STREDNÁ PRIEMYSELNÁ ŠKOLA ELEKTROTECHNICKÁ

**VPN**

ročníkový projekt

**JAKUB ŽÁK**

**2.D**

2024

Obsah

Obsah 2

Anotácia 3

1 VPN 4

1.1 Princíp a funkcia VPN 4

1.1.1 Účel a funkcie VPN 5

1.1.2 Bezpečnostné aspekty a súkromie v súvislosti s VPN 6

1.1.3 Bezpečnosť VPN 8

1.1.4 Princíp šifrovacieho tunela vo VPN 9

2 Tvorba učebného materiálu 10

2.1 Obsah môjho produktu 10

2.1.1 Jasné vysvetlenie základov VPN 10

2.1.2 Detailné zobrazenie princípu a fungovania VPN 11

2.1.3 Výhody a účely použitia VPN 11

2.1.4 Zabezpečenie a bezpečnosť VPN 11

2.1.5 Zameranie na jednoduchosť a zrozumiteľnosť 11

2.2 Vzhľad prezentácie 11

2.2.1 Použitie obrazkov v pozadí 12

2.2.2 Voľba vhodného písma 12

2.2.3 Farebná schéma a konzistencia 13

2.2.4 Animácie a prechody 13

2.2.5 Udržanie jednoduchosti a prehľadnosti 13

3 Záver 14

Zoznam použitej literatúry 15

Anotácia

Prvá časť práce poskytuje podrobný prehľad o virtuálnej privátnej sieti (VPN), ktorá je nevyhnutnou súčasťou súčasného digitálneho prostredia. V tejto časti sa čitateľ dozvie nielen základné definície a princípy fungovania VPN, ale aj dôležitosť a výhody, ktoré táto technológia poskytuje. Zameriava sa tiež na aspekty bezpečnosti a súkromia, objasňuje potenciálne riziká a ako sa im vyhnúť pomocou VPN.

Druhá časť práce je venovaná tvorbe prezentácie o VPN ako učebnom materiáli. Obsahuje popis každej časti prezentácie, vrátane základov VPN, princípu a fungovania, výhod použitia a bezpečnosti. Okrem toho sa zameriava na estetiku a efektivitu prezentácie vrátane výberu vhodných obrázkov, fontov a farebných schém. Cieľom tejto sekcie je vytvoriť prístupný a atraktívny materiál, ktorý umožní študentom a odborníkom lepšie pochopiť túto dôležitú technológiu.

**Annotation**

The first part of the thesis provides a detailed overview of the virtual private network (VPN), which is an essential part of the current digital environment. In this section, the reader will learn not only the basic definitions and principles of VPN operation, but also the importance and benefits that this technology provides. It also focuses on security and privacy aspects, clarifying the potential risks and how to avoid them with a VPN.

The second part of the work is devoted to the creation of a presentation about VPN as a teaching material. It includes a description of each part of the presentation, including VPN basics, principle and operation, benefits of use and security. In addition, it focuses on the aesthetics and effectiveness of the presentation, including the selection of appropriate images, fonts and color schemes. The goal of this section is to create accessible and attractive material that will allow students and professionals to better understand this important technology.

