izkusila start-up podjetja, ter že obstoječa tehnološka podjetja, ki so v tem obdobju začela aktivno neposredno ponujati oziroma dostavljati finančne produkte in storitve podjetij, ter širši javnosti. V 3. obdobju so prisotne 3 različno in medsebojno odvisne sfere:

a. Bančno in finančno institucionalno sistematsko področje uporablja tehnologijo za posodobitev ali nadgradnjo korporativnih sistemov in procesov na interni ravni ali pa kot soudeleženci v konzorciju.
b. Poslovanje podjetja s podjetjem (angl. business-to-business – B2B) je druga sfera, kjer FinTech podjetje sodeluje kot partner oziroma podpornik banki, ter prodaja ali so razvija izdelke FinTech, z namenom posodobitve obstoječih storitev, ter dodatnim razvojem novih storitev – plasiranjem svojim strankam.
c. Kot primer lahko navedem podjetje Backbase, ki je specializirano za pomoč pri posodabljanju in strukturiranju vseh stičnih točk strank, ter pomaga preoblikovati ločene bančne kanale, s tem da stare oziroma zastarele aplikacije posodobi v moderno in privlačno bančno izkušnjo.
d. V poslovanju s stranko (angl. business-to-costumer – B2C) konkurirajo FinTech podjetja obstoječim bankam in finančnim institucijam, ki nudijo bančne storitve. To storijo bodisi s transformacijo običajnih izdelkov in storitev, kot na primer plačilne storitve in posojila, ki vključujejo boljšo uporabniško izkušnjo in vrednost ali pa z uporabo tehnologije za izgradnjo trga, kateri bo ustrezal potrebam običajnih ponudnikov finančnih storitev.

Finančna tehnologija, kot jo poznamo danes, je bila prvo predstavljena v regiji Južne Kalifornije imenovano Silicon Valley, katera je znana kot »tehnološka meka«. Takšno ime je dobila, ker velja za izhodišče vseh tehnoloških projektov, kateri so bili kasneje obravnavani, kot nekakšni »pospeševalci« sodobne finančne tehnologije. Dandanes se pa kot središče FinTecha priznava metropola London, prav zaradi tamkajšnje konstantne rasti

FinTech inovacij in njegovega naložbenega toka. Glavni indikatorji za tamkajšnji razvoj FinTecha so vsekakor dinamična infrastruktura, stabilen pravni red in verodostojen davčni sistem (Kalmykova in Ryabova, 2016 , str. 1).

Kot sem zgoraj omenila je bil FinTech že pred globalno finančno krizo najprej prisoten na ameriškem in evropskem trgu. Šele kasneje po letu 2008 pa se je predstavil na ruskem trgu. Razlog za poznejši vstop na ruski trg je bil politične narave, ker ni bilo tako močnega mednarodnega sodelovanja. To se je spremenilo, ko so ruski mobilni operaterji začeli sodelovati pri razvijanju mobilnih plačil. Dandanes ruski FinTech trg še vedno zamuja v primerjavi z ostalimi bolj naprednimi in hitreje rastočimi trgi, vendar pa kljub temu zelo aktivno raste (Kalmykova in Ryabova, 2016, str. 1).

Kasneje v sredini prejšnjega desetletja (po 2010) so se na finančnem trgu pojavila nova start up podjetja z vseh področij FinTech industrije, s storitvami posojil, bančništva in upravljanjem lastniškega kapitala. Med njimi najbolj izstopajo 16 najuspešnejših FinTech neobank, kot so Revolut, Monzo, Chime, Klarna, Stripe in Ant Financial. Zaradi kapitalskega deleža, ki ga posedujejo v višini več kot milijardo dolarjev posamično, se jih je prijelo ime Samorog (angl. Unicorn). Ta izraz je leta 2013 predstavil vlagatelj tveganega kapitala Alien Lee in s tem imenom definira njihovo redkost, ki meji že na mitsko kategorijo (Ageyev in drugi, 2020, str. 15).

Najnovejši razvoj v FinTech industriji je nezamenljivi žetoni (angl. non-fungible token; v nadaljevanju NFT), kateri so se pojavili leta 2014, vendar jim je popularnost neizmerno zrasla šele po letu 2020. Razlog za priljubljenost NFT je v dejstvu, da jih vse več znanih osebnosti poseduje. Velikost trga NFT je mirovala do sredine leta 2020, in sicer s povprečnim dnevnim obsegom trgovanja 60.000 dolarjev. Največji preskok se je zgodil marca 2021, ko je obseg trgovanja presegel 10 milijonov in s tem postal 150-krat večji, kot pred 8 meseci. NFT deli tudi nekatere podobnosti s kripto valutami, ker se v podobni programski shemi. Prav tako ima vsaka vrsta NFT svoje unikatne lastnosti in namene. Ker pa še vedno velja za zelo novo in neraziskano področje, je zelo malo akademskih raziskav in ugotovitev. NFT je najbolj prisoten izven klasičnega gospodarstva in trgovanja. Natančneje v umetnosti, zbirateljstvu, igrah in metaverse. Metaverse je virtualni prostor, namenjen medsebojnem druženju (Bao in Roubaud, 2022, str. 44 – 46).

2.3 Predpisi in politika FinTech (regulacija)

S prej opisanim razvojem nove tehnologije teh finančnih storitev, kateri poteka z eksponentno hitrostjo se hkrati odpirajo nove priložnosti za dodatni razvoj. Ves ta razvoj pa povečuje tudi tveganja v delovanju. Pred to negotovostjo se je potrebno primerno zavarovati.

Od finančnih nadzornikov se zahteva razvijanje novih pristopov regulacij z uporabo tehnologije, da bi uravnali prednosti inovacij in gospodarskega razvoja s finančno stabilnostjo in varstvo potrošnikov.

Kot pomemben dejavnik za tako hiter razvoj FinTecha je definitivno tudi stalna državna regulativna podpora, predvsem liberalizacija regulacije in ustvarjanje ugodnih pogojev za poslovanje, dostop do trgov in kapitala. Posledica regulacij, ter potrebo po nadzoru skladnosti in obvladovanju tveganj je pripeljalo do vzpostavljanja projektov Regulatorne tehnologije (angl. Regulatory Technology, v nadaljevanju RegTech), kot ločenega sektorja (Ageyev in drugi, 2020, str. 18).

Inštitut za mednarodne finance definira RegTech, kot vpeljavo novih tehnologij za reševanje skladnostnih in regulatornih ovir. Z uporabo inovativnih tehnoloških orodij v kombinaciji z regulativo pomagajo izboljšati kakovost, učinkovitost in skladnost sistemov finančnega sektorja, kateri omogočajo predpogoje za povečanje zaščite vlagateljev, posojilodajalcev. Med leti 2014 – 2018 so se globalne naložbe v RegTech povečale za skoraj petkrat (Ageyev in drugi, 2020, str. 18).

Dandanes so priložnosti za optimizacijo veliko bolj enostavne, s pomočjo uporabe tehnologij, kot so umetna inteligenca, obdelava naravnega jezika, veliki podatki in napredna analitika, računalništvo v oblaku, avtomatizacija robotskih procesov, porazdeljena knjižna tehnologija, vmesniki aplikacijskih programov in biometrija. Vsekakor pa ta enaka orodja lahko povzročijo nove izzive in zakonodajne posledice (Ageyev in drugi, 2020, str. 24).

