STREDNÁ PRIEMYSELNÁ ŠKOLA ELEKTROTECHNICKÁ

**Antivírus**

Spôsob fungovania a hrozby

**LUKÁŠ ELIAŠ**

2024

Obsah

Obsah 2

Anotácia 3

1 Antivírus 4

1.1 Úloha antivírusu 4

2 Vírus 5

2.1 Malware 5

2.2 Spyware 5

2.3 Phishing 5

3 Tvorba učebného materiálu 6

3.1 Začiatok 6

3.2 Hľadanie potrebných materiálov 6

4 Špecifikácia produktu 7

4.1 Dizajn a rozloženie 7

4.2 Fonty 7

4.3 Obrázky 8

4.3.1 Prvky prezentácie 8

5 Vnútorné spracovanie 9

5.1 Jednoduchosť 9

6 Záver 11

Zoznam použitej literatúry (Nadpis Kapitoly, bez čísla) 12

Anotácia

Táto práca sa zameriava na význam antivírusového softvéru v kontexte kybernetickej bezpečnosti. Analyzujem úlohu antivírusového softvéru pri ochrane počítačových systémov pred rôznymi typmi malvéru, vrátane vírusov, spyware a phishingu. Práca obsahuje rozdelenie malvéru do kategórií a diskutuje o ich charakteristikách a metódach infekcie. Okrem toho sa zaoberá aj vývojom antivírusového softvéru a jeho schopnosťou prispôsobiť sa neustále sa meniacim kybernetickým hrozbám. Cieľom práce je poskytnúť ucelený prehľad o význame antivírusového sofvéru v ochrane pred kybernetickými hrozbami a jeho úlohe pri zabezpečovaní bezpečnosti používateľských systémov.

**Annotation**

This work focuses on the importance of antivirus software in the context of cyber security. I analyze the role of antivirus software in protecting computer systems from various types of malware, including viruses, spyware, and phishing. It contains the division of malware into colors and products by their characteristics and methods of infection. In addition, it is also reflected in the development of antivirus software and its ability to adapt to constantly changing cyber threats. The aim of the thesis is to provide a comprehensive overview of the importance of antivirus software in protection against cyber threats and its role in ensuring the security of user systems.

1. Antivírus

Antivírusový softvér, skrátene označovaný ako antivirus, je program navrhnutý na detekciu, prevenciu a odstránenie škodlivého softvéru z počítača, ako sú vírusy, červy, trojanské kone, špionážne programy a iné druhy malware. Jeho hlavným účelom je ochrana užívateľov počítačov pred stratou údajov, poškodením systému alebo zneužitím osobných informácií. Antivírus hrá kľúčovú úlohu v boji proti škodlivému softvéru a ochrane počítačových systémov. Jeho základnou funkcií je monitorovanie aktivít na počítači a detekcia prítomnosti potenciálne škodlivého kódu, ako sú vírusy, červy, trojanské kone a ďalšie formy malware. Keď antivírusový program identifikuje nebezpečný kód, okamžite reaguje a vykonáva kroky na jeho neutralizáciu.

* 1. Úloha antivírusu

Jednou z hlavných úloh antivírusového softvéru je prevencia infikácie systému. To znamená, že sa snaží zabrániť vstupu škodlivého kódu do počítača alebo jeho šíreniu v systéme. Tento cieľ sa dosahuje pomocou rôznych techník, ako sú skenovanie súborov a priečinkov, monitorovanie internetového prehliadania, kontrolovania príchodu a odchodu dát cez sieť, a iných bezpečnostných opatrení. Okrem prevencie sa antivírusový softvér tiež zaoberá liečbou infikovaných systémov. Ak sa počítač napriek opatreniam infikuje, antivírusový program sa snaží identifikovať, izolovať a odstrániť škodlivý kód a minimalizovať tak škody spôsobené infekciou. Tento proces zahŕňa čistenie infikovaných súborov, opravy poškodených systémových súborov a zabezpečenie, že sa infekcia nešíri ďalej. Celkovo možno povedať, že antivírusový softvér je nepostrádateľným nástrojom v ochrane počítačov a sietí pred škodlivým softvérom. Jeho schopnosť monitorovať, detegovať a neutralizovať hrozby je kľúčová pre udržanie bezpečnosti a integrity digitálnych prostredí. Bez neho by boli počítače a zariadenia vystavené vysokému riziku infikácie a možným závažným následkom.