1. VPN

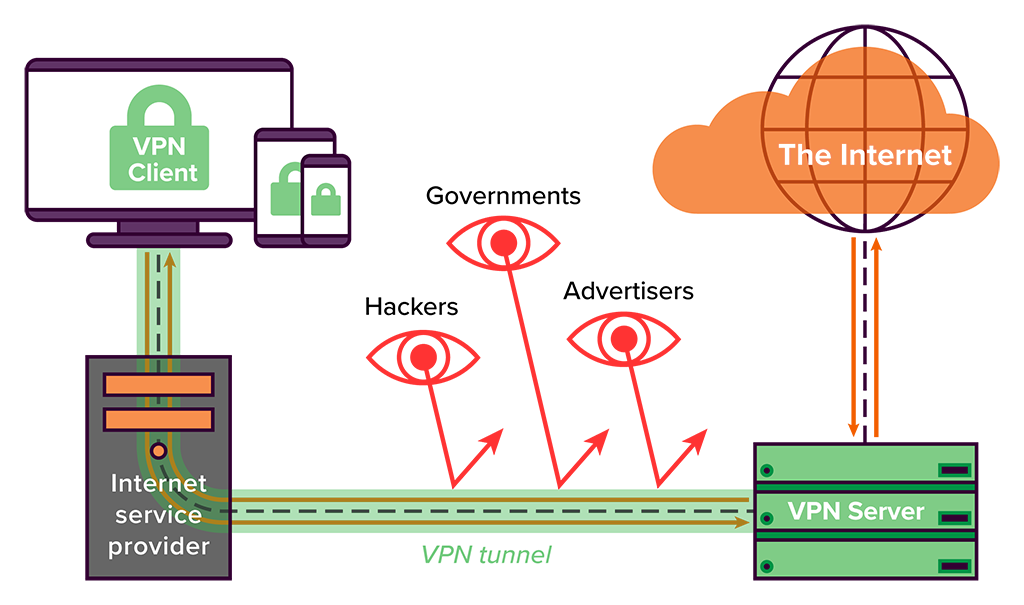
VPN je skratka pre „virtuálnu súkromnú sieť“. Je to služba, ktorá vám poskytuje bezpečný a súkromný prístup na internet. Šifrovaním vášho pripojenia VPN skryje vašu IP a online aktivitu pred špionážnymi očami a ochráni vaše údaje pred kyberzločincami. [1]

* 1. Princíp a funkcia VPN

Sieť VPN funguje tak, že internetové pripojenie zariadenia smeruje cez súkromnú službu a nie cez bežného poskytovateľa internetových služieb (ISP) používateľa. VPN funguje ako sprostredkovateľ medzi tým, že sa používateľ dostane online a pripojí sa na internet skrytím svojej IP adresy.

Pomocou VPN sa vytvorí súkromný, šifrovaný tunel, cez ktorý môže zariadenie používateľa pristupovať na internet a zároveň skryť svoje osobné informácie, polohu a ďalšie údaje. Všetka sieťová prevádzka sa odosiela cez zabezpečené pripojenie cez VPN. To znamená, že všetky údaje prenášané na internet sú presmerované do siete VPN a nie z počítača používateľa.

Keď sa používateľ pripojí na web pomocou svojej siete VPN, jeho počítač odošle informácie webovým stránkam prostredníctvom šifrovaného pripojenia vytvoreného sieťou VPN. VPN potom prepošle túto požiadavku a odošle odpoveď z požadovanej webovej stránky späť do pripojenia. [2]

4

Obr. 1 Zjednodušený VPN diagram [7]

* + 1. Účel a funkcie VPN

Namiesto odosielania vášho internetového prenosu (vyhľadávania, navštívené stránky, nahrávanie, sťahovanie) priamo vášmu poskytovateľovi internetových služieb (ISP), VPN najprv nasmeruje váš prenos cez server VPN. Týmto spôsobom, keď sa vaše údaje konečne prenesú na internet, zdá sa, že pochádzajú zo servera VPN, nie z vášho osobného zariadenia.

Bez VPN je vaša IP adresa – špeciálne číslo jedinečné pre vašu sieť – viditeľná pre web. Sieť VPN maskuje vašu IP adresu tým, že pôsobí ako sprostredkovateľ a presmeruje vašu komunikáciu. Pridáva tiež šifrovanie alebo tunel okolo vašej identity, keď sa pripájate. Kombinácia servera VPN a šifrovacieho tunela blokuje vášho poskytovateľa internetových služieb, vlády, hackerov a kohokoľvek iného, ​​aby vás pri navigácii na webe špehovali. [3]



Obr. 2 Ochrana vďaka VPN [8]

* + 1. Bezpečnostné aspekty a súkromie v súvislosti s VPN

Sieť VPN šifruje vašu komunikáciu a skryje vašu IP adresu. Vďaka tomu skryje aj vašu polohu, históriu prehliadania, vyhľadávania, sťahovanie a akékoľvek ďalšie aktivity, ako je hranie alebo streamovanie. Sieť VPN skrýva tieto informácie pred hackermi, poskytovateľmi internetových služieb, webovými stránkami a dokonca aj utláčajúcimi vládami.