Vsakodnevno se mora globalna banka spopadati kar z 185 regulativnimi spremembami oziroma bolj nazoren prikaz je, da se na vsakih osem minut zgodi sprememba. V primerjavi s tehnološkimi podjetji, ki se ukvarjajo s 27.000 predpisi, se banke vzporedno ukvarjajo s 128.000 predpisi. Med leti 2008 in 2018 so se regulatorne spremembe na razvitih trgih povečale za 1.470 %, kar je povzročilo zaposlitveno prerazporeditev v višini 25 – 30 % celotne delovne sile iz finančnega sektorja v regulativni segment (Ageyev in drugi, 2020, str. 24).

Finančne regulacije se soočajo z množičnimi izzivi, saj se finančno tehnološka panoga konstantno spreminja vzporedno z inovacijami. Največja občutna sprememba, ki se je zgodila v finančni panogi je bila vsekakor po svetovni finančni krizi leta 2008. To se je odražalo predvsem v skrbi ohranjanja finančne stabilnosti, ter v hitrosti sprememb in po povečanju števila udeležencev na trgu (Ageyev in drugi, 2020, str. 24).

Finančne institucije in ureditev se pa srečujejo s številnimi pritiski. Ti zajemajo politični pritisk za zajezitev presežkov, kot primer lahko podam Londonsko medbančno obrestno mero in indeks cen proizvajalcev, povečanje predpisov osredotočenih na Evropsko Unijo. Primer predpisa je MiFID II – direktiva o trgih finančnih instrumentov II je pravni akt Evropske unije (v nadaljevanju EU), ki zagotavlja usklajeno ureditev za investicijske storitve držav članic Evropskega gospodarskega prostora (Treleaven, 2015, str. 4).

Posledica potrebe po dinamični regulatorni ureditvi je pospešitev hitro razvijajočih novih alternativnih ponudnikov finančnih storitev, kot so PayPal, Apple Pay, Facebook in Amazon. Ključnega pomena za razvoj zgoraj omenjenih storitev je bilo vzpostavitev

ravnovesja med FinTech inovacijami in regulacijo. Omenjena vzpostavitev prinaša velik izziv, narediti finančno pregledno, učinkovito in uspešno ureditev, vendar prav tako priložnost za inovacije in analitiko velikih podatkov (Treleaven, 2015, str. 4).

Nenazadnje morajo FinTech podjetja poiskati način za optimizacijo uporabe omejenih sredstev z uporabo inovativnih tehnologij za postavitev učinkovitega sistema, ki temelji na skladnosti in pristopom usmerjenim k tveganju. Rešitev in dograditev učinkovitega sistema je mogoče le s skupnim sodelovanjem tradicionalnih finančnih institucij in z infrastrukturo FinTech podjetij (Ageyev in drugi, 2020, str. 24).

Finančne regulacije postajajo v velikih finančnih institucijah vse bolj kompleksne, saj se srečujejo z večjo količino kontrole, zakonodaje in terjajo vse večje količine natančnih podatkov o podjetjih, s katerimi zagotavljajo bolj jasno dojemanje sistemskih tveganj. Seveda pa ima kompleksnost tudi svojo ceno, s katero so strogo in zahtevno obremenjene finančne institucije. Posledično jih to odvrača od inovacij in novih finančnih produktov (Treleaven, 2015, str. 4).

Pojem RegTech je informacijska tehnologija, katera nudi pomoč podjetjem pri upravljanju regulativnih potreb in zahtev skladnosti s prepoznavanjem regulatornih vplivov na poslovne modele, izdelke in storitve, funkcionalne dejavnosti, politike, operativne postopke in kontrole. Hkrati pa omogoča skladne poslovne sisteme, pomaga pri nadzorovanju in obvladovanju regulativnih finančnih in nefinančnih tveganj in izvaja poročanja o regulativni skladnosti (Butler in O'Brien, 2019, str. 107).

Podjetje PayPal podpira uporabo novo uvedenega modela odločanja SMART upravljanja, ki je zadolženo za boljše doseganje ciljev. Opravljena plačila temeljijo na način, ki koristi vladi, potrošnikom in industriji. Omenjeni model povezuje uporabo tehnologije in podatke s sodelovalnim in iterativnim postopkom za merjenje uspešnosti, kar ustvarja bolj informiran zakonodajni razvojni proces (Treleaven, 2015, str. 9).

Globalna standardizacija pomaga pri usklajevanju podatkov, vendar je proces počasen in vsebuje omejene makro bonitetne vstopne točke. Kot primer lahko omenimo ameriški zakon o oblaku, ki pooblašča, da ponudniki oblakov, kot sta Google in Amazon, posredujejo podatke organom pregona na podlagi naloga ali ob sodnem pozivu, tudi če so podatki v drugi državi. Organi EU poročajo, da je dejanje v nasprotju s Splošno uredbo EU o varstvu podatkov, katera poudarja o nujni potrebi po posodobitvah k pogodbam o medsebojni pravni pomoči, ki vključujejo načela sorazmernosti in minimiziranje podatkov. Da bi podjetja delovala v skladu z obema načeloma morajo v celoti razdeliti svojo mrežo, kar pa predstavlja precejšnjo ranljivost za zaprte podružnice (Buckley in drugi, 2019, str. 22).

2.4 Zakaj je kibernetska varnost pomembna?

Internet in informacijska tehnologija sta spremenila svet in s tem odprla vrata v globalno gospodarstvo za nove priložnosti in izzive. Redna uporaba interneta in informacijske tehnologije, ter hranjenje občutljivih osebnih podatkov na spletu, pa prinaša tudi številne nevarnosti, pred katerimi se je potrebno primerno in pravočasno zavarovati (Spidalieri in Kern, 2014, str. 220 – 225).

Veliko javnih, zasebnih podjetij in vladnih organizacij je tarča kibernetskih napadov s strani hekerjev, kriminalcev, teroristov, državnih in nedržavnih subjektov z interesom kraje občutljivih osebnih podatkov, denarja in drugih dobičkonosnih dobrin. S konstantnim naraščanjem in transformacijo digitalizacije podjetij se povečuje tudi interes in motivacija za kibernetske napade.

Če podjetje ne vzpostavi dobro in učinkovito kibernetsko varnost, lahko pride do številnih kibernetskih groženj. Te ključne in najpogostejše grožnje v digitalnem finančnem sektorju so vdori v informacijski sistem, kraja in prodaja občutljivih podatkov, ter kraja denarja. Prav te naštete grožnje so razlog za uvedbo splošne regulacije, katero lahko razvrstimo v 4 večje kategorije (Buckley in drugi, 2019, str. 10):

1. Finančno stabilnost lahko tretiramo kot negativno v primeru izogibanju kriz ali kot pozitivno v primeru, da finančni sistem ustrezno deluje.
2. Pri finančni integriteti je fokus na preprečevanju kriminalnih aktivnost, oziroma izkoriščanje finančnih trgov za pranje denarja, financiranja terorizma, mednarodnega organiziranega kriminala, ter državno organiziranih napadov.
3. Zaščita potrošnika se osredotoča na sisteme za preprečevanje zlorabe potrošnikov.
4. Finančna učinkovitost, razvoj in vključevanje funkcij finančnega trga se navezujejo na vprašanje, kako podpreti in okrepiti pozitivno delovanje in vlogo finančnega sistema.

