STREDNÁ PRIEMYSELNÁ ŠKOLA ELEKTROTECHNICKÁ

**VPN**

ročníkový projekt

**Jakub Žák**

**II.D**

2024

Obsah (štýl Nadpis Kapitoly, bez čísla)

Obsah (štýl Nadpis Kapitoly, bez čísla) 2

Anotácia (štýl Nadpis Kapitoly, bez čísla) 3

1 VPN 4

1.1 Základné princípy VPN 4

1.2 Šifrovanie 4

1.3 Protokoly 5

1.4 Typy VPN 5

1.5 VPN služby a poskytovatelia 5

1.6 Príklady použitia 6

1.7 Bezpečnostné aspekty VPN 6

2 Ilustrácie, tabuľky, rovnice 7

2.1 Ilustrácie 7

2.2 Tabuľky 7

2.3 Zdrojový kód programu 8

2.4 Rovnice, vzorce 8

3 Záver 9

Zoznam použitej literatúry (Nadpis Kapitoly, bez čísla) 10

Prílohy (štýl Nadpis Kapitoly, bez čísla) 11

Príloha A – CD médium (štýl PodNadpis Kapitoly, bez čísla) 11

Príloha B – <názov prílohy> 11

Príloha C – <názov prílohy> 11

Anotácia

**Annotation**

1. VPN

VPN je počítačová sieť na prepojenie počítačov na rôznych miestach internetu do jednej virtuálnej počítačovej siete. Aj keď počítače môžu byť vo fyzicky nezávislých sieťach na rôznych miestach sveta, prostredníctvom virtuálnej privátnej siete medzi sebou môžu komunikovať, ako keby boli na jednom sieťovom segmente.

* 1. Základné princípy VPN

Virtuálna privátna sieť (VPN) je kľúčovým nástrojom pre zabezpečenie súkromia a bezpečnosti online komunikácie v súčasnom digitálnom svete. VPN vytvára šifrovanú a izolovanú sieťovú cestu cez verejnú sieť, čím umožňuje bezpečný prenos dát medzi pripojenými zariadeniami alebo sieťami. Proces tunelovania vytvára izolovaný tunel, kde sú všetky dáta šifrované, čo zaručuje ich súkromie a integritu. Taktiež VPN umožňuje užívateľom skryť svoju skutočnú IP adresu a identitu tým, že vytvára virtuálny tunel cez verejnú sieť, kde ich internetový tok je smerovaný cez VPN server. Tento proces zabezpečuje, že aktivita užívateľa vyzerá, akoby pochádzala z VPN servera, čo prispieva k anonymite a zvyšuje bezpečnosť používateľov. Okrem toho VPN umožňuje vzdialeným používateľom alebo pobočkám prístup k firemnej sieti cez verejnú sieť, čím umožňuje bezpečný prístup k firemným zdrojom z akéhokoľvek miesta a zariadenia s internetovým pripojením. VPN tiež umožňuje používateľom obchádzať geografické obmedzenia obsahu a poskytuje bezpečnú vrstvu ochrany pri používaní verejných Wi-Fi sietí, čím zvyšuje bezpečnosť používateľov pred odpočúvaním a útokmi typu Man-in-the-Middle. Tieto základné princípy VPN tvoria základný rámec, ktorý umožňuje VPN poskytovať spoľahlivú a bezpečnú sieťovú komunikáciu v dnešnom digitálnom prostredí.

* 1. Šifrovanie

Šifrovanie je kľúčovým prvkom VPN, ktorý zabezpečuje, že všetky prenášané dáta sú chránené pred neoprávneným prístupom. Keď užívateľ odosiela alebo prijíma dáta cez VPN, sú tieto dáta zašifrované pomocou špeciálnych šifrovacích algoritmov. Táto šifrovaná forma umožňuje užívateľovi a VPN serveru komunikovať bez toho, aby tretie strany mohli sledovať alebo čítať prenášané informácie. Typy používaných šifrovacích algoritmov sa môžu líšiť v závislosti od konkrétnej implementácie VPN, ale základným cieľom je vždy ochrana súkromia a bezpečnosti dát užívateľov. Silné šifrovanie je kľúčovým faktorom pri zabezpečení VPN a zvyšuje dôveru v bezpečnosť tejto technológie.