IP adresa: VPN skryje vašu skutočnú IP adresu a nahradí ju IP adresou servera VPN, ku ktorému ste pripojení. To bráni ostatným sledovať vašu online aktivitu späť k vašej skutočnej polohe alebo identite.

Poloha: Zamaskovaním vašej IP adresy VPN skryje aj vašu fyzickú polohu. Aj keď sa webové stránky alebo aplikácie pokúšajú sledovať vašu polohu inými spôsobmi, ako je GPS, VPN im bráni presne určiť, kde sa nachádzate.

História a aktivita prehliadania: VPN šifruje váš internetový prenos, vďaka čomu je nečitateľný pre každého, kto sa ho pokúša zachytiť. To zaisťuje, že vaša história prehliadania, vyhľadávania, sťahovanie a ďalšie online aktivity zostanú súkromné ​​a bezpečné.

Ochrana osobných údajov: Keď používate sieť VPN, všetky údaje prenášané medzi vaším zariadením a internetom sú šifrované. To chráni citlivé informácie, ako sú prihlasovacie údaje, heslá a osobné údaje, pred zachytením hackermi alebo škodlivými subjektmi.

Prevencia obmedzovania šírky pásma: Niektorí poskytovatelia internetových služieb obmedzujú internetové pripojenia na základe typu online aktivity, ako je streamovanie videí alebo hranie hier. Sieť VPN skryje vašu online aktivitu pred poskytovateľom internetových služieb, čím im bráni obmedziť vaše pripojenie a zabezpečiť konzistentné rýchlosti. [4]

|  |  |
| --- | --- |
| Zvýšená bezpečnosť | 80% |
| Ochrana osobných údajov | 66% |
| Používanie verejnej Wi-Fi | 50% |
| Zamaskovať aktivity na internete | 33% |
| Dvojfaktorové overenie | 30% |
| Zvýšené šifrovanie | 18% |
| Vyžaduje zamestnávateľ | 16% |
| Ochrana údajov zamestnávateľa | 6% |
| Aby sa vyhli reklamám | 6% |

Tab. 1 Prečo ľudia používajú VPN? [10]

Graf. 1 Prečo ľudia používajú VPN? [10]

* + 1. Bezpečnosť VPN

Odosielanie údajov na server tretej strany sa môže zdať strašidelné, najmä ak ste to nikdy predtým neurobili. Ako zistíte, či poskytovateľ plní svoje sľuby? Aká bezpečná je VPN?

Aj keď to môže znieť ako niečo, čo by ste našli na dark webe, technológia VPN je úplne legálna, bezpečná a prístupná každému, kto by mohol chcieť chrániť svoje údaje. Organizácie používajú VPN na pridanie ďalšej vrstvy súkromia do svojej siete, zatiaľ čo jednotliví používatelia ju môžu použiť, aby zabránili podvodníkom ukradnúť ich informácie, najmä cez verejnú sieť Wi-Fi. S nárastom krádeží identity a iných foriem počítačovej kriminality nie je táto ďalšia vrstva len príjemným bonusom – je nevyhnutná na udržanie ochrany.

VPN služby a poskytovatelia sú dôležitým aspektom pre tých, ktorí hľadajú spoľahlivý a bezpečný spôsob, ako využívať VPN technológiu. Existuje mnoho komerčných VPN služieb, ktoré ponúkajú rôzne funkcie a cenové modely pre jednotlivcov aj pre firmy. Tieto služby často zahŕňajú rôzne servery umiestnené po celom svete, rôzne protokoly, možnosť použitia na rôznych zariadeniach a rôzne úrovne šifrovania a anonymizácie. Okrem toho existujú aj firemné VPN riešenia, ktoré sú navrhnuté pre špecifické potreby podnikových používateľov a často zahŕňajú možnosti ako riadenie prístupu, monitorovanie aktivít a rozšírené bezpečnostné funkcie. Pri výbere VPN služby alebo poskytovateľa je dôležité zvážiť niekoľko faktorov, vrátane úrovne bezpečnosti, dostupnosti serverov, rýchlosti pripojenia, ceny a zákazníckej podpory, aby ste našli najvhodnejšie riešenie pre vaše potreby. [5]



Obr. 3 Vpn zabezpečenie [9]

* + 1. Princíp šifrovacieho tunela vo VPN

Tunel VPN je bezpečné, šifrované spojenie medzi zariadením používateľa a internetom prostredníctvom virtuálnej súkromnej siete.