Finančna kriza v 2008 je finančne institucije podučila, da je treba preučiti in identificirati morebitne kanale sistemskih groženj za izpolnjevanje finančne stabilnosti. Ob povečanju FinTech podjetij so finančne institucije v letu 2017 prepoznale največ tveganj kibernetske varnosti, kot katerekoli drugo področje. Takojšnje ukrepanje s pospeševanjem varnostnega sistema v finančnem sektorju je bilo nujno potrebno. Podjetja vsakič bolj spreminjajo strategijo varnosti iz pasivne kibernetske zaščite v aktivne kibernetske zaščite. Pasivna zaščita je v pretežni obliki reaktivna, kar pomeni, da je bolj ranljiva, ker ni v neposredni osebni interakciji. Z aktivno strategijo pa se podjetja povezujejo izven omrežja in neposredno sodelujejo s spreobrnjenimi hekerji in tistimi, ki so podjetju v preteklosti poskušali škodovati (Altman, 2018).

Po besedah predsednika banke Barclays o zaščiti bank pred vdori in krajami, John McFarlane: »naša tradicionalna obramba ni več ustrezna, da bi se zaščitili na vseh nivojih – na nivoju sistema skupne industrije, nivo podjetja ali kot posamezniki. To je vojna in vojna potrebuje aktivacijo ukrepov za vojne čase. Ni miru brez nujnosti ukrepanja.«

Kot posledica večanja kibernetskih tveganj je veliko podjetij že začelo z novimi metodami aktivne kibernetske zaščite in ena izmed teh je iskanje sodelovanj z vojaškimi in obveščevalnimi službami. Izpostavila bi nekatere organizacije, ki to že uporabljajo in sicer: Mastercard, Visa, Citigroup, Wells Fargo, Bank of the West, Fifth Third Bank, ki so že začele razvijati sobe za kibernetsko vojno, s katerimi usklajujejo obveščevalne podatke o grožnjah in odzivih na napade. Pod pojmom kibernetska vojna soba se lahko nanaša na dejansko dobro računalniško opremljeno sobo ali virtualno programsko opremo, kjer se zoperstavijo ključni odločevalci in sprejemajo hitre odločitve v situacijah z visokim tveganjem (Altman, 2018).

Investicijske banke, za primer navajam ameriško investicijsko banko Goldman Sachs, so začele vizualizirati vojaške »vojne igre« za usposabljanje v primeru kibernetskih napadov. Veliko več finančnih podjetij je začelo vlagati v umetno inteligenco vojske, katera zaznava kriminalna dejanja s pomočjo prepoznavanja vzorcev napadov. Na tak način ujamejo kibernetske goljufe (Altman, 2018).

Podobna metodi sodelovanja z obveščevalnimi službami je metoda aktivne kibernetske zaščite, ki se že uporablja v praksi v finančnih organizacijah Mastercard in Western Union, s katero pozivajo hekerje z belimi klobuki (angl. white hat hackers), da bi preizkusili njihove sisteme kibernetske varnosti (Altman, 2018).

Hekerji z belimi klobuki (angl. white hat hackers) so znani po etičnem varnostnem hekanju. Definicija etičnega hekanja je samo testiranje in s soglasjem organizacije oziroma lastnika si z njihovim sodelovanjem prizadevajo odkriti vse ranljivosti trenutnega varnostnega sistema v organizaciji (Wikipedia, 2022).

Poleg zgoraj omenjenih metod banke pogosto nadzorujejo temni splet za vse ukradene finančne podatke. Na ta način ujamejo spletne tatove identitet. Temni splet imenujemo spodnji sloj interneta, kjer kriminalci trgujejo z ilegalnimi podatki, storitvami in izdelki.

Temni splet je podomrežje interneta, kjer ljudje povezujejo strežnika med seboj prek zasebnih omrežij. Delovanje temnega spleta temelji na tem, da so uporabniki med seboj povezani in zaščiteni pred sledljivostjo in pravnim pregonom. To pomeni, da temni splet zagotavlja 100 % anonimnost in ne sledljivost vira dejavnosti na spletu. Ogroženost finančnih institucij je že tolikšna, da predstavljajo 40 % celotne vsebine na temnem spletu njihovi ukradeni in razkriti podatki (Altman, 2018).

Primer FinTech goljufije na temnem spletu je kreiranje kozarcev. Ta izraz se uporablja za skrivanje virov transakcij v kripto valutah. Spletni goljufi to dosežejo s pošiljanjem transakcij preko kozarcev in s tem prikrijejo resnični izvor transakcije. Kozarci zamenjujejo transakcije in delujejo kot nekakšni posredniki. Za to delo potem zaračunavajo ilegalno provizijo. Kozarci so algoritemske storitve, ki se lahko samodejno povežejo z nekaterimi kripto valutami (Das, 2019, str. 995).

Vsekakor pa lahko trdimo, da prevzemanje bančnih računov postaja vse manj zahtevna grožnja, kot pa lažni računi in goljufije s sintetično identiteto, kjer so ukradeni podatki priloženi izmišljenim računom in identitetam. Sintetična identiteta je kombinacija ukradenih podatkov iz bančnih kartic ali osebnih izkaznic in izmišljenih podatkov, ki niso povezani z resnično osebo. Sintetične identitete kriminalcem omogočajo krajo sredstev, nelegalni nakup orožja in prepovedanih substanc in storitev, ter bežanje pred oblastjo in ostalih kaznivih dejanj (Altman, 2018).

Banke vlagajo v specifična varnostna orodja, katera temeljijo na načrtovanih prevarah in podvajanju podatkov. Ta varnostna orodja so dodatna varovala s pomočjo katerih ujamejo hekerje (Altman, 2018).

3 KIBERNETSKA VARNOST

3.1 Oblike kibernetske varnosti

Trenutno že skoraj vsi lastniki pametnih mobilnih telefonov uporabljajo mobilno banko, oziroma aplikacijo, preko katere lahko uporabniki upravljajo svoje finance. Le-ta postaja tudi vedno bolj pogosta oblika bančnega poslovanja, zaradi preproste in hitre uporabe. Obisk banke ni več potreben niti za odprtje bančnega računa, najemanja posojila, izvajanje transakcij. Tudi finančni nasveti od uradnega finančnega svetovalca se lahko izvajajo preko mobilne banke.

Visoka stopnja preverjanja je definirana kot postopek preverjanja pristnosti, ki uporablja elemente iz spodnjih treh naštetih kategorij (za nekatere uporabnike zadostujeta že dva elementa) (Mallat in drugi, 2004, str. 42 – 46):

1. nekaj kar uporabnik pozna (geslo);
2. nekaj kar ima uporabnik pri sebi (mobilni telefon, pametna kartica);
3. nekaj kar je sam uporabnik (biometrija – prstni odtisi, skeniranje mrežnice ali šarenice).

Med uporabniki postaja mobilno bančništvo vse bolj priljubljeno zaradi prihranka lastnega časa in neodvisnosti od kraja uporabe. Za identifikacijo uporabnika mobilnih bančnih storitev je dovolj že osebna mobilna naprava. Kljub dvomom o varnosti teh identifikacij, uporabniki z zaupanjem sprejemajo uporabo preprostih identifikacijskih metod, kot so številka mobilnega telefona uporabnika (angl. Mobile Station Integrated Services Digital Network – MSISDN) in unikatna identifikacijska številka uporabnika (angl. Personal identification number, v nadaljevanju PIN) za avtorizacijo mobilnih mikroplačil (Mallat in drugi, 2004, str. 42 – 46).