* 1. Protokoly

Protokoly sú dôležitou súčasťou fungovania VPN, keďže definujú spôsob, akým sa dáta prenášajú a šifrujú cez VPN tunel. Existuje niekoľko rôznych protokolov, ktoré sa používajú v rôznych VPN implementáciách, pričom každý má svoje vlastné výhody a obmedzenia. Napríklad protokol OpenVPN je populárnym voľbou pre svoju spoľahlivosť a flexibilitu, zatiaľ čo protokol IPSec je často preferovaný pre svoju silnú šifrovaciu bezpečnosť. Ďalšie známe protokoly zahŕňajú L2TP/IPSec, SSTP a WireGuard. Pri výbere protokolu je dôležité zvážiť potreby konkrétnej implementácie VPN, ako aj požiadavky na bezpečnosť a výkon. Správny výber protokolu môže mať významný vplyv na celkovú úroveň bezpečnosti a výkonu VPN spojenia.

* 1. Typy VPN

Existuje niekoľko rôznych typov VPN, ktoré sa používajú v závislosti od konkrétnych potrieb a použití. Jedným z najbežnejších typov je vzdialený prístupový VPN, ktorý umožňuje jednotlivcom alebo zamestnancom pripojiť sa k firemnej sieti z akéhokoľvek miesta pomocou verejnej siete, ako je internet. Ďalší typ, site-to-site VPN, umožňuje propojenie dvoch alebo viacerých sietí cez verejnú sieť, čo je ideálne pre podniky s viacerými pobočkami alebo oddeleniami. Okrem toho existujú VPN riešenia špeciálne navrhnuté pre mobilné zariadenia, čo umožňuje užívateľom bezpečný prístup k firemným zdrojom aj na cestách. Každý typ VPN má svoje vlastné výhody a použitie, a je dôležité zvážiť konkrétne požiadavky a scenáre použitia pri výbere najvhodnejšieho typu VPN pre danú situáciu.

* 1. VPN služby a poskytovatelia

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.

* 1. Príklady použitia

VPN má mnohé praktické aplikácie a príklady použitia, ktoré zvyčajne slúžia na zabezpečenie a zlepšenie online skúseností užívateľov. Jedným z najbežnejších príkladov je ochrana súkromia a bezpečnosť pri pripájaní k verejným Wi-Fi sieťam, čo môže byť problematické bez použitia VPN kvôli riziku odpočúvania a útokom typu Man-in-the-Middle. Ďalším príkladom je obchádzanie geografických obmedzení obsahu, kde používatelia môžu použiť VPN na získanie prístupu k obsahu, ktorý by inak nebol dostupný v ich regióne, ako napríklad sledovanie obsahu na streamovacích platformách. VPN tiež poskytuje bezpečný prístup k firemným zdrojom pre vzdialených pracovníkov alebo zamestnancov na cestách, čo zvyšuje produktivitu a zároveň zabezpečuje citlivé firemné informácie. Ďalšie príklady zahŕňajú zvýšenie bezpečnosti a súkromia pri online bankovníctve, anonymné prezeranie internetu a ochranu pred sledovaním online aktivít. Tieto príklady použitia jasne demonštrujú všestrannosť a dôležitosť VPN vo svete súkromnej a bezpečnej online komunikácie.