Tunel VPN šifruje internetový prenos používateľa a smeruje ho na vzdialený server VPN. Odtiaľ sú údaje dešifrované a doručené na určené miesto.

Šifrované pripojenie umožňuje bezpečnú, súkromnú cestu pre internetový prenos používateľa. V dôsledku toho zostávajú online aktivity používateľa skryté pred zvedavými očami a kybernetickými hrozbami. Tunel VPN tiež pomáha zabezpečiť dôvernosť, integritu a autentickosť všetkých údajov pri ich prenose cez verejné siete.

Tunelovanie VPN vytvára bezpečné a šifrované spojenie medzi zariadením používateľa a vzdialeným serverom VPN.

Pozrime sa, ako funguje proces tunelovania VPN:

Krok 1: Používateľ získa službu VPN a pripojí sa k požadovanému serveru prostredníctvom svojho zariadenia.

Krok 2: Klient alebo aplikácia VPN vytvorí šifrovaný tunel pre internetový prenos používateľa. Odtiaľ je prevádzka smerovaná na vzdialený server VPN cez internetové pripojenie používateľa.

Krok 3: Údaje, ktoré prechádzajú tunelom VPN, sú šifrované pomocou protokolu. Týmto spôsobom nikto nemôže zachytiť alebo získať prístup k údajom. Údaje sú tiež transformované do „šifrovaného textu“, vďaka čomu sú nečitateľné.

Krok 4: Vzdialený server VPN prijíma a dešifruje šifrovaný prenos, čo umožňuje, aby internetová prevádzka používateľa prešla do zamýšľaného cieľa. Klient a server VPN používajú na dešifrovanie údajov kľúče alebo reťazec čísel.

Krok 5: Údaje používateľa sú smerované späť zo šifrovaného tunela do jeho zariadenia, ku ktorému majú pristupovať.

Väčšina sietí VPN má tzv. “killer switche“, ktoré odpoja používateľa od tunela VPN pri prerušení spojenia, chrániac tak jeho IP adresu. Bez tohto “killer switchu“ by zariadenie automaticky prešlo na bežné pripojenie, čo by mohlo odhaliť citlivé online aktivity, napríklad online bankovníctvo. [6]

1. Tvorba učebného materiálu

Ako súčasť praktickej časti mojej ročníkovej práce som vypracoval prezentáciu o VPN, ktorá má slúžiť ako učebný materiál. Môj cieľ bol jednoznačný: vytvoriť zrozumiteľný a prístupný materiál pre tých, ktorí sa s touto tematikou ešte len zoznamujú. Tu je pohľad na to, ako som to dosiahol:

* 1. Obsah môjho produktu

V obsahu môjho produktu sa zameriavam na detailný prehľad mojej práce pri tvorbe prezentácie o VPN. Mojím hlavným cieľom bolo poskytnúť jasné a prehľadné informácie o tejto téme pre tých, ktorí sa s ňou len zoznamujú. Rozhodol som sa venovať každej časti zrozumiteľným spôsobom, aby bola pre užívateľov ľahko prístupná a pochopiteľná.

V kapitolách o základoch VPN, princípe a fungovaní VPN, výhodách a účeloch použitia VPN, ako aj o zabezpečení a bezpečnosti VPN, sa snažím prezentovať dôležité aspekty tejto technológie. Zdôrazňujem význam ochrany súkromia, bezpečnosti online aktivít a možností, ktoré VPN poskytuje.

Okrem toho som sa v poslednej kapitole zameriaval na spôsoby, ako urobiť tému VPN prístupnú a zrozumiteľnú pre širšiu verejnosť. Použil som jednoduché termíny a príklady, aby som zjednodušil komplexné koncepty a zabezpečil, že každý, bez ohľadu na svoje predchádzajúce skúsenosti, bude schopný pochopiť tému VPN.

Týmto spôsobom som sa snažil vytvoriť užitočný a informatívny materiál, ktorý pomôže ľuďom získať základné znalosti o VPN a lepšie porozumieť jeho významu v dnešnej digitálnej dobe.