Kot prej omenjeno poznamo več stopenj preverjanja. Prav tako so tudi bančne kartice zavarovane s PIN številko, katera prepreči zlorabo kartice. Plačila s kartico lahko ločimo na mikroplačila in markoplačila. Mikroplačila so vsi manjši zneski plačil, ki vključujejo

možnost nakupa mobilnih vsebin in storitev, kot so novice, igre, vstopnice. Na fizičnih prodajnih mestih pod mikroplačila lahko štejemo nakup pijač in hrane na avtomatih, plačil parkirnine, ter plačil na samopostrežnih blagajnah. Vključujejo tudi plačila v manjših zneskih v trgovinah in restavracijah, pri katerih običajno ne potrebuješ identifikacijskega potrdila. V Sloveniji je nastavljena meja mikroplačil na vrednost 25 evrov, to pomeni, da za nakupe do te vrednosti ne potrebuješ PIN številke (Mallat in drugi, 2004, str. 42-46).

Makroplačila so vsa plačila, ki so izvedena elektronsko v večjih zneskih (elektronsko trgovanje, vstopnice, mobilne igre) in na prodajnih mestih, kot so restavracije in trgovine. Koncept makroplačil pa se ne uporablja samo pri tradicionalnih plačilnih instrumentov ampak tudi pri digitalnih podpisih, mobilnih vladnih storitvah in nadzor mejnih prehodov (Mallat in drugi, 2004, str. 42-46).

Mnogo digitalnih denarnic ima za še večjo zaščito večkratna gesla, najpogosteje trikratna, katere se lahko odklenejo le s kombinacijo vseh gesel. Četudi je račun zaščiten s preverjanjem identitete, je ta zaščita neuporabna v primeru, da je nekdo ukradel informacije in zlorabil podatke. Sistem za preverjanje identitete ne more zaznati zlonamerne uporabe dostopanja podatkov. Ukradena številka kreditne kartice nudi spletnemu tatu popoln dostop do nakupne sposobnosti, zato je treba take kršitve odkriti s prepoznavanjem in sledenjem uporabniškega vedenjskega vzorca. To storimo z uporabo družbenih omrežij za odkrivanje anomalnega vedenja, opazovanje tujih naprav, nepričakovano vedenje pri uporabi e-pošte, nenavadne in neznane lokacije uporabe kreditne kartice. To analizo imenujemo tudi področje prilagodljive vedenjske analize, na katerega so osredotočena podjejta Bionym, EyeVerify in BioCatch (Das, 2019, str. 997).

Za obvladovanje goljufij je potrebno voditi popolno evidenco vseh transakcij. Ključnega pomena je zabeležiti vse spletne dejavnosti, da je sledenje sploh možno. Nadaljnjo je pomembno dodati tudi več faktorsko overjanje oziroma preverjanje v dveh korakih, katerega že izvajajo številne finančne institucije (Das, 2019, str. 997).

Šifriranje od konca do konca (angl. end-to-end encryption, v nadaljevanju E2EE) je pomembno pri odpravljanju napada vmesnega človeka (angl. man-in-the-middle). Predstavlja metodo varne komunikacije, brez možnosti dostopa tretjih oseb do podatkov. Medtem pa se podatki, ki so šifrirani, varno prenašajo iz enega končnega sistema v drugega in jih lahko samo druga naprava, oziroma prejemnik dešifrira. Primer aplikacije z zelo dobro razvito metodo E2EE je WhatsApp (Das, 2019, str. 997).

Najbolj učinkovita zaščita za uporabnike mobilnih bank je vsekakor biometrična prijava v spletno banko s pomočjo funkcije identitete obraza (angl. Face Identity) ali prstnim odtisom, katera sta na voljo na vseh pametnih telefonih. Večina bančnih aplikacij zahteva osebno geslo, kjer lahko dodatno nastaviš še biometrično prijavo za boljšo zaščito. Samo geslo je neučinkovito, saj se ga brez problema dokaj hitro razkrije. Biometrična prijava je zelo varna,

saj je tehnologija le-te toliko napredna in natančna, da je nemogoče brez fizične prisotnosti te osebe vdreti v mobilni bančni račun.

3.2 Tveganja kibernetske varnosti

Kot sem že zgoraj omenila je v FinTech podjetjih vključenih ogromno tveganj. Ena izmed ključnih oblik in tradicionalnih tveganj v tehnologiji in njej povezanih podjetij je operativno tveganje. Operativno tveganje je eden izmed najbolj pogostih oblik tveganj, s katerim se srečujemo v vseh podjetjih in organizacijah. Poleg operativnega tveganja se pogosto srečujejo tudi s kreditnim, tržnim in pravnim tveganjem (Buckley in drugi, 2019, str.11).

Zaradi pojavljanja digitalizacije in datafikacije v podjetjih je pomembno, da posebej ločimo tehnološka tveganja, v katerih so vključena vsa tveganja povezana z digitalizacijo, kibernetsko varnostjo in zasebnostjo občutljivih in nejavnih podatkov. Ta oblika tveganja presega tradicionalno kategorizacijo operativnih tveganj. Tehnološka tveganja nastanejo v okviru posamičnih institucij in v medsebojnih odnosih med institucijami. Pomembno je razumeti, da imajo tehnološka tveganja velik vpliv na neposredno zaupanje in finančno stabilnost finančnega sektorja (Buckley in drugi, 2019, str.11).

Posledica vse večjega investiranja in zanimanja v digitalizacijo financ je, da je postala kibernetska varnost eden izmed glavnih virov sistemskega tveganja v finančni sistem. Sam razvoj finančne ureditve je zato posledično še bolj dal poudarek na reševanju sistemskega tveganja (Buckley in drugi, 2019, str.12).

Splošna klasifikacija kibernetskih napadov je teoretično strukturirana iz treh slojev, pri čemer notranji sloj predstavlja osnovne napade, ki so po navadi nezahtevni in oportunistični napadi in so razširjeni v javnosti z namenom izkoriščanja že obstoječih slabosti v informacijskih sistemih. Srednji sloj predstavlja napade zlonamerne programske opreme in je malo bolj napredna različica osnovnih napadov, ki imajo določeno stopnjo prilagajanja glede na ciljno panogo. Zunanji sloj pa sestavljajo bolj izpopolnjeni in napredni kibernetski napadi, ki so prilagojeni in osredotočeni na posamezno podjetje, z namenom škodovati točno tej organizaciji. Delujejo bolj na sofisticiran način in se jih je zelo težko obraniti. Večina napadov, ki se zgodijo, spadajo v kategorijo naprednih napadov (Zhuo in Solak, 2014, str. 2).

Nešifrirani podatki so ena izmed največjih nevarnosti in napak, katere lahko nastanejo v organizaciji. Vsi shranjeni podatki v sistemu morajo biti zaščiteni z unikatnimi šiframi. Čeprav hekerji lahko ukradejo tudi šifrirane podatke, jim je uporaba precej otežena, ker jih morajo najprej dešifrirati, kar jim vzame precej časa in so zato hitreje izsledljivi.

Resne posledice lahko pustijo tudi zlonamerne programske opreme, kajti vsaka neznana programska oprema, ki jo naložimo na telefon, računalnik, tablici itd. lahko povzroči ogromno škodo na napravi. Pred tako nevarnostjo se zavarujemo s požarnim zidom, s

pomočjo katerega se blokirajo prenosi škodljivih programov in virusov. Med najbolj znane zlonamerne programske opreme sodijo: računalniški virusi, trojanski konji, črvi in vohunska programska oprema (Srivastava in Kumar, 2023, str. 2 – 3).