* 1. Bezpečnostné aspekty VPN

Bezpečnosť je kľúčovým faktorom pri používaní VPN a je dôležité mať na pamäti niektoré bezpečnostné aspekty. Aj keď VPN poskytuje vysokú úroveň ochrany súkromia a bezpečnosti, stále existujú niektoré potenciálne riziká, ktoré by mali byť brať do úvahy. Jedným z takýchto aspektov je dôvera v poskytovateľa VPN, pretože používatelia musia dôverovať tomu, že poskytovateľ dodržiava ich sľuby o súkromí a bezpečnosti dát. Ďalším dôležitým aspektom je výber správneho šifrovacieho protokolu a silných šifrovacích kľúčov, aby sa minimalizovalo riziko prelomenia šifrovania útočníkom. Je tiež dôležité mať na pamäti, že VPN nechráni pred všetkými typmi útokov, a preto je dôležité dodržiavať základné bezpečnostné opatrenia, ako je aktualizácia softvéru, používanie antivírusového softvéru a opatrnosť pri otváraní príloh alebo klikaní na odkazy. Zabezpečenie správneho konfigurácie a správneho používania VPN je kľúčom k zabezpečeniu súkromia a bezpečnosti online komunikácie.

1. Ilustrácie, tabuľky, rovnice

V práci sa môžu vyskytovať okrem slovného textu aj informácie vyjadrené v obrazovej forme a symbolmi.

* 1. Ilustrácie

**Ilustrácie** sú obrázky obsahujúce **grafy**, **diagramy**, **mapy**, **schémy** a pod. Nie je potrebné rozlišovať rozličné typy ilustrácií, stačí, ak sa všetky označia ako „Obrázok”. Všetky ilustrácie musia byť očíslované súvislým radom číslic v celej práci a musia mať titulky (názov obrázku) pri každom obrázku. Text titulku musí byť pochopiteľný aj bez kontextu. Majú sa zaradiť bezprostredne za textom, kde sa spomínajú po prvýkrát (najlepšie na tej istej strane). Obrázok by mal byť podľa možnosti centrovaný. Pri odkazovaní na daný obrázok v texte použijeme odkaz uvedený v zátvorke (napr. Obr. 1).



Obr. 1 Názov obrázka (štýl Popis, Popiska-Caption)

* 1. Tabuľky

Tabuľky prezentujú myšlienky a tvrdenia popisované v práci. Akýkoľvek tabuľkový materiál, ktorý sa skladá z viac než štyroch alebo piatich riadkov, by mal byť spracovaný do formy tabuľky. Popis a záhlavie tabuľky má byť zrozumiteľné samostatne bez odkazu na text. Záhlavia majú vyjadrovať druh veličiny a typy jednotiek vo forme „veličina/jednotka”, je potrebné používať rovnaké symboly a skratky ako v texte. Každá tabuľka musí mať poradové číslo a titulok, umiestnený zvyčajne nad tabuľkou. Tabuľka by mala mať rovnakú orientáciu, ako text práce.

Tab. 1 Názov tabuľky (štýl Popis, Popiska-Caption)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | 1.A | 1.B | 1.C | 1.D |
| prezentácie | 10 | 12 | 13 | 11 |
| videá | 7 | 4 | 6 | 3 |
| počítačové hry | 5 | 6 | 3 | 4 |
| blogy | 6 | 8 | 7 | 8 |
| postery | 4 | 3 | 5 | 6 |

* 1. Zdrojový kód programu

Na zápis zdrojového kódu programu použijeme štýl kód (písmo Courier New 11, zarovnanie vľavo, orámovanie s tieňom).

viem hľadajCestu

  kým [farbabodu <> "čierna] [vz 1]

  do 1 vp 90

  kým [farbabodu <> "červená] [

   vp 90 do 1

   ak farbabodu = "čierna [

    vz 1 vl 90 do 1

    ak farbabodu = "čierna [vz 1 vl 90]

   ]

   čakaj 1

  ]

koniec

* 1. Rovnice, vzorce

Rovnice sa uvádzajú v strede riadka, vysvetlivky symbolov na začiatku riadku. Vysvetlivky symbolov sa uvádzajú od začiatku riadka. Ak je v práci viac vzorcov, uvádzame číslo vzorca do okrúhlych zátvoriek bez medzier umiestnených na pravom konci riadka. Pre písanie fyzikálnych veličín a matematických premenných sa používa kurzíva. Používame sústavu jednotiek SI (ISO 31 a ISO 1001). Pri písaní rovníc používame **editor rovníc (musíme ho mať nainštalovaný)**.