1. Vírus

[Počítačový vírus](https://sk.wikipedia.org/wiki/Po%C4%8D%C3%ADta%C4%8Dov%C3%BD_v%C3%ADrus) je program, ktorý dokáže rozmnožovať sám seba pridávaním svojho kódu do iných [programov](https://sk.wikipedia.org/wiki/Po%C4%8D%C3%ADta%C4%8Dov%C3%BD_program). Pre svoje rozširovanie teda podobne ako biologický vírus potrebuje hostiteľa – iný program. Z toho vyplýva, že do počítača sa môže dostať jedine tak, že spustíme nainfikovaný program. Spolu so spustením nainfikovaného programu sa aktivuje vírus v operačnej pamäti, a potom napadne i ďalšie [súbory](https://sk.wikipedia.org/wiki/S%C3%BAbor_(informatika)) v počítači.

* 1. Malware

Malware je zlomyseľný kód či softvér, ktorý obyčajne poškodí alebo zablokuje, zmocní sa alebo odcudzí informácie z počítačového systému. Malware sa do počítača v dnešnej dobe dostáva zvyčajne cez [Internet](https://sk.wikipedia.org/wiki/Internet), hlavne pri prezeraní škodlivých stránok s nie dobre zabezpečeným systémom.

* 1. Spyware

Spyware je počítačový program, ktorý sa bez vedomia používateľa pokúša „vyšpehovať“ citlivé dáta z počítača (napr. heslá). Tieto dáta sa potom pokúša poslať tretej strane. Následné posielanie informácie tretej strane značne spomaľuje chod počítača na internete a môže aj prepisovať URL zadané v internetovom prehliadači. Spyware sa nešíri vlastnou replikáciou ako je tomu pri [počítačových vírusoch](https://sk.wikipedia.org/wiki/Po%C4%8D%C3%ADta%C4%8Dov%C3%BD_v%C3%ADrus) a [červoch](https://sk.wikipedia.org/wiki/Po%C4%8D%C3%ADta%C4%8Dov%C3%BD_%C4%8Derv) ale najčastejšie sa do počítača dostáva nainštalovaním samotným používateľom. Keďže je nepravdepodobné, že by si niekto takýto softvér nainštaloval dobrovoľne, snaží sa spajvér tváriť ako užitočný program.

* 1. Phishing

Phishing je „pokus o podvodné získanie citlivých informácií, ako sú heslá a podrobnosti o kreditných kartách, maskovaním sa za dôveryhodnú osobu alebo dôveryhodný obchod (alebo banku) pri elektronickej komunikácii“. Existuje viacero spôsobov „lovenia hesiel“. Najčastejšie phishing prebieha tak, že podvodník (útočník) sa pomocou podvodného ([klamlivého](https://sk.wikipedia.org/wiki/Klam)) [e-mailu](https://sk.wikipedia.org/wiki/E-mail) snaží nasmerovať používateľa na [webstránku](https://sk.wikipedia.org/wiki/Webstr%C3%A1nka) alebo všeobecnejšie [URL adresu](https://sk.wikipedia.org/wiki/Jednotn%C3%BD_vyh%C4%BEad%C3%A1va%C4%8D_prostriedku), ktorú pripravil práve na tento podvodný účel.