Novejša vrsta nevarnosti je spletna prevara, s katero se hekerji s pomočjo ponarejanja lažno predstavijo, kot uradna spletna stran finančne institucije, ki izgleda enako kot prava stran. Ko obiskovalec vnese svoje podatke za prijavo v banko, jih hekerji ukradejo. Zato je potrebno, da se finančna institucija poveže s podjetji, katera lahko vnaprej predvidevajo grožnje in jih pravočasno preprečijo. Primer takega podjetja je Q6Cyber (Srivastava in Kumar, 2023, str. 3).

Spremenjeni in zmanipulirani podatki so podatki, ki so bili spremenjeni s strani hekerjev in se jih zelo težko predvidi. Ta napad finančni instituciji povzroči ogromno denarno škodo, saj spremenjeni podatki bistveno ne odstopajo od nespremenjenih, zato jih je nemogoče razlikovati (Srivastava in Kumar, 2023, str. 3).

Da bi banke bile bolj uporabne in koristne za končne uporabnike, se povezujejo in zakupijo storitve tretjih oseb. V primeru, da ponudnik storitev nima dobro razvitih ukrepov kibernetske varnosti, lahko tudi mi utrpimo posledice. To lahko preprečimo, da temeljito preverimo ponudnika in segmentiramo. Ključnega pomena je upoštevanje posledic kibernetske varnosti, ko vključujemo ponudnika. Po pregledu je pomembno, da ponudnika vprašamo, kateri podatki se bodo delili, kje bodo shranjeni, kako jih varujejo in kdo je odgovoren, če pride do kršitev. Varno poslovanje si lahko zagotovimo tudi z izvajanjem več faktorske avtentikacije med samimi dobavitelji in tako preprečimo napade (Zhuo in Solak, 2014, str. 2).

3.3 Investiranje v kibernetsko varnost

Iz vidika pomena kibernetske varnosti za obstoj in normalno delovanje vsakega podjetja, se postavlja ključno vprašanje, in sicer: Koliko bi bilo potrebno vložiti v kibernetsko varnost in vrste teh storitev?

Ker imajo organizacije omejena sredstva je odgovor na to vprašanje dokončna odločitev o dodelitvi sredstev. Rešitev o dodelitvi sredstev je dobra iztočnica ocen stroškov in koristi, katero imenujemo analiza stroškov in koristi, ki so povezani z naložbami v kibernetsko varnost. To pomeni, da dokler pričakovane dodatne koristi presegajo pričakovane dodatne stroške je smiselno povečati naložbe v kibernetsko varnost. Iz ekonomskega vidika leži optimalna raven naložbe v kibernetsko varnost za neko podjetje na točki, kjer so pričakovani mejni stroški naložbe enaki pričakovanim mejnim koristim, ki izhajajo iz te naložbe (Gordon in drugi, 2016, str. 2).

Velikost investicije v kibernetsko varnost se pa seveda razlikuje glede na velikost in prepoznavnost podjetja, saj je večje podjetje z večjo prepoznavnostjo veliko večja in bolj pomembna tarča izkušenih hekerjev in napadalcev.

Kot vpogled v resnost te problematike navajam, da so izgube velikih podjetij s 500 do 1000 zaposlenimi, ki so izpostavljeni tudi do 100 kibernetskih napadov na teden, velike od 1.4 milijonov do 46 milijonov ameriških dolarjev škode na leto (Zhuo in Solak, 2014, str. 1).

Izgubo in posledico kibernetskih napadov je mogoče omiliti z investiranjem v tehnologijo in storitve, ki preprečijo nadaljnje kibernetske napade in okrepijo varnostni sistem podjetja. Kibernetska varnost je sestavni element pri upravljanju podjetja in pomen kibernetske varnosti je kot ključno področje za uspešno poslovanje podjetja (Zhuo in Solak, 2014, str. 1).

Protiukrepi kibernetske varnosti so niz varnostnih ukrepov, katerih cilj je zaščititi premoženje podjetja pred potencialnimi kibernetskimi napadi. Protiukrepe lahko razdelimo v dve skupini, in sicer preventivni protiukrepi, kateri vključujejo metode šifriranja, uporaba forenzičnih orodij in sezname za nadzor dostopa, namenjenih pripravi podjetja na kibernetske napade. Druga kategorija so detektivski protiukrepi, ki so posvečeni prepoznavanju in odstranitvi kibernetskega napada med ali po napadu. Orodja, katera uporabljamo pri detektivskih protiukrepih so protivirusna programska oprema, požarni zidovi in sistemi za odkrivanje vdorov (Zhuo in Solak, 2014, str. 2).

3.4 Kaj lahko pričakujemo v prihodnosti?

S konstantno rastjo in napredkom v FinTech industriji lahko pričakujemo tudi povečanje varnosti občutljivih podatkov in odkrivanje novih načinov zaščite le-teh.

Inovacije in nove tehnologije, ki poskrbijo za enostavnejšo uporabo finančnih storitev, spreminjajo potrošnikovo vedenje. To je velik izziv in grožnja za tradicionalne banke, da sledijo trendu digitalizacije, s katero bi ostale na pravi poti. Prav lahko se zgodi v bližnji prihodnosti, da bodo FinTech banke zamenjale tradicionalne banke. FinTech podjetja delujejo kot banke, razmišljajo kot banke, ampak niso regulatorne kot banke (Vasiljeva, in Lukanova, 2016, str. 25).

V prihodnosti bodo finančne institucije lahko uporabile potrošnike kot aktivne branilce. Vsa podjetja, ki zagovarjajo proaktivno varnost, bodo dala možnost aktivne obrambe v roke potrošnikov. Podobno varnost so bančne institucije že začele zagovarjati z uvedbo polimorfnih kreditnih kartic. To je kartica, na katero ima potrošnik možnost povezati do 8 različnih načinov plačila. Le-ta vključuje tipkovnico z zaslonom, na kateri se z vsako transakcijo prikaže unikatna PIN koda (Altman, 2018).

V razvijanju so tudi sintetični materiali, ki se vstavijo v notranjost kartice. V primeru izgube ali tatvine te kartice, lahko lastnik pošlje signal na kartico in v tem trenutku kartica postane popolnoma neuporabna (Altman, 2018).

Poleg vseh zgoraj naštetih novosti bi primarna obramba proti kibernetskim napadom lahko postala tudi metoda s povratnim vdorom. Predlogi za legalizacijo povratnega vdora finančnim podjetjem so bili predstavljeni leta 2017 in omogočajo razkrinkanje hekerjev. Toda povratni vdor bi znal biti dokaj rizičen, saj omogoča in odpira vrata za neskončne kibernetske napade (Altman, 2018).