1. Záver

Záver obsahuje vecné závery, sumarizáciu, vlastný prínos alebo pohľad autora, odporúčania pre prax (výučbu). Záver je uvedený na maximálne 1 stranu.

Zoznam použitej literatúry (Nadpis Kapitoly, bez čísla)

Všetky dokumenty, ktoré v práci použijete, je potrebné zoradiť do zoznamu pozostávajúceho z  bibliografických odkazov, ktorý označujeme **Zoznam použitej literatúry**. Pre tvorbu zoznamov použitej literatúry platia štandardy. Cieľom je, aby zo zoznamu použitej literatúry bolo možné jasne identifikovať použitý zdroj a aby ho bolo možné bez ťažkostí opäť vyhľadať.

Hlavným zdrojom údajov pre tvorbu bibl. odkazov je **titulný list** (tzn. prvý list v knihe, kde sú uvedené údaje o názve autorovi atď.), príp. jeho rub. Odkazy sa môžu týkať knižných, časopiseckých a iných zdrojov informácií (zborníky z konferencií, patentové dokumenty, normy, odporúčania, kvalifikačné práce, osobná korešpondencia a rukopisy, odkazy cez sprostredkujúci zdroj, elektronické publikácie), ktoré boli v práci použité.

**Technika citovania** určuje spôsob, akým označujeme citácie v dokumente, pričom podľa normy (pozri STN ISO 690) existuje viacero spôsobov citovania. Pri metóde **číselných citácií** sa v zozname bibliografických odkazov každé citované dielo uvádza v tom poradí, v akom bolo uvedené a číslované v texte. Číslované odkazy v texte sú uvedené v zátvorkách [3] a odkazujú na dokumenty v takom poradí, v akom sa citujú po prvýkrát. Nasledujúce citácie dostávajú také isté číslo, ako má prvá citácia. Ak sa citujú osobitné časti dokumentu, môžu sa za číslom citácie uviesť čísla strán.

**Príklad zoznamu použitej literatúry:**

1. KALAŠ, Ivan – BLAHO, Andrej: *Tvorivá informatika. 1. zošit z programovania.* Bratislava: SPN - Mladé letá, 2007. 48. s. ISBN 80-10-01723-2
2. CIMBALA, Roman – BALOGH, Jozef – DŽMURA, Jaroslav: Diagnostika výkonových transformátorov s využitím prvkov umelej inteligencie 1. In: *Elektrotechnický magazín ETM*. roč. 14, č. 1 (2004), s. 8-9.
3. Kolektív autorov: *Štátny vzdelávací program*. [online] Bratislava: ŠPU v Bratislave, 2008. Aktualizované 14.2.2010 [cit. 2010-02-17]. Dostupné na internete: <http://new.statpedu.sk/sk/filemanager/download/987>
4. Elektronické diplomové a dizertačné práce SR: ETD SK. [online]. Košice : ETD SK, 2004. Aktualizované 14-2-2005 [cit 2005-03-10]. Dostupné na internete: <http://www.etd.sk/>.
5. KATUŠČÁK, Dušan: *Ako písať záverečné a kvalifikačné práce*. Nitra: Enigma, 2004. 162 s. il. ISBN 80-89132-10-3

Prílohy (štýl Nadpis Kapitoly, bez čísla)

Zoznam príloh záverečnej práce:

* Príloha A – CD médium
* Príloha B – <názov prílohy>
* Príloha C – <názov prílohy>

Táto časť záverečnej práce obsahuje zoznam všetkých príloh. Číslovanie strán príloh nadväzuje na číslovanie strán v hlavnom texte.

Príloha A – CD médium (štýl PodNadpis Kapitoly, bez čísla)

Priložené CD médium **povinne** obsahuje text záverečnej práce vo formáte PDF. CD môže obsahovať edukačný hypertext, metodické listy, dotazníky a ukážky projektov atď. CD médium zabalené do papierového obalu sa vlepí na vnútornú stranu zadnej obálky záverečnej práce.

Príloha B – <názov prílohy>

<popis prílohy>

Príloha C – <názov prílohy>

<popis prílohy>