1. Tvorba učebného materiálu

Úvod do mojej prezentácie o antivírusovom softvéri je vchodová brána do sveta kybernetickej bezpečnosti. Snažil som sa vytvoriť atmosféru zvýrazňujúcu dôležitosť ochrany našich digitálnych prostriedkov, ktorá sa stáva nevyhnutnosťou v dnešnej digitálnej ére. Antivírusový softvér, ktorý budem predstavovať, je viac než len obyčajný program - je to štít, ktorý bráni naše dáta, súkromie a identitu pred rôznymi kybernetickými hrozbami. Cieľom mojej prezentácie je priblížiť divákom základné pojmy a princípy, ktoré sú spojené s antivírusovým softvérom, a ukázať, ako môže táto technológia pomôcť chrániť nás a naše digitálne zariadenia. Chcem, aby diváci odchádzali s jasným pochopením toho, ako môžu chrániť seba a svoje digitálne životy pred kybernetickými hrozbami, a aby sa cítili povzbudení k aktívnej ochrane svojich dát a zariadení.

* 1. Začiatok

Začiatky tvorby prezentácie sú ako prvý krok na dlhej ceste od myšlienky k hotovému výsledku. Vymyslenie vhodnej témy je rozhodujúcim momentom, ktorý určuje smer a zameranie celej prezentácie. Téma je veľmi zaujímavá, produkt bol robený rovnako pútavo aby čitateľa nielen zaujal ale dokonca aj presvedčil a vstúpil do jeho mysle, aby sa nad danou problematikou zamyslel. Týmto chcem dosiahnuť aj to aby si čo najviac ako sa dá zabezpečil svoju elektroniku, či je to počítač, notebook alebo mobilný telefón a neveril všetkému na internete, takisto sa nedal nachytať osobám páchajúcim zločiny cez internet.

* 1. Hľadanie potrebných materiálov

Moja príprava na prezentáciu o antivírusovom softvéri bola veľmi dôkladná. Začal som s literatúrou a online zdrojmi, kde som sa hlbšie ponoril do tém ako kybernetické bezpečnostné hrozby, fungovanie antivírusového softvéru a trendy v oblasti ochrany pred malwarom a phishingom. Skúmal som rôzne zdroje, aby som získal široký pohľad na tému, a snažil som sa overiť autenticitu informácií. Bolo to veľmi náročné pretože som sa stretol s duplikátmi ktoré každý uvádzali inú skutočnosť. Analyzoval som prípadové štúdie a reálne príklady, čo mi pomohlo lepšie pochopiť úlohu antivírusového softvéru. Príprava mi dáva dobrý základ pre úspešnú prezentáciu, ktorá bude dúfam zaujímavá pre čitateľov.

1. Špecifikácia produktu

Táto kapitola je zameraná na dizajn a rozloženie prezentácie o antivírusovom softvéri a kybernetickej bezpečnosti. Dizajn a rozloženie sú kľúčovými prvky, ktoré ovplyvňujú úspech prezentácie a schopnosť publiku efektívne absorbovať informácie. Budeme skúmať spôsoby, ako správne využiť obrázky, grafiku, text a ďalšie prvky, aby sme vytvorili prezentáciu, ktorá bude nielen atraktívna vizuálne, ale aj informatívna a ľahko pochopiteľná pre naše publikum. Pri navrhovaní dizajnu a rozloženia sme sa snažili dosiahnuť rovnováhu medzi estetikou a funkcionalitou, aby sme maximalizovali efektivitu komunikácie a zanechali trvalý dojem na našich poslucháčov. Poďme teraz spoločne preskúmať, aké konkrétne kroky sme podnikli pri tvorbe dizajnu a rozloženia tejto prezentácie.

* 1. Dizajn a rozloženie

Pri tvorbe dizajnu a rozloženia prezentácie som sa zameriaval na jednoduchosť a estetiku, aby som zabezpečil, že moje posolstvo bude jasne a účinne komunikované. Prezentácia má moderný a futuristický vzhľad, s obrazmi a grafikou, ktoré okamžite pritiahnu pozornosť čitateľa a udržia ju. Využil som obrázky s hravými a inovatívnymi formami, ktoré majú za cieľ zapôsobiť na čitateľa a zanechať si v jeho mysli trvalý dojem. Rozloženie textu som zvolil tak, aby bolo prehľadné a organizované. Text bol umiestnený po stranách prezentácie, čím som dosiahol rovnováhu medzi obsahom a vizuálnym prvkom. Tento prístup mi umožnil vytvoriť prezentáciu, ktorá pôsobí dobre premyslene a usporiadané, čo pomáha udržať pozornosť diváka a zabezpečiť, že informácie sú ľahko dostupné a zrozumiteľné. Týmto spôsobom som sa snažil minimalizovať chaotický dojem a zabezpečiť, že prezentácia bude pôsobiť profesionálne a presvedčivo.