* + 1. Jasné vysvetlenie základov VPN

V tejto rozsiahlej kapitole sa poglobíme do základov virtuálnej súkromnej siete. Okrem definície VPN sa budeme venovať aj histórii vzniku tejto technológie, uvádzajúc príklady z minulosti, ktoré ilustrujú potrebu a vývoj VPN služieb. Ďalej rozoberieme rôzne typy VPN a ich aplikačné oblasti v súčasnom digitálnom svete. Spojíme teóriu s praxou, prinášajúc rozsiahle vysvetlenie, ktoré pomôže čitateľovi získať komplexnejší pohľad na túto problematiku.

* + 1. Detailné zobrazenie princípu a fungovania VPN

Táto podkapitola bude podrobnejšie rozpracovaná s dôrazom na technické aspekty fungovania VPN. Okrem popisu procesu vytvárania šifrovaného tunela sa budeme venovať aj rôznym typom šifrovacích protokolov, ich silným a slabým stránkam. Vysvetlíme aj rôzne architektonické modely VPN a ich využitie v rôznych odvetviach, aby sme poskytli komplexný obraz o tom, ako táto technológia funguje v praxi.

* + 1. Výhody a účely použitia VPN

Rozsiahla analýza výhod a účelov použitia VPN zahrnie nielen obvyklé aspekty ako ochranu súkromia a bezpečnosť online aktivít, ale aj širšie súvislosti. Budeme diskutovať o dopade VPN na firemné prostredie, spoločenské súvislosti a geopolitické faktory ovplyvňujúce využitie tejto technológie. Rozoberieme aj aktuálne trendy v oblasti kybernetickej bezpečnosti a to, ako VPN prispieva k ich riešeniu.

* + 1. Zabezpečenie a bezpečnosť VPN

Táto podkapitola bude obsahovať rozšírené vysvetlenie bezpečnostných opatrení, ktoré sú súčasťou prevádzky VPN. Okrem tradičných techník šifrovania a autentifikácie sa zameriame aj na nové prístupy k zabezpečeniu VPN sietí, ako napríklad použitie rozšírenej reality alebo umelá inteligencia na detekciu hrozieb. Budeme analyzovať aj prípady útokov na VPN a spôsoby, ako sa im efektívne brániť.

* + 1. Zameranie na jednoduchosť a zrozumiteľnosť

V tejto rozšírenej časti sa budeme venovať nielen jednoduchosti obsahu, ale aj spôsobom, ako efektívne komunikovať tému VPN širokej verejnosti. Okrem príkladov a ilustrácií budeme diskutovať aj o psychologických a kognitívnych faktoroch ovplyvňujúcich pochopenie nových konceptov. Analyzovať budeme aj rôzne didaktické metódy a prístupy k výučbe VPN, aby sme našli optimálne spôsoby, ako učiť a šíriť informácie o tejto dôležitej technológii.

* 1. Vzhľad prezentácie

Pri vytváraní vizuálneho vzhľadu mojej prezentácie som venoval veľkú pozornosť niekoľkým kľúčovým aspektom, ktoré som dôkladne premyslel a upravil, aby dosiahli maximálny efekt.

* + 1. Použitie obrázkov v pozadí

Pri prehĺbení tejto časti sa budeme venovať nielen výbere vhodných obrázkov, ale aj ich historickým a kultúrnym kontextom. Budeme analyzovať vplyv vizuálnej komunikácie na porozumenie obsahu a spôsoby, ako správne interpretovať obrázky vo vzťahu k textu. Diskutovať budeme aj o etických aspektoch používania obrázkov v prezentáciách a možných dôsledkoch ich nesprávneho interpretovania.

* + 1. Voľba vhodného písma

Voľba správneho písma je kľúčovým prvkom pri navrhovaní vizuálneho dojmu prezentácie. Nie je to len otázka estetiky, ale aj funkcionality a efektívnosti komunikácie. Preto som venoval veľkú pozornosť výbere písma, aby som dosiahol optimálny vplyv na divákov.

Rozhodol som sa použiť písmo Arial, pretože je to osvedčený klasik, ktorý je všeobecne uznávaný pre svoju jednoduchosť a univerzálnosť. Jeho čistý a rovný vzhľad poskytuje stabilitu a dôveryhodnosť, čo je dôležité pre prezentáciu serióznych tém.