Ob vse večjem razvoju bodo organizacije potrebovale kvantne strategije in kvantne računalnike, da bodo ostale kibernetsko varne. Kvantni računalniki so ultra hitri in uporabljajo načela kvantne mehanike. Ti omogočajo izvajanje izračunov, z veliko močnejšo zmogljivostjo od tradicionalnih računalnikov. Veliko največjih svetovnih podjetij, kot Google, IBM, Microsoft, Airbus, HP, Samsung, Alibaba.com, Intel in Toshiba so prepoznale potencial v kvantnih računalnikih in trdijo, da je prihodnost v kvantni znanosti. Tudi investicijske banke vstopajo v kvantno znanost za izdelavo in izvajanje hitrih računov. Finančne institucije pa vsekakor potrebujejo narediti korak dlje za bolj dovršeno kibernetsko varnost s pomočjo kvantnih računalnikov. Vendar kvantni računalniki ogrožajo vse sodobne oblike varovanja občutljivih podatkov, ampak prav oni so ključni za aktivno obrambo prihodnosti FinTecha – povezovanje s spletnimi storitvami, preverjanje pristnosti plačil, preverjanje pristnosti bančnih nakazil, prenos naslovov, upravljanje identitete (Altman, 2018).

4 INTERVJU NA TEMO ZAKLJUČNE NALOGE

V nadaljevanju zaključne naloge sledi intervju z mojim bratom Markom Studen, ki je strokovnjak za varnostne operacije in je odgovoren za komercialno izvedbo izdelka za varnostne operacije imenovanega ArcSight in ArcSight Operations na angleškem trgu. Na tem področju deluje že 2,5 leti tako, da ima dober vpogled v trg kibernetske varnosti.

1. Kakšno je tvoje mnenje o kibernetski varnosti v FinTech podjetjih trenutno?

Njegov pogled v FinTech je, da je kibernetska varnost glavni fokus FinTech podjetij, z namenom, da zaščitijo podatke in stranke. Da bi preživeli, morajo to videti kot primarno operacijo za preživetje, zato morajo finančne storitve aplicirati na tehnološko varen način.

V Veliki Britaniji FinTech banka Monzo povprečno vsak dan blokira veliko količino uporabniških računov zaradi suma goljufije. Veliko bolj so previdni, ko gre za goljufije in zlorabe bančnih kartic.

2. Kaj bi po tvojem mnenju lahko izboljšali?

Kibernetska varnost je sestavljena iz treh komponent: ljudi, procesov in tehnologije. Marko deluje na tehnološki strani in njegovo stališče je večinoma na sami rešitvi, ki zagotavlja samo varnost. Le-ta je lahko zelo dobro dovršena, ampak če zaposleni nimajo pravega razumevanja do zdravih praks, je vsakršna varnost neuporabna. Kot primer navaja, da je še tako izpopolnjena tehnološka rešitev v podjetju, tudi z velikim finančnim vložkom zaman, v kolikor zaposleni brez poznavanja uporabljajo tehnologijo, ter klikajo na vse povezave. Komponenta: človeški faktor je ključnega pomena, ter je potrebno konstantno izobraževanje zaposlenih na tem področju.

Če se heker lažno predstavlja in mu uspe priti v omrežje podjetja pod lokalnim ali skrbniškim uporabniškim računom, postane organizacija zelo omejena v svojem delovanju, zaradi prisotnosti hekerjev v njihovem omrežju. Šibka točka v kibernetski varnosti so pravzaprav ljudje, vse procese pa obravnava regulativni pritisk, kateri se ukvarja s tehnologijo. Potrebno je imeti določeno rešitev, katera bo sprožila, odklapljala in analizirala, da ugotovi zlonamerne dejavnosti. Je kot tiktakajoča bomba.

Osnovni kriteriji za zagotovitev skladnosti kot nenehen proces so pogojevani z obveznimi tečaji za prihajajoči kader. Ti pomagajo zaposlenim preden jih vključijo v omrežje, kaj lahko naredijo in česar ne. Vendar kljub tečajem nekateri zaposleni niso toliko vešči in bodo zagotovo naredili napake v omrežju.

Izboljšanje kibernetske varnosti bi pomenilo še strožji nadzor nad izvajanjem procesov. To lahko storijo z implementacijo naključnih testov zaposlenih, z vprašanji o kibernetski varnosti. Te teste bi morali pogosto izvajati zlasti med zaposlenimi, ki imajo dostop do kritičnih informacij ali orodij.

Kot sem že omenil, so v kibernetski varnosti vključene tri komponente: ljudje, proces in tehnologija in vsi so enako pomembni, saj med seboj tvorijo povezano verigo. V primeru, da ena komponenta odpove, se vsa kibernetska varnost zruši. Najpomembnejši dejavnik za učinkovito varnost bi bil koherenten medsebojno povezan sistem med ljudmi, procesi in tehnologijo, pri čemer bi bili vsi učinkoviti na sprejemljivi ravni.

3. Kaj so največja tveganja kibernetske varnosti?

Tveganje kibernetske varnosti je nerazumevanje tveganj. Podjetja so izpostavljena določeni meri negotovosti in nestanovitnosti. Naloga oddelka za informacijsko varnost je, da to kvantificira in odloči, koliko tveganja je še sprejemljivo. Nikoli ne morejo pričakovati, da so 100% varni, kar tudi ni cilj. Morajo pa poskrbeti, da so dovolj varni za kritičnost informacij, ki jih držijo. Njihova drža glede kibernetske varnosti mora biti dovolj čvrsta glede na dejavnost, ki jo zastopajo in vertikalo v kateri so. Še eno tveganje je, da je organizacija v zelo kritični funkciji, ter da državna zakonodaja ne razume, kako pomembni so, oziroma v kolikšni izpostavljenosti se nahaja organizacija.

Marko mi je izpostavil dejavnosti, ki so najbolj izpostavljene napakam, katere so razvrščene po močnem tržnem pritisku – cenovni konkurenci, vendar se hkrati ukvarjajo z zelo občutljivimi informacijami o strankah. Mednje sodijo: letalski transport, hotelirstvo.

Letalske družbe so bile vedno problematične, saj poskušajo povsod znižati stroške. Panožno med seboj zelo agresivno tekmujejo in hkrati zbirajo zelo občutljive informacije, kot so podatki o kreditnih karticah in identifikacijske informacije. To je zelo slaba kombinacija dejavnosti, kjer je diferenciacija zelo nizka, zato so tudi dobički zelo nizki, saj tekmujejo med sabo samo po ceni. Posledično nimajo denarja, ki bi ga lahko porabili za kibernetsko varnost. Možnost propada je ogromna, ker razpolagajo z informacijami o milijonih ljudi. Letalska in hotelirska industrija sta zelo zapleteni in po Markovih izkušnjah se tam običajno zgodijo hude kršitve v smislu kibernetske varnosti.

4. Ali lahko uporabimo pretekle hekerske izkušnje, kot orodje za izboljšanje kibernetske varnosti?

Hekanje vsekakor pomaga organizacijam pri izboljšanju varnosti v prihodnosti. V procesu razvoja operacij, ko se pišejo novi programi ali aplikacije, vanj vgradijo razvojne in varnostne operacije. Varnostno testiranje premaknejo povsem v levo v razvojni življenjski cikel izdelka, tako da hkrati testirajo kodo, ko se ta zapisuje.

Tehnološke rešitve se implementirajo preko notranjih operativnih izpadov, oziroma ko se zaznajo kršitve, katere aktivirajo določene matrike. Za pomoč sta matriki Lockheed Martin Cyber Kill Chain in Mitre Attack, kateri učinkovito orišeta več stopenj kršitev. Ključno je, da se kršitve odkrijejo še preden se dejansko zgodijo.

Hekanje se izvaja v organiziranih skupinah z razlogom finančne koristi, ki imajo določen način delovanja z najboljšo prakso pri hekanju. Seveda se načini hekanja spreminjajo, prav tako pa se spreminjajo tudi okvirji njihovega delovanja.