* 1. Fonty

Fonty, ktoré som použil vo svojej prezentácii, boli starostlivo vybrané s ohľadom na ich vhodnosť pre tému a rozloženie textu. Pre telo textu som zvolil font Tw Cen MT, ktorý je moderný a plynulý, čo zabezpečuje ľahkú čitateľnosť. Tento font sa hodí k téme antivírusového softvéru a kybernetickej bezpečnosti svojím profesionálnym vzhľadom a moderným štýlom. Na nadpisy som použil font Tw Cen MT Condensed, ktorý pridáva určitý nádych štýlu a zároveň pomáha zvýrazniť dôležité body a hlavné témy prezentácie.

* 1. Obrázky

Obrázky v mojej prezentácii sú podobné kruhom v digitálnom vesmíre, ktoré pripomínajú moderné portály do sveta IT bezpečnosti. Ich futuristický dizajn a formy do kruhov dodávajú vizuálnu atraktivitu a zároveň evokujú pocit inovácie a technologického pokroku. Tento estetický prístup bol zvolený s cieľom zaujať a udržať pozornosť divákov. Každý slide obsahuje iba jeden obrazok, ktorý sa nachádza vo vyváženom stredovom bode, čo umožňuje divákom ľahko sa sústrediť na jeho obsah. Okrem toho boli do obrazov pridané malé detaily a prvky, ktoré pomáhajú vytvoriť atmosféru a zvýrazňujú ich význam v kontexte prezentácie o kybernetickej bezpečnosti. Tieto prvky dopĺňajú hlavný obsah a podčiarkujú hlavné myšlienky, čo prispieva k celkovému dojmu profesionality a vizuálnej príťažlivosti prezentácie.

* + 1. Prvky prezentácie

V mojej prezentácii som zahrnul niekoľko dizajnových prvkov, ktoré pomáhajú vizualizovať koncepty a hrozby v oblasti kybernetickej bezpečnosti. Do produktu boli implementované, pretože si čitateľ bude môcť lepšie zapamätať danú tému aj pri pohlade na objekty. Uľahčuje mu to potom učenie. Prvým dizajnovým prvkom je oranžová ryba, ktorá symbolizuje phishing. Tento 3D objekt predstavuje, ako rýchlo sa človek môže stať obeťou útoku phishingu a ako ľahko môže byť zvedený na klamné správy a podvodné požiadavky. Ryba je výrazná a zaujímavá, čo pomáha upútať pozornosť divákov a zdôrazniť vážnosť tohto typu kybernetického útoku. Ďalším dizajnovým prvkom je modré oko, ktoré reprezentuje spyware. Tento symbol zdôrazňuje, že používateľ je pod dohľadom pri útoku spywareu. Oko evokuje pocit sledovania a invázie do súkromia, čím vizuálne demonštruje nebezpečenstvo, ktoré predstavuje tento typ malvéru. Nakoniec, na slide o malvéroch, som zahrnul obraz vírusu v ktorý bežne napáda ľudské telo. Tento obraz ponúka ďalší spôsob, ako vizualizovať škodlivé účinky malvéru na počítačové systémy. Podobnosť s ľudským telom môže zdôrazniť invazívnu a deštruktívnu povahu malvéru a jeho schopnosť poškodiť a infikovať cieľový systém. Tieto dizajnové prvky nielenže pomáhajú vizualizovať rôzne hrozby v kybernetickej bezpečnosti, ale aj pridávajú estetickú hodnotu prezentácii a pomáhajú udržať pozornosť divákov.