Pri zvážení použitia iných písiem som dospel k záveru, že Arial ponúka najlepšiu čitateľnosť a jasnosť na rôznych zariadeniach a obrazovkách. Jeho bezpochyby jednoduchý dizajn zaisťuje, že text na slajdoch bude ľahko rozpoznateľný a čitateľný nielen na počítačoch, ale aj na projekčných obrazovkách či mobilných zariadeniach.

Okrem toho, použitie jednotného písma prispieva k celkovej estetike prezentácie a pomáha udržať konzistenciu medzi jednotlivými slajdmi. Tým sa minimalizuje rozptyľovanie pozornosti divákov a zabezpečuje sa, že sa budú sústrediť na obsah prezentácie, nie na rôzne vizuálne prvky.

V konečnom dôsledku, voľba písma Arial je strategickým rozhodnutím, ktoré prispieva k efektivite a účinnosti mojej prezentácie o VPN. Je to rozhodnutie založené na zásadách jednoduchosti, univerzality a čitateľnosti, ktoré sú kľúčové pre úspešné prezentovanie informácií.

* + 1. Farebná schéma a konzistencia

Pri navrhovaní farebnej schémy som venoval osobitnú pozornosť tomu, aby bola nielen esteticky príjemná, ale aj funkčná a efektívna vo vizuálnom komunikovaní. Rozhodol som sa zostať verný zásade jednoduchosti a konzistencie, pretože viem, že to prispieva k lepšiemu porozumeniu a zapamätaniu si obsahu prezentácie.

Zvolil som neutrálnu paletu farieb, ktorá zahŕňa odtiene ako biela, sivá a béžová. Tieto farby sú univerzálne akceptované a majú tendenciu minimalizovať rušenie, čím umožňujú divákom sústrediť sa na esenciálny obsah prezentácie. Avšak, aby som dodal dynamiku a zaujatie do mojej prezentácie, pridal som niekoľko farebných akcentov na dôležité miesta, ako sú nadpisy, kľúčové pojmy alebo významné údaje.

Táto konzistentná farebná schéma nie len zabezpečuje harmóniu medzi jednotlivými slajdmi, ale aj zvyšuje vizuálnu atraktivitu celej prezentácie. Farebné akcenty slúžia nielen ako estetický prvok, ale aj ako navigačný prvok, ktorý pomáha divákom orientovať sa v obsahu a identifikovať dôležité informácie.

Celkovo, navrhovaná farebná schéma je zameraná na dosiahnutie optimálneho vizuálneho dojmu, ktorý podporuje efektívne komunikovanie obsahu prezentácie. Je to kombinácia jednoduchosti, konzistencie a šikovného použitia farebných akcentov, ktorá vytvára atraktívnu a zároveň funkčnú prezentáciu o VPN.

* + 1. Animácie a prechody

Pri používaní animácií a prechodov som sa snažil byť striedmy a funkčný. Animácie boli prítomné len tam, kde som považoval, že prispievajú k lepšiemu porozumeniu obsahu a neodvádzali pozornosť divákov. Prechody medzi slajdmi boli plynulé a diskrétne, aby prezentácia pôsobila profesionálne a elegantne.

* + 1. Udržanie jednoduchosti a prehľadnosti

Napriek estetickému zameraniu som vždy dbal na to, aby bola prezentácia jednoduchá a prehľadná. Text bol usporiadaný tak, aby bol jasne štruktúrovaný a ľahko čitateľný. Obrázky boli umiestnené tak, aby podporovali obsah a neodvádzali pozornosť od hlavných myšlienok.