5. Kaj misliš, da se bo zgodilo v prihodnosti v FinTech industriji?

Pozicija kibernetske varnosti v FinTech industriji je v zadnjih 3 letih postala zelo determinirana. Banke imajo podatkovne točke o količini blokiranih računov. V primerjavi med FinTech bankami in tradicionalnimi bankami, je ta delež pri FinTech bankah precej višji. Razlog je, ker so bolj previdni in je, regulativni okvir v katerem delujejo, precej strožji. To gre na račun tega, da v FinTech bankah bolj opazujejo, ker so novejši in so izzivalci tradicionalnim bankam. Z regulativne strani so FinTech banke zelo dobro pokrite.

Marko je mnenja, da se bo s časom in tržnim deležem, ki ga pridobijo, nanje vršil dokaj manjši regulativni pritisk, saj bodo veliko bolj dobičkonosni in bodo lahko, kot zdaj že delajo standardne banke, vse bolj lobirali pri regulatorjih. Posledično se bo regulativni pritisk zmanjšal in postali bodo uveljavljen igralec na trgu.

5 SPREMLJANJE PRIJAVLJENIH GOLJUFIJ

5.1 Primerjava prijavljenih goljufij

Kot glavno vprašanje, ki me je vodilo skozi diplomsko nalogo je vprašanje, ali so FinTech banke bolj varne kot klasične banke. Zato sem se odločila, da primerjam delež prijavljenih goljufij klasičnih in FinTech bank. Za lokacijo primerjave sem si izbrala Združeno kraljestvo (kasneje v besedilu, kot ZK) iz večih razlogov. V ZK se je, kot sem že zgoraj omenila, ustanovilo veliko FinTech podjetij in je zato tudi njegova uporaba veliko bolj pogosta, kot v drugih državah. Drugi razlog je, da je po besedah revije PCmag ZK prva po številu kibernetskega kriminala na prebivalca (Mangis, 2022).

Odgovor na zgoraj omenjeno vprašanje sem dobila s pomočjo podatkov. Prikazuje jih tabela 1, katera vsebuje število uporabnikov FinTech bank, ki so bili oškodovani s strani hekerjev in skupno število uporabnikov FinTech bank. Enake podatke sem pridobila tudi za klasične banke. Podatke sem pridobila iz aktivnih raziskav in poročil iz leta 2021. Nato sem podatke med seboj primerjala in dobila rezultat, kateri delež goljufij je večji (White in Whiters, 2022).

Tabela 1: Podatki prijavljenih goljufij v prvi polovici leta 2021

	Celotno število uporabnikov	Celotno število prijavljenih goljufij	Delež prijavljenih goljufij
Klasične banke	52,583,622	6,216,311	11.82 %
FinTech banke	14,000,000	1,491,656	10.65 %
Skupno	66,583,622	7,707,967	

Vir: lastno delo.

Podatke uporabnikov sem črpala iz uradne spletne strani vlade Združenega Kraljestva. Število goljufij klasičnih bank sem pridobila iz uradnega poročila, kjer sem našla podatek o skupnem številu prijavljenih goljufij FinTech bank (UK Finance, 2021a; UK Finance, 2021b).

Nato sem zbrane podatke vnesla v spodnjo enačbo (1), s pomočjo katere sem dobila delež prijavljenih goljufij v ZK v prvi polovici leta.

$$Delež\ prijavljenih\ goljufij = \frac{Celotno\ število\ prijavljenih\ goljufij}{Celotno\ število\ uporabnikov} \times 100 \qquad (1)$$

Po dobljenih rezultatih lahko vidimo, da so FinTech banke nekoliko bolj varne in sigurne, kot klasične banke. Delež goljufij pri klasičnih bankah znaša 11,82 % in delež goljufij pri FinTech bankah znaša 10,65 %.

5.2 Omejitve in ideje za prihodnje raziskave

Potrebno je pripomniti, da je zgornja primerjava goljufij zelo posplošena in ima več omejitev, in sicer v raziskavi nastopa več faktorjev, ki bi lahko vplivali na trenuten rezultat.

Povprečna starost uporabnika klasičnih bank je višja, kot pa uporabnika FinTech bank. Iz tega pač sledi, da sta računalniška pismenost in s tem osveščenost o možnih prevarah med mlajšo populacijo veliko bolj prisotna, kot med starejšo populacijo. Nadaljnje raziskave bi lahko potekale s točno analizo starosti uporabnikov, ter bi v prihodnosti primerjavo delali med enakimi starostnimi skupinami.

Omejitev glede na stopnjo izobrazbe. Uporabniki FinTech bank so ne samo mlajši, ampak tudi bolj izobraženi, kar posledično tudi vpliva na rezultat raziskave. Izobrazbena struktura uporabnikov bi gotovo vodila do ugotovitve, da so tehnično bolj izobraženi kadri (predvsem na področju tehnologije in informatike) tudi bolj osveščeni pri varni uporabi spletnih omrežij. Segmentiranje po izobrazbeni strukturi (ne samo po stopnji izobrazbe ampak tudi po vrsti) bi bila lahko dobra iztočnica za dopolnjevanje in nadgradnjo obstoječih FinTech storitev. Vsekakor bi si tudi ta omejitev zaslužila svojevrstno raziskovalno delo.

Primerljivost podatkov ne kaže na pretirano razliko, vendar pa je potrebno poudariti, da so klasične banke manj kontrolirane in bi z enako kontrolo, kot jo imajo FinTech banke ta korelacija bila bistveno večja na škodo klasičnih bank. Na to temo bi dodala izvleček iz zgoraj navedenega intervjuja, da so trenutno FinTech banke precej pod drobnogledom in zato bolj nadzorovane, kar se odraža z ekstremnimi kontrolnimi rezultati. Odraz tega so analitični indeksi katere sem predstavila. Po predvidevanjih bo kontroliranje FinTech bank v prihodnosti precej manj, zato bi bila raziskava čez 5 let veliko bolj primerljivejša od zgoraj predstavljene raziskave.

Podatki niso popolnoma relevantni, ker sem delala na enem podatkovnem modelu in sicer samo na trgu ZK. Tako ozka usmerjenost ne odraža pravega analitičnega dela, ker bi za primerjavo vsekakor bili dobrodošli vsaj 3 podatkovni modeli. Razmišljala sem, da bi poleg modela ZK definitivno ustrezala še dva podatkovna bolj razvita modela, in sicer ZDA in Japonske. Za ta dva modela bi se odločila predvsem na podlagi hitro rastoče tehnologije v teh dveh državah, ter kulturološke in tehnične raznolikosti.

Za nadaljevanje te raziskave bi bila lahko to dobra iztočnica za izpeljavo trenutne primerjave oziroma kreiranje novih raziskovalnih del.

6 SKLEP

V današnjem času smo priča vse večji digitalizaciji, še posebej v finančni panogi, saj digitalizacija ponuja hitrost in preprostost uporabe. Zaradi povečane uporabe storitev FinTech bank, so tudi večja tarča kibernetskih napadov in potrebujejo dobro zaščito pred takimi napadi.

V svoji zaključni strokovni nalogi sem proučila kako pomembna je kibernetska varnost za FinTech podjetja. Za ta namen sem v prvem delu zaključne naloge teoretično opisala delovanje FinTech bank in pomen kibernetske varnosti le-teh.