1. Vnútorné spracovanie

V rámci vnútorného spracovania produktu som sa zameral na štruktúrovanie textu a obsahu tak, aby boli pre čitateľa jasné a prístupné. Rozhodol som sa umiestniť text do malých odsekov na pravú alebo ľavú stranu snímky, čo umožňuje plynulé čítanie a zabraňuje divákovi v záplave informácií. Tieto odseky dodávajú estetickú hodnotu prezentácii a zabezpečujú, že čitatelia sa v texte nestratia. Umiestnenie textu na pravú alebo ľavú stranu snímky zlepšuje celkovú rovnováhu dizajnu a umožňuje efektívnejšie využitie priestoru na prezentácii. Tento prístup tiež pomáha divákom sústrediť sa na obsah, keďže text je jasne oddelený od ostatných vizuálnych prvkov. Spoločne s kvalitným obsahom textu tieto estetické prvky pridávajú hodnotu prezentácii a zabezpečujú, že jej vizuálny dojem bude príťažlivý a profesionálny.

* 1. Jednoduchosť

V tejto podkapitole sa zameriavam na jednoduchosť textu a predstavujem veľmi jednoducho spracovaný obsah, ktorý je priateľský k čitateľovi nielen vo svojom dizajne, ale aj vo svojom obsahu. Cieľom je poskytnúť čitateľovi rýchlo pochopiteľné a zrozumiteľné informácie, ktoré sú vystihnuté jasne a stručne.

Pri tvorbe tejto časti som sa snažil o minimalizáciu odborných termínov a zložitých konceptov, aby bol obsah prístupný širokej škále divákov, dokonca aj študentom. Text bol navrhnutý tak, aby bol priateľský a prístupný, pričom sa zároveň zachováva jeho informačná hodnota. Tieto jednoducho spracované informácie budú rýchlo pochopiteľné pri pohľade na slide, čo umožní čitateľovi rýchlo sa oboznámiť s obsahom a porozumieť mu bez zbytočného zaváhania. Výsledkom je prezentácia, ktorá je jednoduchá, zrozumiteľná a prívetivá pre svoje publikum.



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

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

1. Záver

V závere mojej práce o antivírusovom softvéri a kybernetickej bezpečnosti by som rád zdôraznil niekoľko kľúčových myšlienok. Táto práca mi poskytla možnosť hlbšie sa ponoriť do problematiky kybernetickej bezpečnosti a porozumieť dôležitosti antivírusového softvéru v ochrane našich digitálnych systémov. Jedným z hlavných zistení tejto práce je, že dôkladná príprava a použitie spoľahlivých zdrojov sú nevyhnutné pre úspech v akejkoľvek prezentácii alebo projekte.

Hľadanie kvalitných informácií a ich overovanie je kľúčové pre vytvorenie dôveryhodného a informatívneho obsahu. Okrem toho som sa naučil, že estetický a priateľský dizajn môže zlepšiť celkový dojem prezentácie a pomôcť divákom lepšie pochopiť a zapamätať si prezentované informácie. Použitie vizuálnych prvkov, ako sú obrázky a grafika, môže výrazne obohatiť prezentáciu a prispieť k efektívnej komunikácii obsahu. Nakoniec, táto práca ma motivovala k ďalšiemu preskúmaniu problematiky kybernetickej bezpečnosti a k neustálemu vzdelávaniu sa v tejto oblasti. Súčasný digitálny svet prináša stále nové výzvy a hrozby, a je nevyhnutné byť neustále informovaný a pripravený na ochranu našich systémov a údajov. Celkovo som presvedčený, že pochopenie a osvojenie si princípov kybernetickej bezpečnosti a dôkladná príprava sú kľúčovými krokmi k zlepšeniu bezpečnosti a ochrany našich digitálnych prostredí. Som vďačný za túto príležitosť sa venovať tejto problematike a verím, že moja práca môže prispieť k šíreniu informácií a zvýšeniu povedomia o dôležitosti kybernetickej bezpečnosti v dnešnom digitálnom veku.

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