1. Záver

V rámci tejto ročníkovej práce som sa podrobne venoval problematike virtuálnych súkromných sietí (VPN) a ich významu v súčasnom digitálnom svete. V teoretickej časti som podal komplexný prehľad o základných princípoch, funkciách a bezpečnostných aspektoch VPN. Zdôraznil som ich úlohu v ochrane súkromia, zabezpečení online aktivít a obmedzení rizík spojených s kybernetickými hrozbami. V praktickej časti som sa zameriaval na tvorbu prezentácie o VPN, ktorá slúži ako učebný materiál pre širokú verejnosť. Vytvoril som prehľadné a prístupné informácie o VPN, zdôrazňujúc jeho výhody, fungovanie a bezpečnostné opatrenia. Cieľom tejto prezentácie bolo poskytnúť študentom, odborníkom aj laikom zrozumiteľné informácie o dôležitosti a využití VPN v dnešnej dobe. Celkovo som presvedčený, že táto práca prispieva k lepšiemu porozumeniu VPN technológie a jej významu v súčasnom digitálnom prostredí. VPN nie je len nástroj na ochranu súkromia, ale aj prostriedok na zabezpečenie bezpečnosti a stability online prostredia. Dúfam, že moje úsilie a práca pomôžu ľuďom lepšie pochopiť túto technológiu a využiť ju na ochranu svojich online aktivít v dnešnej dobe neustále sa meniacej kybernetickej hrozby. V rámci ďalšieho výskumu by bolo zaujímavé preskúmať aktuálne trendy v oblasti VPN technológií a ich prispôsobenie sa narastajúcim požiadavkám na bezpečnosť a súkromie. S nástupom nových technologických hrozieb a legislatívnych zmien je neustále potrebné aktualizovať a zdokonaľovať metódy ochrany online prostredia. Možno rozšíriť aj obzory empirických štúdií, ktoré by preskúmali skúsenosti užívateľov s VPN službami, ich preferencie a úrovne dôvery voči rôznym poskytovateľom. Okrem toho by som rád v budúcnosti preskúmal možnosti implementácie VPN technológií v rámci firemných prostredí a inštitucionálnych sietí. Integrácia VPN do podnikových infraštruktúr môže posilniť bezpečnostné opatrenia a zabezpečiť bezpečný prístup k citlivým údajom a zdrojom. Porozumenie tohto procesu a jeho výhod môže pomôcť podnikom lepšie chrániť svoje dáta a zabezpečiť kontinuálnu prevádzku v digitálnom svete neustále sa meniacich hrozieb. Tieto budúce smerovania výskumu by mohli poskytnúť ďalšie cenné poznatky o význame a využití VPN technológií v súčasnom digitálnom veku a prispieť k ďalšiemu zlepšeniu ochrany online súkromia a bezpečnosti.

Zoznam použitej literatúry

[1] NordVPN. [online]. [Citované 2.5.2024]. Dostupné na: <https://nordvpn.com/>

[2] Fortinet. How Does VPN Work? [online]. [Citované 2.5.2024]. Dostupné na: <https://www.fortinet.com/resources/cyberglossary/how-does-vpn-work#:~:text=The%20VPN%20acts%20as%20an,%2C%20location%2C%20and%20other%20data>.

[3] Avast. What is a VPN? [online]. [Citované 2.5.2024]. Dostupné na: <https://www.avast.com/c-what-is-a-vpn>

[4] Surfshark. What Does a VPN Hide? [online]. [Citované 2.5.2024]. Dostupné na: <https://surfshark.com/blog/what-does-a-vpn-hide>

[5] Microsoft Azure. Is a VPN Safe? [online]. [Citované 2.5.2024]. Dostupné na: <https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-a-vpn#is-a-vpn-safe>

[6] Forbes. What Is VPN Tunnel? [online]. [Citované 2.5.2024]. Dostupné na: <https://www.forbes.com/advisor/ca/business/software/what-is-vpn-tunnel/#:~:text=A%20VPN%20tunnel%20is%20a,delivered%20to%20its%20intended%20destination>.

[7] Forscope. Čo je VPN? [online]. [Citované 2.5.2024]. Dostupné na: <https://www.forscope.sk/blog/co-je-vpn/>

[8] Airtel. What is VPN, Its Types and How It Works [online]. [Citované 2.5.2024]. Dostupné na: <https://www.airtel.in/blog/broadband/what-is-vpn-its-types-and-how-it-works/>

[9] Jarvee. Enhanced Privacy and Security on Social Media: How VPNs Protect Your Data [online]. [Citované 2.5.2024]. Dostupné na: <https://jarvee.com/enhanced-privacy-and-security-on-social-media-how-vpns-protect-your-data/>

[10] Forbes. VPN Statistics [online]. [Citované 2.5.2024]. Dostupné na: <https://www.forbes.com/advisor/business/vpn-statistics/>