Teoretični del vsebuje definicijo FinTech bank, ter predstavitev delovanje FinTecha. V nadaljevanju sem opisala razvoj FinTech bank skozi čas, in povzela kako se FinTech banke zavarujejo pred kibernetskimi napadi, ter opisala metode, s pomočjo katerih banke zavarujejo svoje komitente. Kot sem omenila, so najbolj pogoste metode: sodelovanje z vojaškimi in obveščevalnimi službami, kibernetske vojne sobe in sodelovanje s hekerji z belimi klobuki (angl. white hat), kateri poskusijo vdreti v sistem FinTech bank in s tem preizkusijo kibernetsko varnost teh. Najbolj uporabljena metoda pa je nadzorovanje temnega spleta s strani banke za ukradenimi podatki.

V delu zaključne naloge, kjer sem povzela teorijo kibernetske varnosti sem opisala oblike kibernetske varnosti, tveganja s katerimi se soočajo, ter kaj lahko pričakujemo v prihodnosti. Glede na to, da je to zelo hitro rastoča dejavnost, lahko pričakujemo veliko sprememb v krajšem času. Nadaljnji razvoj kibernetske varnosti veliko vlaga v kvantne računalnike in različne sintetične materiale, ki se vstavijo v bančno kartico.

V drugem delu sem s pomočjo intervjuja z Markom prikazala njegov vpogled v delovanje kibernetske varnosti, po njegovih besedah so za kibernetsko varnost ključne tri komponente: ljudje, proces in tehnologija. Brez koherentnosti vseh treh komponent kibernetska varnost ne more pravilno delovati. Velik poudarek je na konstantnem izobraževanju kadra. V nadaljevanju sva izpostavila nivo tveganja, predvsem v letalski dejavnosti, kjer podjetja tekmujejo po ceni in posledično zmanjka denarja za kibernetsko varnost. Vpliv hekerskih izkušenj lahko pomembno vpliva na nadaljnji kibernetski razvoj. Glede prihodnosti FinTech dejavnosti je prevladalo njegovo mnenje, da bo bodo FinTech banke z zmanjšanjem regulativnega pritiska prevzele vodilno vlogo v finančni panogi.

Za lažjo predstavo sem v zaključku naloge opravila primerjavo goljufij med klasičnimi in FinTech bankami, ter povzela, da so FinTech banke nekoliko bolj varne, kot klasične banke. Utemeljitev te primerjave pa sem povzela še z omejitvami in idejami za prihodnje raziskave.

Namen naloge je bil raziskati trg FinTech bank in dokazati pomembnost kibernetske varnosti za FinTech podjetja. To sem dosegla s podrobnim branjem in analiziranjem trga finančne tehnologije iz različnih strokovnih revij in člankov te stroke in s pomočjo intervjuja, ki sem

ga opravila z Markom, v katerem je podal svoje strokovno mnenje o kibernetski varnosti in kakšna se mu zdi varnost FinTech podjetij.

Moje mnenje je, da FinTech banke precej investirajo v razvoj kibernetske varnosti, močna regulativa jih vzpodbuja, da iščejo še boljše tehnološke rešitve. Vsekakor bi prihodnost razvoja FinTech bank, ki je v strmem vzponu omogočilo nam uporabnikom varno uporabo njihovih storitev.

LITERATURA IN VIRI

1. Ageyev, D., Radivilova T. in Kryvinska, N. (2020). *Data-Centric Business and Applications: Evolvements in Business Information Processing and Management, Volume 3.* Springer.
2. Altman, W. [Will Altman]. (2018, 28.junij). *Cybersecurity in Financial Services: Future of Fintech Conference* [Youtube]. https://www.youtube.com/watch?v=x1tSXW2GBto
3. Bao, H., in Roubaud, D. (2022). Recent Development in Fintech: Non-Fungible Token. *FinTech, 1*(1), 44–46.
4. Bates, R., (2017). Banking on the Future: An exploration of FinTech and consumer interest. *Consumers International.*
5. Buckley, R. P., Arner, D. W., Zetzsche, D. A., in Selga, E. (2019). The New Risks of FinTech and the Rise of TechRisk. *UNSW Law Research Paper No. 19-89, European Banking Institute Working Paper 2019/54, University of Luxembourg Law Working Paper 2019-009, University of Hong Kong Faculty of Law Research Paper No. 2019/112, Singapore Journal of Legal Studies.*
6. Butler, T. in O'Brien, L. (2019). Understanding RegTech for Digital Regulatory Compliance. V T. Lynn in P. Rosati (ur.), *Disrupting Finance. Palgrave Studies in Digital Business & Enabling Technologies* (str. 85–102). Palgrave Pivot.
7. Das, S. R. (2019). The Future of fintech. *Financial Management, 48*(4), 981–1007.
8. Gomber, P., Koch, J. A., in Siering, M. (2017). Digital Finance and FinTech: current research and future research directions. *Journal of Business Economics, 87*(5), 537–580.
9. Gordon, L. A., Loeb, M. P. in Zhou, L. (2016). Investing in Cybersecurity: Insights from the Gordon-Loeb Model. *Journal of Information Security, 7*(2), 49–59.
10. Kalmykova, E., in Ryabova, A. (2016*).* FinTech Market Development Perspectives. *SHS Web of Conferences,* 1 – 5.
11. Mallat, N., Rossi, M. in Tuunainen, V. K. (2004). Mobile banking services. *Communications of the ACM, 7*(5), 42–46.
12. Mangis, C. (2022, 6. maj). *Which Country Has the Most Cybercrime Per Capita? It's Not the US.* https://www.pcmag.com/news/which-country-has-the-most-cybercrime-per-capita-its-not-the-us
13. Puschmann, T. (2017). Fintech. *Business & Information Systems Engineering, 59*(1), 69–76.

14. Spidaleri, F. & Kern, S. (2014*). Professionalizing Cybersecurity: A path to universal standards and status*. Salve Regina University.
15. Thakor, A. V. (2020). Fintech and banking: What do we know?. *Jornual of Financial Intermediation, 41*.
16. Treleaven, P., Brown, R. G. in Yang, D. (2017). Blockchain technology in Finance. *Computer, 50*(9), 14–17.
17. Treleaven, P. (2015). Financial Regulation of FinTech. *Journal of Financial Perspectives, 3*(3).
18. UK Finance. (2021a). *2021 Half Year Fraud Report*. UK Finance.
19. UK Finance. (2021b). *Annual Fraud Report: The Definitive Overview of Payment Industry Fraud in 2021.* UK Finance.
20. Varga, D. (2017). Fintech, the new era of financial services. *Budapest Management Review, 48*(11), 22–32.
21. Vasiljeva, T. in Lukanova, K. (2016*).* Commercial banks and FINTECH companies in the digital transformation: Challenges for the future. *Journal of Business Management, 11*, 25 – 33.
22. Zhuo, Y. in Solak, S. (2014). Measuring and optimizing cybersecurity investments: A quantitative portfolio approach. *Annual Conference and Expo of the Institute of Industrial Engineers 2014, 1*(64), 1620–1630.
23. White, L. in Whiters, I. (2021, 14. oktober). *Insight: Welcome to Britain, the bank scam capital of the world.* https://www.reuters.com/world/uk/welcome-britain-bank-scam-capital-world-2021-10-14/
24. Wikipedia. (brez datuma). *White hat (computer security).* https://en.wikipedia.org/wiki/White_hat_(computer_security)